UNIVERSITÀ DEGLI STUDI DI PADOVA

DIPARTIMENTO DI INGEGNERIA INDUSTRIALE

CORSO DI LAUREA MAGISTRALE IN
CHEMICAL AND PROCESS ENGINEERING

Tesi di Laurea Magistrale in Chemical and Process Engineering

IMPROVING THE SAFETY IN ACADEMIC RESEARCH LABORATORIES: THE CASE OF THE FISCHER-TROPSCH SYNTHESIS

Relatore: Ing. Paolo Mocellin
Correlatore: Prof. Carlo Pirola

Laureanda: GASPAROTTO FRANCESCA

ANNO ACCADEMICO 2022 - 2023

Abstract

Injuries, accidents, and facility-related incidents are commonly reported in pilot plants and academic laboratories worldwide. These contexts are characterized by variable operating conditions, equipment setups, high potential for human error, and lack of training, resulting in high-risk scenarios. Despite the availability of dedicated risk assessment techniques, hazards and risks associated with research activities are often underestimated.

This work proposes a structured implementation of a risk assessment framework to identify, manage, and reduce risks associated with an experimental setup for conducting Fischer-Tropsch syntheses. The study analyzes high-risk scenarios associated with deviations from the experimental test intent and implements proper risk reduction strategies. Additionally, the effects of manual procedures during experiments and laboratory infrastructure on risk levels are quantitatively assessed.

Table of contents

Introduction

The lack of a well-developed safety culture is the leading cause of accidents in academic laboratories during research and development activities. Differently from the industrial framework, research laboratories are characterized by various additional vulnerabilities, including variable operating conditions and equipment setup, high impact of human error, and improper training and determination of emerging risk scenarios.

This has determined a high-frequency environment for near misses, incidents and accidents, also resulting in severe outcomes. Although a portfolio of dedicated risk assessment techniques is available, a generalized underestimation of hazards and risks emerges.

A risk assessment should identify potential hazards and implement controls to eliminate or reduce risks to people, operations or property. Moreover, a new risk assessment should be completed and documented each time a new potentially hazardous experiment is planned. This aspect is often overlooked, leading to risk misperception or inadequate risk-reduction measures. Consequently, experiment participants can face associated tasks with imperfect operating procedures or without available or up-to-date documentation.

Current statistics show that academic laboratories share the majority of accidents. This poses a serious concern that urges robust, extensive and comprehensive actions. Unfortunately, research hazard analysis and risk assessment is more complex than in industrial settings.

This work conducts a risk assessment for a Fischer-Tropsch pilot plant in an academic lab. Various techniques, including interaction matrix and HAZOP analysis, identify material incompatibilities and potential hazards. Results are analyzed by risk class, and a Layer of Protection Analysis (LOPA) is done to define protective measures for high-risk events.

This thesis consists of four chapters. The first chapter provides an overview of risk scenarios and accidents related to the academic setting and pilot plants. Chapter 2 mainly focuses on the peculiarities of pilot plants and research infrastructures when dealing with safety, hazards and risks. In particular, it analyzes the intrinsic hazardous features of pilot plants, including the management of hazardous substances, second-hand equipment, limited availability of information and the role of human error and training. Chapter 3 illustrates the techniques used to perform the risk assessment of the case study, i.e. the interaction matrix, the HAZOP and the LOPA analyses. The results and the discussion are provided in Chapter 4, including proper recommendations and improvements for reducing high-risk scenarios.

This work was carried out in collaboration with the Università degli Studi di Milano, which provided key information for developing the risk assessment under discussion.

Chapter 1

Academic laboratories: framework and statistics of accidents

Academic laboratories and associated activities can be hazardous and lead to associated risk scenarios. Moreover, everyone working is adequately trained to deal with hazardous scenarios, and properly structured steps are rarely implemented to identify hazards and risks. This chapter provides the framework of academic laboratories and analyses the leading causes and consequences of incidents and accidents in chemistry and engineering laboratories, including pilot plants.

1.1 Introduction

Chemical and engineering laboratories are inherently dangerous places. Students, principal investigators and workers may handle hazardous substances and equipment such as solvents (i.e. toxic, flammable, corrosive, explosive), glassware (i.e. flasks, pipettes, burettes, etc.) and specific engineering equipment such as valves, reactors, separators and pressurized equipment. [1]. Although the culture of safety is changing, incidents and fatalities still occur in chemical laboratories [2,3]. High schools usually use standard equipment, but universities and industry may also work with equipment that operates at high pressures or other hazardous conditions, including pilot plants and *ad-hoc* developed technologies and assemblies. Indeed, Figure 1.1 [3] shows that universities have the highest number of incidents and injuries.

The possible cause of the accidents is that the hazardous scenario remains unidentified or underestimated. Risk analysis errors determine an unsafe working condition and a false sense of security, with an altered risk perception [4]. Studying previous incidents is essential for training workers and avoiding the same mistake. Unfortunately, not all accidents are reported because they do not result in any or major consequences in the laboratory or pilot plant and are classified as “near misses” [5]. However, these near misses should also be reported in the literature with the other accidents to avoid repeating mistakes that could lead to more severe consequences.

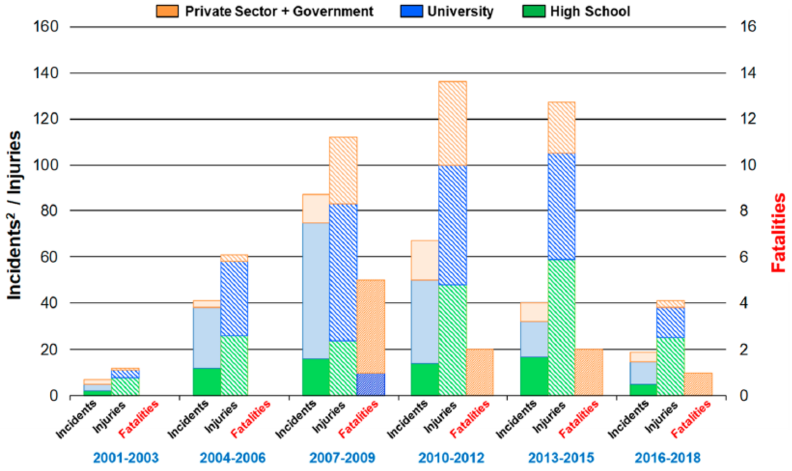


Figure 1.1: *Number of reported incidents, injuries and fatalities reported by CSB from January 2001 to July 2018 [3] .*

The aspects related to accidents in academic laboratories are analyzed in depth in this chapter, which first presents and discusses some case studies. Then, the leading causes and consequences of the incidents are presented to understand that accidents in academic laboratories occur due to a lack of training and a lack of compliance with specific safety regulations.

1.2 Case studies

There are many reports in the literature of accidents in academic laboratories worldwide and concerning pilot plants. Not all the case studies reported in the following paragraphs occurred in an academic setting. Nevertheless, they may help understand the leading causes and consequences of accidents in a laboratory setting.

Worldwide, more than two hundred accidents have occurred in chemical laboratories and pilot plants. The most common scenarios causing deaths/accidents are fires, explosions, and exposure to toxic materials (chemical and biological). Over the years, half of the deaths in chemical laboratories and pilot plants are due to explosions and fires, while 25% are due to exposure to toxic materials [5].

1.2.1 Case study: Dichloromethane injection injury

In July 2018, a student was attending an academic chemistry lab for two weeks and accidentally injected a small amount of dichloromethane (100µL) into one of his fingers.

The student was trying to fill an empty flask with the required dichloromethane, and a small amount of the solvent remained in the needle of the pipette.

The leader professor was immediately informed about the situation, and he understood that something was going wrong. The student went to the hospital, where he had a surgeon to remove all the dead flesh to avoid possible infections or gangrene.

The professor looked for more details about the effects related to dichloromethane injections. For instance, he searched for some information in the Material Safety Data Sheet (MSDS), but he found nothing. Unfortunately, other similar cases have been recorded worldwide, but safety data sheets have not been updated consequently [1,6].

This case study is about a widely used solvent in organic chemistry and common glassware. A reasonable conclusion could be that studying or using equipment with no sharp components is necessary, which can hurt the workers [1].

1.2.2 Case study: Hexane fire

A hexane fire starts due to the wrong handling of a flammable substance.

A new technician had to clean metal parts with hot hexane. A quantity of 100 mL of hexane was placed inside a 500 mL beaker. This beaker was placed upon a hot plate, and a magnetic stirrer was used to mix the contents. The working area was on an open bench near some bottles with different solvents, including hexane and paper towels. The fire started from the paper towel, which was too close to the hot plate and soaked in hexane. Another worker immediately extinguished the fire, and no injuries or significant damages were observed. A hood was indicated as a proper risk-reduction strategy.

Such an accident can be avoided through periodic training of employees and with adequate supervision of the new members of the laboratory [7].

1.2.3 Case study: Reflux system failure

In an academic research laboratory, a fire occurred due to a failure of the reflux system.

In the chemical laboratory, it was studying polymerization reaction with tetrahydrofuran (THF) system at reflux. A three-neck flask was used as a reactor; inside it, a mixture of sodium and potassium metal was used to obtain the amalgam NaK. The initial temperature at the reflux was equal to 66°C, but the overhead stirrer shaft jammed, and the flask cracked. All reacting mixture was released, and the reactive amalgam caught fire. This first fire destroyed a portion of the lab and damaged a part of the building, but no worker was injured. Later, a second fire was led by cleaning operations and two people got burned.

After 15 years from this accident, another similar incident occurred [7].

The lesson learned from this case study is that the hazard identification lacked relevant scenarios. In addition, some procedures are required when managing hazardous substances [7,8].

1.2.4 Case study: Unexpected reaction caused by excessive reactant

This case study is about an overpressure inside a pilot plant reactor after overcharging raw material.

The pilot plant considered was working in a batch condition to synthesize an organic compound. Three chemicals were involved: an aromatic compound (reactant), sodium hydroxide and another organic compound. The sodium hydroxide was added to the reactant to form the resulting sodium salt.

A human error led to the hazardous condition: the operator charged twice the amount of sodium hydroxide needed. Half of the sodium hydroxide (i.e., the extra quantity) reacted with a different substituent group, generating a by-product that polymerised when the reactor's temperature increased. Polymerization is an exothermic reaction that increases the reactor's pressure, and the rupture disk was broken. The safety device was well-sized and able to manage the associated scenario. So, no injuries were observed.

In a later analysis, it was discovered that the side reaction was known to the chemists, but it was not known to the people involved in the analysis of the safety of the pilot plant. This incident occurred before HAZOP analysis (discussed in Chapter 3) was introduced as a structured methodology in the chemical industry. HAZOP analysis is critical to prevent such a risk scenario since deviations analyzed include human errors, batch operations and deviations related to the quantity of materials [9].

1.2.5 Case study: Reaction between organic solvent and chlorine

A human error in a pilot plant caused an uncontrolled reaction between the organic solvent and chlorine.

This case study is about a batch pilot plant whose main objective was to develop the chlorination process. The reactor was first filled with an organic solvent, then an organic substrate was added to react with chlorine, which was gradually added. The by-product was HCl. The error in the process was that the organic substrate was not charged. Chlorine did not react with the organic compound, and the vapor phase of the reactor was rich in Cl_2. The solvent was sufficient to form a reactive and flammable mixture with the gas phase in the reactor, where the chlorine acted as the oxidizing agent. The mixture started to burn, and the installed rupture disk broke.

No safety analysis was carried out for this pilot plant, and this omission led to the incident described. In addition, there were insufficient safeguards to manage eventual flammable mixtures [9].

1.2.6 Case study: Purification of an organic product

When a fire occurred, a graduate student was working on the purification of a synthesis product via recrystallization.

The student wanted to purify the compound already obtained with diethyl ether. Still, the ventilated bench (bench with a chemical hood) was completely chaotic, so he decided to work on an open bench. A hot plate was used to heat the organic solvent mixture and the product from the synthesis. When the hot plate was switched on, a flash fire occurred, burning the student's hair, right arm and eyebrows. Fortunately, another graduate student saw the incident and extinguished the fire. The injured student suffered no severe injuries.

This incident could have been avoided if the student had followed the guidelines and worked under a fume hood, as the substances involved were flammable. In addition, a safe workplace in a chemical laboratory is a clean one, so he had to tidy up the messy bench [10].

1.2.7 Case study: Cumene hydroperoxide detonation

A detonation occurred at a pilot plant investigating the production of cumene hydroperoxide. The pilot plant was completely destroyed.

Two different studies have been performed in the past: laboratory-scale and kilo-scale. Both have been completed successfully, and a pilot plant has been designed to study the scale-up (the reactor capacity was equal to 400 L). One of the characteristics of the pilot plant, which is inherently dangerous, is that the operating conditions can change. The detonation was due to insufficient cooling in the reactor. The catalyst used in the last run differed from the one studied in previous kilo-scale studies. Heat transfer was also reduced by internal corrosion of the reactor. The operator observed a rapid temperature increase due to the reaction's exothermicity, leading to a rapid internal pressure increase. Unfortunately, the ventilation system was not correctly sized and cannot cope with the resulting scenario.

The incident could not have occurred if the operator had been sufficiently trained to deal with such a hazardous scenario. A HAZOP analysis and better plant monitoring could have prevented or assisted the operator in dealing with hazardous situations such as the one reported [11].

1.2.8 Case study: Pressure Vessel Release

On the evening of May 24, 1994, an employee of the Massachusetts biotechnology company died after opening a pressure vessel that was still under pressure [12].

1.2.8.1 Pilot Plant Description

The pilot plant was designed to extract taxol from yew needles with a supercritical fluid. The capacity of the extractor was equal to 25 L, and this equipment could work with a pressure of up to 5000 psi. To enhance the separation, chromatography columns were used.

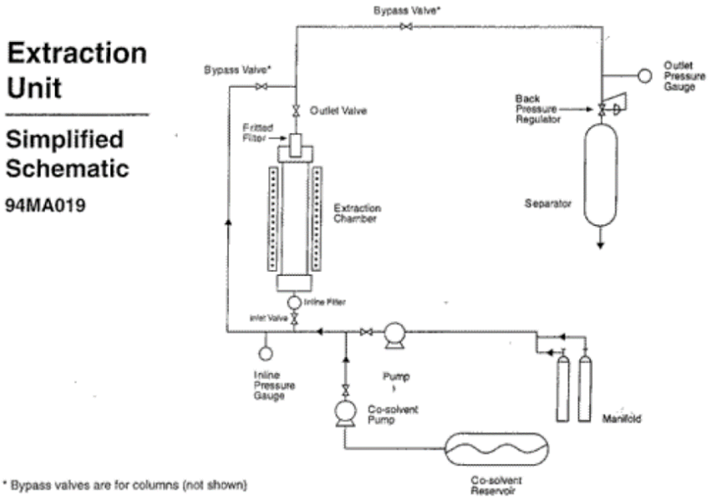


Figure 1.2*: Scheme of the pilot plant [12].*

Figure 1.2 [12] is the simplified scheme of the pilot plant walled in a plexiglass room. The back pressure regulator maintained the operative pressure equal to 2000 psi. The pressure inside the vessel was monitored by two pressure gauges (Figure 1.2).

The chemicals involved were carbon dioxide (75-90%) and methanol (10-25%). This second compound was pumped with two different flow rates into the process. Initially, the flow rate had a speed that allowed mixing with CO_2. After, the mixture was pumped at a higher rate where the carbon dioxide could not mix with methanol any more. This second step was essential to obtain a “plug” of methanol and yew material, which was successively washed in the extractor. After the final wash with CO_2, the depressurization of the system began, but the carbon dioxide exited through the separator [12].

1.2.8.2 The incident

When the incident occurred, the company was studying different operative conditions of the pilot plant to decrease the processing time and the amount of methanol. The victim was a 22-year-old operator who used the operative condition with a higher methanol flow rate. In addition, the organic compound was also recovered since it was the only one available that day. The run started at 4 PM, and at 5:22 PM, the first two extracted fractions were collected. It has been reported that after almost half an hour, the pressure decreased from 2000 psi to 800 psi in 17 minutes, and the flow rate of CO_2 was equal to zero. This decrease in pressure was too fast, so, according to coworkers, there are two possible hypotheses:

- There was a possible plug in the extractor;
- The operator opened the back pressure valve to decrease the pressure and increase the system's flow rate. This option could lead to a plug formation inside the extractor.

At 6:01 PM, the victim observed a very small flow rate of carbon dioxide, and after 14 minutes, he decided to depressurize the system since the plug was still inside the chamber. At 6:36 PM, the pressure system was equal to 2400 psi in the inlet line and 1700 psi in the outlet line. This was another indicator that a plug was still in the extractor. At 7:07 PM, the operator wrote that the plant was depressurised and was not working. The incident occurred at 8:45 PM when the victim decided to open the reactor since it was completely drained.

An assistant of the company's president noticed that the building's alarm and sprinkler system had been activated. The victim was on the floor with a slight pulse, and the body was more or less 10 feet from the extractor.

Investigators found that the extraction system was drained from the bottom, but the valve on the top was closed [12].

1.2.8.3 Hypothesis about possible scenarios

Further studies showed that the pressure gauges did not fail since if the pressure was much higher than 100 psi, the equipment cover would have been blown through the roof [12]. It is possible that the victim interpreted in a wrong way the value of pressure gauges since they had a low sensibility (1000 psi) and a margin of error equal to 10%.

Different hypotheses are studied to explain the plug inside the system:

- Plugs were inside one or both the filters (Figure 1.2)
- The inlet line was frozen after the depressurization
- A plug of methanol with yew material in the vessel

From the OSHA analysis, the third scenario is the most probable [12].

1.2.8.4 Final discussion

The company did not have a safety program or committee for the pilot plant. The operators were trained just for fire safety and hazard communication but no training about hazards connected to high-pressure systems. Another problem was that the company did not have standard operating procedures to open the equipment.

In order to avoid similar accidents in the future, the MA FACE (Fatality Assessment and Control Evaluation) Program [13] wrote some recommendations to the employers:

- Equipment cannot be opened if it is still under pressure;
- Verify through balances that there is no residual pressure inside the system;
- Specific training for equipment under pressure;
- Write procedures to avoid hazardous scenarios;
- A periodic safety review of the system [12].

All these recommendations should always be considered a good training practice (primarily in academic settings) and a safety culture standard.

1.2.9 Case study: fire in a lab

On February 20, 2021, a fire damaged the Resource Laboratory of the University of Vienna. The fire was caused by the failure of the laptop's lithium battery[14]. No one was injured.

At 01:42, the fire alarms and the smoke detection system sounded, but no one in the central security service noticed that. At 2:00, two security operators smelled smoke and called fire brigades. These latest arrived seven minutes late. At the beginning, the fire's location was unclear, but after it was located, the fire was extinguished by foam. The laptop had not been used for at least three years before and was inside a cabinet close to a bench and two fume hoods. The smoke and the fire's temperature completely damaged the ventilation system. In addition, the other four laboratories were irreparably damaged by smoke, water and foam near the source. The University lost five resourcing laboratories and more or less 60% of its equipment. Most of the glassware was unusable as the specific equipment.

In the following period, all the employers were interviewed by the police and insurance agents to determine the possible cause of the incident. The laboratories could not be rebuilt. Luckily, no one was injured, but the costs to repair the laboratories and buy the damaged equipment have been high, around 1.4 M€.

Despite the incident, the management of the storage of hazardous chemicals was good, as was the ventilation system. Still, the fire alarm protocol was weak, as was the cooperation with the fire brigade [14].

1.3 Accidents in China

Between 2000 and 2018, China reported 110 accidents in research laboratories [15] related to the increasing number of students and laboratories in Chinese universities [16]. There is a high probability that some chemical incidents from 20 years ago or more were not publicly reported since there was no internet and social media [15].

The rapid development of laboratories raises issues, such as safety management and a lack of rules and regulations [17]. Figure 1.3 [16] shows the trend over the years of accidents and the resources of the research laboratories. In 2010, there was a peak in the number of accidents. Then, the blue trend decreased since the government obliged the university laboratories to follow the fire safety management regulations and increase the laboratory's safety rules.

Almost half of the laboratory accidents occurred at universities in Beijing, Jiangsu and Shanghai (the highest percentage is in Beijing), as they have the highest number of graduate students. This confirms that the number of students participating in laboratories correlates with the number of accidents [16].

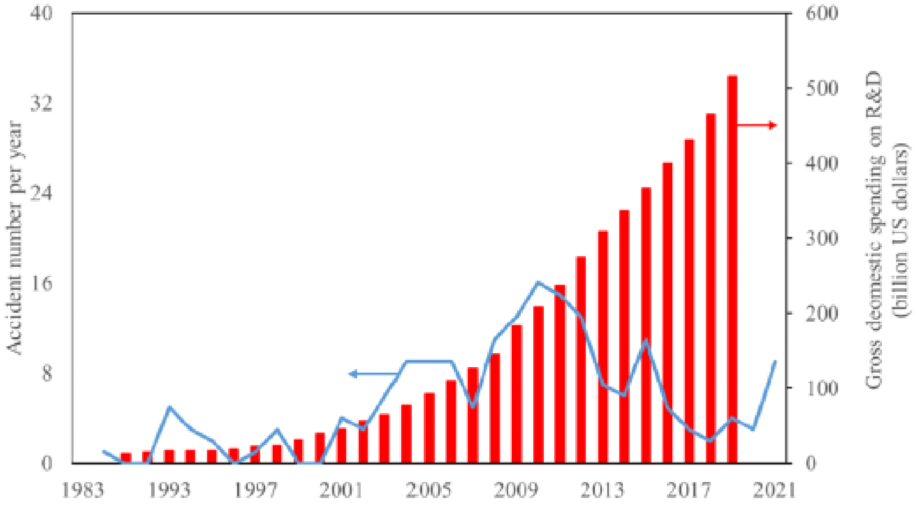


Figure 1.3: *Number of accidents for each year [16].*

1.3.1 Case study: Explosion in a chemical lab

The accident considered occurred at a Chinese university. The building had two floors with five labs in the first and four in the second. The incident was on the first floor, near almost 1 ton of magnesium powder stored in different containers. Seven students mixed phosphoric acid and magnesium power under a professor's guidance a couple of days before the incident. During this experiment, some magnesium powder exited from the mixer. The professor asked the students to cover the mixer's top with their lab coats. Almost 115 kg of magnesium powder (3/4 barrels) was used that day. The following day, the mixture was reacted with another component to obtain round particles placed on a bench in a neighbouring laboratory. Successively, two containers of magnesium were moved into the previous lab, but an explosion occurred along the transport of these barrels. The neighbouring laboratories were seriously damaged, and three students died.

Subsequent analysis revealed that the source of the explosion was the ignition of hydrogen generated during the mixing process the day before. A second explosion occurred due to the ignition of magnesium powder. This incident could have been avoided with a proper ventilation and insulation system. In addition, incorrect handling of hazardous chemicals can be a common mistake if the safety knowledge is inadequate. Correct training about safety and more regulations and rules are required to improve safety management [18].

1.3.2 Statistics of accidents in China

Some studies report that laboratory accidents in China have a certain regularity. In one paper, two periods are reported in which the majority of the accidents occur at the college, and these periods are March-June and October-December.

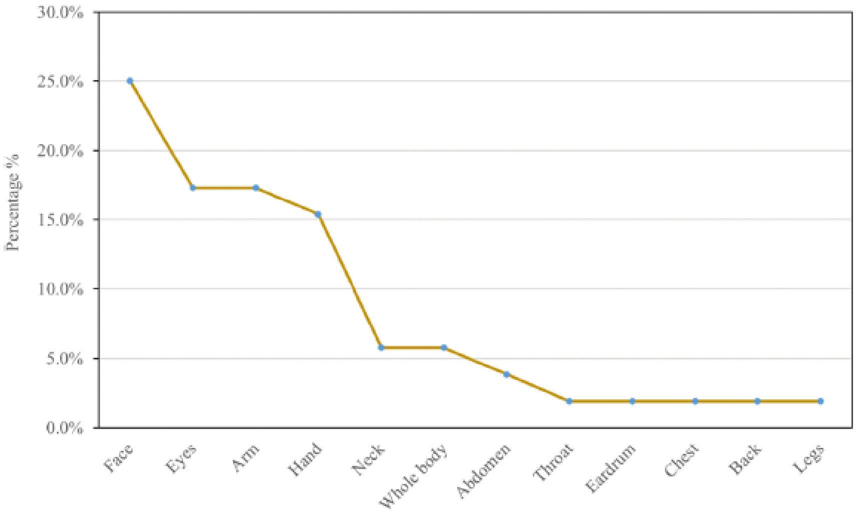


Figure 1.4: *Distribution of the causalities [16].*

Institutes and colleges do not have the same time management, so the period with the highest number of incidents at institutes differs from that at colleges between February and August.

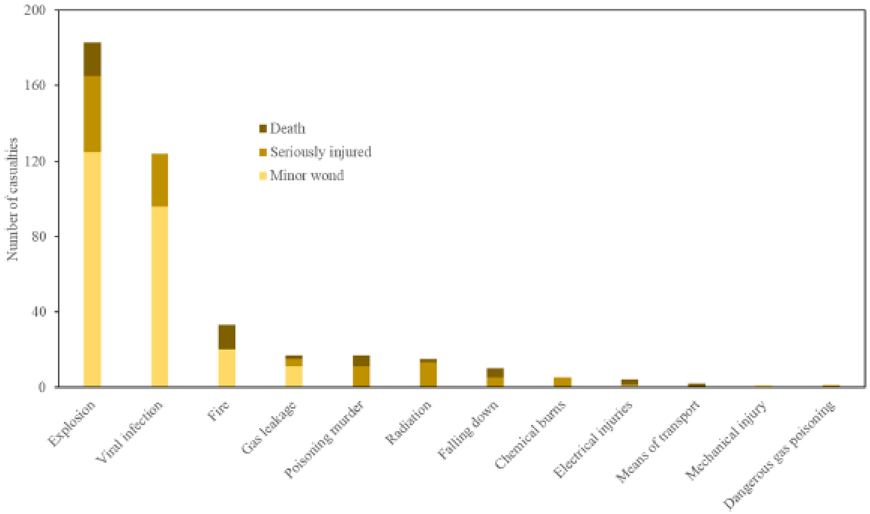


Figure 1.5: *Distribution of injured parts [16].*

In the last 39 years, 197 laboratory accidents have occurred, resulting in 365 injuries (255 minor and 110 serious) and 51 deaths [16].

Figure 1.4 [16] shows that explosions have the highest number of casualties. The distribution in Figure 1.4 is primarily related to the primary sources of danger in a chemical laboratory, mainly the usage of hazardous chemicals and their mishandling.

The most common body parts to be injured in a chemical accident are the upper body, such as the face, eyes and fingers (Figure 1.5) [16].

1.4 Causes of chemical incidents

As in China, other countries have seen rapid development in science and technology [17]. Over the years, the ACS (American Chemical Society) has wanted to add chemical/laboratory safety to the chemistry curriculum [10]. The education about safety should be based on the RAMP concept (Recognize hazards, Assess risk of hazard, Minimize risk of hazards, Prepare for emergencies) [10]. Figure 1.6 [17] describes the accident-type statistics in university laboratories from 2005 to 2017.

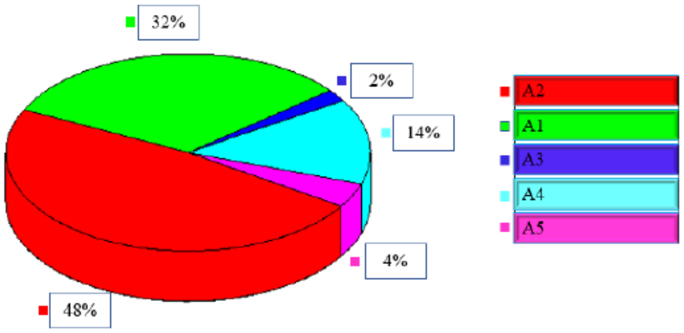


Figure 1.6: *Distribution of accident types from 2005 to 2017 [17]. Classification: (A1) fire accidents; (A2) explosion accident; (A3) mechanical injury accidents; (A4) toxic and hazardous substance injury accidents; (A5) biological safety accidents*

The following subsections will analyse the leading causes of different accidents.

1.4.1 Poor identification of hazards

From the case studies described in section 1.2 and others reported in the literature, mishandling hazardous substances is one of the main causes of an accident in a chemical laboratory. Most of the incidents involve students, and almost 70% of these accidents are caused by a misunderstanding and underestimation of the experiment's inherent dangers [10]. This can happen because the operator does not recognize or underestimate the hazardous condition [4]; consequently, the protection measures applied may be insufficient to deal with the hazardous scenario.

Usually, it is not straightforward to recognize that a specific scenario is dangerous. This is due to the knowledge of the chemicals or the operation involved (e.g., reaction, separation, crystallization, etc.). It is not easy to recognize or know the possible hazardous scenarios of a specific operation because, in an R&D laboratory, some experiments have never been performed before. A good starting point is to study the chemicals involved and their SDSs (Safety Data Sheets). A thorough study of the possible incompatibilities between the different substances should be done, particularly for new experiments. In addition, it is useful to increase the safety training for all the people working in the laboratory since some studies observed that people with high-level training also show better risk perception [4].

1.4.2 Ventilation system and misusage of hoods

A chemical laboratory usually requires a ventilation system for constant airflow [19]. It is not uncommon for protective layers to be used without following specific regulations. An example is to open the hood's doors more than the indicated height for the correct usage [20]. The problem with opening the door too far is that the aspiration/ ventilation system would not handle all the exhaust gases at the proper rate. In addition, if there are too many dangerous gases, the operator may not realize that they are coming out of the hood and inhaling them.

Another problem related to the hood is working with too much equipment inside [19], which can decrease the efficiency of the hood.

1.4.3 Inappropriate storage of chemicals

A typical issue is storing hazardous chemicals inappropriately. Many regulations about the storage of chemicals (e.g., NFPA, OSHA, etc.) must be followed to avoid possible accidents in academic laboratories. The wrong storage of substances is due to a lack of knowledge about the regulations and the inherent chemical properties. Moreover, new and innovative materials can be processed in academic research laboratories, thus increasing the uncertainty of hazardous properties.

The most common mistakes are the following:

- Excessive amounts are stored under the hood.
- Incompatible materials are not segregated.
- Chemicals are left on the edge of the bench
- The storage area has no or poor ventilation.
- The storage of flammables occurs in a ventilated cabinet.
- Chemicals are stored unsafely.

All the areas assigned to the storage of chemicals have to be approved areas and labelled.

Since most accidents involve fires or explosions, the flammable substances must be stored in an "approved" cabinet, not a ventilated one. The ventilation system causes a drop in pressure inside the cabinet, which can increase the spread of flames in an external fire. An "approved" cabinet for flammable chemicals isolates its internal area so that a possible external fire does not spread [20]. Finally, ensuring that two incompatible substances are not stored together is important, as this can lead to unexpected or expected dangerous scenarios such as fires and explosions.

Cryogenic and compressible gases are also hazardous, and regulations govern the storage. A common mistake is not following the required standards, such as ensuring a safe distance or placing an "approved" fire protection wall between two different classes of chemicals. Storing too many compressed gases or cryogenic fluids in a confined area can be dangerous as the ventilation system does not handle all gases [20]. Another cause of chemical accidents that can be considered in the context of improper chemical storage is improper waste management [21]. At the end of an experiment, glassware and residual solutions must be handled according to the regulations for solutions (considering their intrinsic hazards and classification) and for cleaning all used stuff.

1.4.4 Failure of the "failsafe" protection

Chemical laboratories are full of heating systems that act as hotplates. In recent years, these units have been fitted with independent "fail-safe" protection that stops the heating process if the temperature of the system exceeds a set maximum temperature. Unfortunately, this type of protection is not sufficient as it can fail. In addition, the failsafe protections (at least two systems) of complex appliances may share sensors or components; if one fails, both systems will fail [20].

1.4.5 Incorrect usage of electrical equipment

Extension cords and other electrical extensions are commonly used. It is common to see more than one extension cord connected in a cascade or a plug connected to an inappropriate adapter or socket. It is also typical to connect many devices to a power strip to compensate for the small number of sockets available in the laboratory. [20]. These scenarios are associated with electrical hazards that can lead to a short circuit and subsequent fire or explosion. This fire could be fed, causing damage to the laboratory. The same occurs if the electrical cables are aged and their insulation system is damaged.

It is essential to check the electrical equipment periodically and to use proper extension cords and sockets. The electrical system must comply with regulations, and the cables must be properly organized and compliant (ATEX Directive 2014/34/EU, [22]).

1.4.6 Pilot plants

Pilot plants involve more significant quantities of hazardous chemicals than is usual in a chemical laboratory, particularly flammable substances. Pilot plants are usually located in a laboratory building or a dedicated area, as the space required for the equipment is larger than for bench-top or laboratory pilot plants. The R&D pilot plants typically involve pipes with diameters between 6 and 50 mm [5] and small flow rates (e.g. 100 ml/min), much smaller than the quantities involved in an industrial plant where flow rates can be in the range of thousands of kg/h. Usually, pilot plants are placed in a fume cupboard, and a prior risk assessment has already been carried out if the risk level is "low" [20]. Most accidents in pilot plants are related to a lack of risk assessment or clear procedures for specific operations or scenarios. This is possible since the laws for pilot plants are less restrictive than the ones for chemical plants [23]. An in-depth analysis of the pilot plants is discussed in Chapter 2.

1.5 Main consequences of an accident in a chemical laboratory

Figure 1.6 [17] describes the distribution of the different types of accidents in a chemical laboratory. Figure 1.1 [3] shows the statistics of the different types of causalities. The possible consequences of the accidents include injuries and fatalities. The associated health problems may be acute or chronic [24]. Figure 1.1 shows that over the last 20 years, the number of fatalities in a chemical laboratory is much lower than the number of injuries. Usually, fires and explosions damage the laboratory and sometimes the building itself or nearby laboratories. When an accident occurs, an investigation is carried out to understand the causes and to learn from what happened. This investigation can take weeks or months; meanwhile, the laboratory cannot be used. This period can be very stressful for employers as they have to deal with many interviews with the police and insurance companies [14]. One of the most common issues in a chemical or academic lab is inaccessible escape routes. A safety issue is that some exits are blocked by boxes or equipment falling into disuse [20]. The presence of obstacles increases the probability of more severe injuries or fatalities.

Avoiding or reducing all possible causes of chemical accidents and establishing procedures to manage hazardous scenarios is the best way to minimize the potential consequences on human health and building damage.

1.6 Conclusive remarks

Chemical laboratories are hazardous places where several accidents occur every year. According to the OSHA (Occupational Safety and Health Administration), academic laboratories are 11 times more dangerous than those in the industrial sector [24]. Incidents in R&D laboratories can be minimized if operators and students are adequately trained to increase their ability to recognize hazardous scenarios.

Table 1.1: *Additional activities to reduce the frequency of accidents in academic laboratories.*

Activities	**Comments**
Written procedure for specific tasks	Clear written procedures can prevent some mistakes when carrying out a specific task.
Do not use damaged equipment	Damaged equipment can be hazardous. If the glassware is broken, it may have cutting edges that can injure the worker. If technical equipment (such as valves, pipes, seals, etc.) is broken, the resulting scenario can be very harmful.
Read the MSDS of the chemicals involved	Knowing the intrinsic properties of the chemicals involved is essential to know what protective measures (individual and collective) are required and how they should be managed.

The lack of hazard identification is the leading cause of chemical accidents since an unrecognised scenario comes with a defective consequent risk assessment. Moreover, preventive and protection measures can be insufficient. There are examples in the literature where good training of workers has resulted in no serious injuries. At Ohio State University, a fire and explosion destroyed the laboratory. A subsequent analysis reported that despite a three-alarm fire, no one was seriously injured due to previous training [25].

Table 1.2: *Additional activities to reduce the impact of the accidents*

Activities	**Comments**
Written procedure for hazardous scenarios	Clear written procedures for the most common hazard scenarios can reduce the impact of the consequences by ensuring workers know how to deal with them.
Periodic check of the equipment	Regularly checking the equipment (both glassware and technical equipment) is essential to ensure that the equipment works as expected.

In conclusion, risk assessment and worker training should be carried out regularly to reduce the likelihood of serious injury and to comply with new legislation. However, additional activities Table 1.1-2) should also be applied to reduce the frequency and impact of accidents.

Chapter 2

Experimental setups and pilot plants: features, hazards and risks.

Pilot plants and research apparatus are essential in academic settings for experimental investigations. They are considered the pre-scale-up step for industrial production, where the plant is typically located in a laboratory, so their size is small compared to chemical plants. Such installations are usually managed and supervised by the Principal Investigator (PI), typically a researcher or professor, and the staff is usually represented by PhD and undergraduate students.

There is no single definition of a pilot plant, as they are between research and full-scale process plant production [23]. The definition of the pilot plant in NFPA-45 is "*An experimental assembly of equipment for exploring process variables or for producing semicommercial quantities of materials*" [26]. Regulations for pilot plants are less restrictive than those for full-scale plants because of the smaller quantities of chemicals involved. In full-scale chemical plants, standards and regulations are required to define the minimum distance between pieces of equipment. These standards do not exist for pilot plants, so there can be a high density of operations, which can worsen credible hazardous scenarios [23]. Accidents in pilot plants are usually reported as laboratory accidents, which are discussed in Chapter 1. The causes of these accidents are usually similar to those recorded in a full-scale industrial chemical plant [8].

Compared to an industrial process or a chemical laboratory, a pilot plant may have additional hazardous characteristics, including:

- A not established technology;
- Variability of operating conditions, materials and molecules;
- A high density of equipment and operations;
- A relevant role played by the human factor;
- Different manual operations;
- A lack of procedures or procedures verbally passed on;
- Not continuous supervision of the plant;
- Scale-up from bench scale;
- Second-hand equipment or patchy installations.

The frequency of incidents shows that research institutions are not used to managing risks associated with pilot plants [8]. In this chapter, a brief definition of an experiment will be provided. Then, the hazardous properties will be analyzed to understand how to reduce the associated risks.

2.1 Pilot plant: the concept of experiment

One of the possible ways to define an experiment is as follows: "*a scientific test that is done in order to study what happens and to gain new knowledge*" [27].

The definition of a pilot plant from NFPA-45 as "*an experimental assembly of equipment* [26]" helps us to understand that this type of operation is an experiment. In the scientific world, there are two different approaches to designing an experiment: the scientific method and the engineering method.

The scientific method is based on formulating a thesis, which is analyzed according to a defined procedure to obtain and discuss final results [28]. There is a classification of scientific research based on experiments since they can be of different natures (e.g., observational/experimental, descriptive/analytical, retrospective/prospective/cross-sectional, clinical/laboratory/social descriptive research) [29]. The engineering method can be divided into seven steps, which can be summarized as follows: defining the problem, theoretical study, defining the requirements, developing possible solutions and defining which is the best, developing the prototype, testing, revising the prototype (if necessary), final results [28,30]. From this summary description of the two possible methods, it can be seen that the pilot plants follow the engineering method.

Safety in pilot plants is strictly related to two steps of the engineering method: the development of the prototype and its revision after some tests. The hazardous characteristics mentioned in the previous paragraph can be observed in both steps. As the definition of an experiment states, the aim is "*to gain new knowledge* [27]", which also describes one of the most hazardous characteristics of the pilot plants. As these installations are experimental, most combinations between the operating conditions, the chemicals and the materials involved have never been tested or are poorly recorded in the literature. In addition, these combinations may change during the study, both the operating conditions and the substances, so the "revision" step should include an in-depth analysis of the new combinations or whether the equipment can handle the new conditions or combinations of chemicals and materials.

2.2 Change in operative conditions and technology

It is common in R&D settings to work with different operating conditions. The same experimental infrastructure is sometimes used under different operating conditions ([12]). In research laboratories, deviations in the operating variables, such as temperature and pressure, are usually minor, such as a few temperature units. Significant deviations could be in the form of a different solvent, catalyst, reactive conditions or replaced materials/equipment. This second type of change is too often made without a proper safety analysis [8]. It is essential to underline that the pilot plant equipment is typically unsuitable for all possible operating conditions. Therefore, before any change in operating conditions, materials or equipment is made, a compatibility study is imperative to identify potential new hazards and risks. A small change in temperature or pressure could push side reactions or undesired phenomena, leading to dangerous scenarios. In this regard, the *Management of Change* (MOC) is crucial, as well as implementing robust procedures that should be updated regularly ([8]). Identification of the main variables of the process is crucial to work in a safe condition. If there is a small change, these variables should be enough to keep the process under control. However, the situation can be critical under significant deviations, especially if such deviations have not been appropriately identified and managed. When there is a significant change, a document should be drawn up, including the following details:

- Explanation of the reasons for supporting the intended design modifications;
- Effects on health and safety;
- Adaptation of the operating conditions and compatibility issues;
- Time required for implementing the modifications;
- Authorization process for implementing the modifications.

The full description and recording of the above points will assist in updating the risk assessment. Therefore, The MOC can help reduce the potential for hazardous scenarios [8].

2.3 Equipment used

In a pilot plant, it is essential to have accurate information about the process and the technology used in order to develop a correct risk assessment. The P&ID and information on all equipment should be provided in a preliminary report. If this information is not provided, the risk analysis may be incorrect or deficient due to an inappropriate definition of nodes and deviations [23].

Many documents must be submitted for full-scale chemical plants before the plant is built, but this is not mandatory for pilot plants. Some of the documents required for a full-scale chemical plant are the process design basis, a description of the process, PFDs (process flow diagrams), calculations about mass and energy balances, properties and specifications of the materials involved, list and specifications of the equipment and detailed engineering, P&ID (piping and instrumentation diagram) and risk assessment. Typically, R&D infrastructures are not as well documented but only provide a summary of the plant itself, as operating conditions can change over time. Moreover, whether the documentation is available, it can be out of date. In addition, it is not uncommon to find second-hand equipment in this type of plant. The problem with the latter is that important information, such as construction materials and compatibility data, can be lost over the years. If there is no information on a particular aspect, it is advisable to take a conservative approach and consider the worst-case scenario.

2.4 Scale-up and experimental scale

Pilot plants are the next step after laboratory-scale plants. Usually, the product involved in pilot plants has a significant cost, so data are needed to manage it best. Often, knowledge of this data is limited at this preliminary stage, resulting in a potential lack of safety.

Scale-up requires in-depth knowledge of the process and the various process units, such as the reactor and separation units. This is not always possible, as one of the characteristics of pilot plants is the change in operating conditions. Proper scale-up is essential to understand what the limitations of the process are. It may be that the amount of heat removed at the laboratory scale is not sufficient for the pilot plant because the heat generated is higher than predicted at the smaller scale [5]. This is a typical concern when working with potentially runaway reactions. In this regard, the changes in heat loss behavior with scale are central to scale-up risks. In fact, many reactions are exothermic and require cooling to ensure safe operation when performed on a large scale. In other words, reactions can behave differently at large scale due to changes in heat transfer, reagent addition method, or stirring.

Another example of poor scale-up is an incorrect sizing of the mixer, resulting in segregated zones within the equipment where relevant secondary reactions can occur.

Similar considerations can be made for scale-up from pilot plants to full-scale industrial processes. However, the data available is usually more extensive than that for pilot plant scale-up. The final geometry of the equipment for industrial processes may differ from that studied in the pilot plant to comply with specific regulations [5].

In conclusion, scale-up, related to the management of change and the equipment used, is one of the hazardous aspects of pilot plants.

2.5 Human factor: procedures and manual operations

The R&D infrastructures do not have the same level of automation as a full-scale chemical plant. Many operations are performed manually, such as loading materials during a batch operation or responding to an alarm. Dangerous scenarios could arise from incorrect operations by the current operator, who, under stress, may not know how to manage the different process behaviors. As mentioned in Chapter 1, focused training on the equipment used is crucial to reducing the incidence of hazardous scenarios. Some universities develop SOPs, which are standard operating procedures for the experiment in the laboratory, but also to educate students about safety issues [31].

2.5.1 Standard Operating Procedures (SOPs)

SOPs are protocols related to the handling of chemicals, but they are not sufficient for chemical manipulations. These procedures[1] are usually written with a step-by-step structure to provide a clear protocol to follow. There are many guidelines from different communities on the content of SOPs in the literature. However, no information is given on how to develop this type of document in the context of academic research facilities. If the protocol structure is inadequate and the procedure is unclear, the frequency of undesired scenarios could increase, also pushed by a potential increase of wrong or late human actions [31].

SOPs are one of the pillars of safety, which can be divided into facilities, equipment and procedures. In high-risk industries, 60 to 90% of incidents can be caused or co-caused by human error. In fact, in 2014, the NGAP (next-generation advanced procedures) consortium added the science of human factors and ergonomics as a relevant contribution to reducing the frequency of human errors [31].

A possible structure of a SOP is one focused on the user, called User-Centered Design (UCD). The following six aspects develop this protocol:

1. Define the context of the task and the employer involved in the task;
2. Develop the SOP based on the information reported in the first stage;
3. Definition, through requirements, of the various possible interactions between the SOP and the operator;
4. Develop and test the SOP in order to determine if it meets the requirements defined in step 3;
5. Review and test the SOP to determine if the protocol is effective;
6. Repeat step 5 until the targets are met.

Another common approach is that a Subject Matter Expert (SME) writes the required SOP [31]. Usually, protocols written down by a SME are less detailed than UCDs SOP since the matter expert considers some steps related to the protocol obvious. These procedures are usually intended for trained operators. Their drawback is that a less trained worker could not remember all the steps required for the applied procedure. This can require more attention and a higher concentration level from the operator than a SME. Usually, it is recommended that the person who draws up the SOP write down all the critical steps and not consider some stages as evident. As the final step, the subject matter expert should review the SOP [31]. It should be noted that, in the academic setting, the variety of people acting on the equipment could be significant, ranging from the PIs to the researchers, PhD students and undergraduates. Each actor could have a different degree of knowledge and risk perception.

---

[1] In this paragraph, procedures and protocol are used as synonymous.

2.5.2 Guidelines to write a SOP

In the literature, there are many guidelines for writing procedures. This paragraph[2] discusses only the central elements needed when writing a procedure.

Firstly, a procedure should be written with a step-by-step structure, where long/narrative phrases should be avoided or reduced to a minimum [31].

The steps and information in the protocol should follow a chronological order so that it is easy to understand the order of the steps and the associated hazards. This means the data relating to the chemicals involved must also be placed before the protocol procedure. In addition, the operator must be aware of the equipment used and the precautions to be taken in the event of a hazardous scenario. So, the relevant aspects of the materials involved in the process should be reported at the beginning of the protocol and during the hazardous steps of the process, as it is not obvious that the operator will remember the intrinsic hazards of each substance [31].

The steps required in an SOP may or may not be sequential. Specific procedures do not necessarily have to be carried out sequentially. An SOP should clarify whether a procedure must be carried out sequentially and indicate why the order of the steps is critical. This is especially true when operating discontinuously on an experimental setup or upon modifications to the experimental setup and during transients [31].

A protocol must be clear and direct. To achieve this, the sentences in the procedure should begin with an action, but if there is a conditional state, it must be placed first to show that it is a relevant condition. A clear and direct protocol is one with a simple font and good use of white space. In addition, it is common in protocols to use colors to highlight hazards and special instructions. However, the NGAP studies showed they were not as effective (the results could differ for experienced and new workers) [31].

To help the operators with the protocol, a square could be added for each of the main steps of a particular task. This addition aims to avoid errors caused by distractions, which can be frequent when the procedure is not linear. Unfortunately, it is common practice for workers to do step-by-step reviews of procedures after the task has been completed [31].

In conclusion, SOPs can have different formats but must be clear and direct. Writing at least two different versions of the same protocol is recommended, one detailed and one shorter. These different versions are intended for operators with different levels of experience, as it has been observed that an experienced operator will make mistakes if the procedure has more words than necessary. After their draft, the SOPs must be tested to identify possible mistakes or unclear steps. Testing the SOP must be done by the worker who will work on that protocol without assistance or instructions. When all sensitive parts of the SOP are identified, the protocol must be corrected. It is crucial that all the SOPs have periodic feedback by the user

---

[2] In this paragraph, procedure will not be considered as synonymous with protocol, but as a part of it.

and that these updates and corrections must be done fast always to have an available procedure (§2.5.3) [31].

2.5.3 SOPs format: paper vs. digital

SOPs can be digital or printed on paper. The latter is the most common but can be easily damaged or lost. Updating paper procedures is more labor-intensive than updating digital ones, and the protocols could be unreliable for a period of time. The paper procedure could sit for days or weeks on the desks of people who cannot change it.

Some platforms for procedures have been developed over the years. They can be used instead of paper procedures because tablets and smartphones are as reliable as paper. Digital procedures can be modified more quickly than printed ones, as possible errors or different conditions can be reported directly to the person who decides to change the procedures. Digital procedures also allow different users to work on the same protocol simultaneously. On the other hand, digital SOPs require significant time and money to train people to use them. Another challenge is that there could be some limitations due to the infrastructure available, such as Wi-Fi and stands for phones or tablets. The decision to use digital procedures instead of paper, or vice versa, should be made considering their advantages and disadvantages and whether the procedures are short-term or long-term [31].

Concerning the academic settings, it should be noted that written procedures on paper are usual. One of the main issues is related to the availability of such papers, provided that users can change frequently and time limitation constraints can induce overlooking training upon written procedures. Moreover, statistics on past accidents show that extemporary modifications of procedures or unauthorized customization critically contribute to undesired events.

2.5.4 Manual operations: SOP vs. “Know-How”

Pilot plants and their hazards are usually regulated by OSHA (Occupational Safety and Health Administration) in the USA [32] or by specific committees set up by the European Commission in Europe [33]. Unlike industrial plants, R&D settings are peculiar for many manual operations, which could also be hazardous.

In pilot plants, automated tasks can be performed, but it is not uncommon for some tasks to be performed manually, such as shutting down the plant. Most incidents in pilot plants are due to human error associated with a manual operation.

Academic research infrastructures are associated with innovative experimental conditions, new processes, and equipment, which can lead to hazardous scenarios. Some procedures and protocols are required to respond promptly and efficiently to deviations from the experiment intent. The main problem is that these procedures are not always available, as the necessary steps are given to students and operators as *know-how* by the PI or the supervisor. The same issue arises with frequent tasks such as loading or unloading pieces of equipment or cleaning. As mentioned above, pilot plants are usually not highly automated, and the common tasks are usually related to batch behavior (e.g., activities in §1.2.4 and §1.2.5). Loading and unloading of the equipment may involve very hazardous materials or conditions. It is crucial to know the intrinsic properties of the substances and compatibility issues with materials and operating conditions. However, if the operator (usually undergraduate and graduate students) is poorly trained, it can be challenging to recognize possible hazardous scenarios. The *know-how* instead of written SOPs has many shortcomings. As reported in Table 2.1, even severe consequences are determined when written protocols are not correctly observed.

Table 2.1: *Common mistakes when a written SOP is not in place or observed.*

Common mistakes	Possible consequences
Forget key passages	Reaction: the intended reaction does not occur, whereas side reactions could be promoted. Equipment: if the equipment is not equipped with sensors related to the specific key passage, the equipment cannot manage the intended operative condition.
Incorrect sequence of actions	Reaction: the intended reaction does not occur. Side reactions could be led. Equipment: if the proper sequence for equipment set-up is not followed, the equipment cannot accommodate the required operative conditions. Hazardous scenarios for the operator can also occur with possible injuries.
Incorrect handling of materials	Reaction: side and undesired reactions could be led. Hazardous scenarios for the operator can also occur with possible injuries. Equipment: damage in case an incompatible material comes into contact with the equipment.
Incorrect execution of tasks	Reaction: the wanted reaction could not occur, whereas side and unwanted reactions could be promoted Equipment: the equipment could not be able to accommodate the operative conditions. Hazardous scenarios for the operator can also occur with possible injuries.

Table 2.1 summarizes the possible consequences when the setup is required for a desired task. It can be seen that the main consequences are related to hazardous scenarios due to undesired or side reactions and damage to the equipment. The resulting scenarios can be more or less extensive, and the associated consequences can range from minimal to fatal.

The probability of human error is strictly related to the user training (BS EN 61511-3:2017 [34]). In an academic setting, the operator is usually a student who may react differently to an experienced actor (e.g., a PI or a supervisor). Human error cannot be avoided entirely, even with written SOPs, but predictable errors can be managed through a robust risk assessment.

In conclusion, written SOPs are always preferable to orally communicated *know-how*, but protocol alone is insufficient to operate safe research equipment.

2.6 Desired vs. undesired chemistry

One of the most critical issues in a chemical process is to achieve the ideal operating condition where side reactions and products are known, controlled and minimized. Unfortunately, achieving this ultimate goal is complex, and the operating conditions often compromise the chemistry of the desired product (e.g., reaction mechanism) and all the side reactions. Understanding the characteristics of the reactions involved in the process is essential to prevent possible deviations from the design intent.

The equipment may operate under pressure or vacuum conditions in R&D settings and pilot plants, as in industrial chemical plants. In addition, high-temperature conditions and the production of toxic or flammable materials are common. The equipment is designed to suit the operating conditions. The equipment can usually cope with operating conditions more severe than desired, but if the pressure and temperature exceed specific limits, the equipment could collapse or explode. To avoid these scenarios, knowledge of the kinetics and thermodynamics of the reactions is essential to define the monitoring and control strategy and prevent such scenarios.

2.6.1 Desired chemistry: required knowledge

Parameters in a chemical plant, such as temperature and pressure, are strictly related to the thermodynamics of the system. Therefore, good related knowledge is critical to properly designing the experiment. To identify these ranges, it is necessary to define the heat of the reaction and the rate of pressure generation [35].

The heat of reaction ΔH_R can be estimated from data from databases, handbooks and literature by applying equation 2.1. H_i is the heat of formation of species i, and v_i is defined as the associated stoichiometric coefficients, which are positive for the products and negative for the reactants.

$$\Delta H_R = \sum_i v_i H_i \tag{2.1}$$

The heat of the reaction can also be determined by modelling or by using calorimeters to calculate the enthalpy difference and the adiabatic temperature. The latter is a key parameter used to assess potential consequences when a loss of temperature control occurs or in the case of uncontrolled heat release.

Pressure generation is related to the evolution of gas in the system. It is essential to define this to predict possible pressure increases in the equipment and to control possible gas emissions from the equipment. FTIR (Fourier Transform Infrared) instruments are usually used to determine the gases evolved and their kinetics [35]. GC (gas chromatography) is used instead of FTIR, where hydrogen may be formed. The gas phase composition is also important to avoid explosive/flammable mixtures such as those within the flammability limits [35].

2.6.2 Undesired chemistry

Operative conditions can deviate from the design intent when the equipment is poorly designed to manage the resulting scenarios or does not work. The deviated state can lead to side reactions, which in turn can support the generation of unexpected molecules, even toxic or flammables.

Usually, undesired chemistry is related to a secondary decomposition. As for the primary reaction, secondary reactions require a complete understanding to design the experiment correctly. A DSC (differential scanning calorimeter) and MMC (multiple module calorimeter) are used for screening purposes. The calorimetry can help detect potentially hazardous exotherms once the temperature deviates from the design intent. A minimum number of tests are required to define the heat and the evolved gasses. The calorimeters can detect all the secondary decomposition at high temperatures, even during transient conditions or when the ultimate experimental conditions are still under debate [35].

Different scenarios can be obtained during tests with DSC and MMC:

- small pressure variation and small exothermicity;
- large pressure variation and small exothermicity;
- small pressure variation and large exothermicity;
- large pressure variation and large exothermicity.

The resulting pressure and heat are fundamental in determining the materials and thickness of the equipment to manage the resulting scenarios [35]. No further steps are required if the pressure and exothermicity are small and do not exceed the defined operating pressure thresholds, usually less than the Maximum Allowable Working Pressure (MAWP). This is not true if the pressure or exothermicity is of high magnitude. If the amount of non-condensable gases produced is high, the pressure obtained should be considered a reference point to compare with the MAWP. If the pressure released is not too high, but the exothermicity of the undesired chemistry is high, simulations are required to define the maximum temperature the system can reach, i.e., adiabatic conditions. This result is helpful in understanding if further testing is required and what the safeguards might be to manage the upcoming scenario. In the case of the fourth scenario (large ΔP and large exothermicity), the considerations described for the second and third scenarios should be applied [35].

However, undesirable chemistry also considers side reactions that are not classified as secondary decomposition and can be exothermic or endothermic. Typically, mildly endothermic reactions do not lead to different hazardous scenarios than exothermic ones. If the undesirable chemistry involves equilibrium reactions, we can reduce their impact by the Le Chatelier principle with a small addition of their products or by working with unfavorable operating conditions. If irreversible side reactions are involved, inhibitors compatible with the desired chemistry or operating conditions selective to the main reaction must be used.

Another strategy to assess potential reactivity hazards is to derive the stability diagram from measured calorimetric data. Such a representation helps delimit inherent safe operating regimes to drive a proper experiment design and alarms [36–38].

2.7 High density of equipment

Different equipment in an industrial chemical plant must have a minimum distance between them, which is not mandatory for pilot plants [23].

As reported in Chapter 1, the main scenarios of an incident in a chemical laboratory are related to fires and explosions. The magnitude of these final events is closely related to the substances involved, flammable and explosive properties, and the amount involved. Explosions and fires can develop in many different ways, and their behavior depends on the geometry and distribution of the equipment.

There are several methods for calculating the magnitude of an explosion:

- TNT equivalency model;
- TNO Multi Energy Method (TNO-MEM);
- Baker-Strehlow-Tang (BST) method;
- Computational fluid dynamics.

The first method is based on calculating the equivalent quantity of TNT (trinitro toluene) and is independent of the density of the equipment. Equation 2.2 is the equation required to perform the TNT equivalence method. E_{TNT} is the explosive energy of TNT, which is 4686 kJ/kg, and ΔH_c is the heat released by the combustion of the flammable gas. From equation 2.2 it can be seen that the equivalent quantity of TNT is a function of the reactivity (η) and quantity (m) of the compound [39].

$$m_{TNT} = \frac{\eta m \Delta H_c}{E_{TNT}} \tag{2.2}$$

The second (TNO-MEM) and third (BST) methods are almost equivalent and are based on the density of the obstacle. The results of these methods are obtained from experimental curves, which require the definition of the strength coefficient and the flame speed. The latter is a function of fuel reactivity, flame expansion and obstacle density [39,40].

Table 2.2: *Example of a table to define the Mach number of the flame front as a function of the geometry and the reactivity [40].*

2.5 D Flame Expansion Case		Obstacle Density		
		High	*Medium*	*Low*
Reactivity	*High*	DDT*	DDT*	0.47
	Medium	1.0	0.55	0.29
	Low	0.50	0.35	0.053

* DDT: Deflagration to detonation transition (for this condition, the BST method cannot be used).

Table 2.2 [40] is an example of the table structure used to determine the flame speed for the BST method. For higher obstacle densities, the Mach number increases as the flame speed increases, and the resulting consequences are more severe than those observed for lower obstacle densities [39,40].

A fire can start when the lower flammable limit (LFL) is reached and an ignition source, such as a flame or spark, is present. Each flammable compound has its flammability/explosion limits, which can be found in the literature and the MSDS. The transition from fire to explosion can be observed when the flame of the fire takes into account not only the ignition source but also the entire flammable mixture [41]. The explosion limits depend on the phase and environmental conditions (e.g. pressure, temperature, humidity, etc.) of the flammable substance but may also depend on the equipment involved [41]. An explosion is easier to observe in an area with a high equipment density, as the flame can spread from the ignition source/equipment to nearby equipment.

R&D infrastructures, especially in the academic setting, are usually installed inside a laboratory, and the equipment density is often classified as high. Therefore, the resulting scenarios of an explosion in a pilot plant may be more severe if minimum distance rules are not followed.

2.8 Final aspects

Hazard identification for pilot plants is usually controlled by the standards of the U.S. OSHA Laboratory [11]or other legislation [33].

Many aspects of the R&D settings and pilot plant have been discussed in this chapter. However, the leading causes of chemical laboratory incidents analyzed in Chapter 1 should also be considered hazardous characteristics in a pilot plant. The last essential point for pilot plants is the building in which the plant is installed. It must have a ventilation system and doors that comply with the legislation and the substances used in the experiment [42,43]. In addition, the electrical system must be classified and evaluated [26] to minimize possible hazard scenarios that may arise from electrical materials or uncontrolled ignition sources.

In conclusion, an experiment involving chemical or physical transformations can have inherent hazardous features that require proper risk assessment, operator training and written procedures. Aggravating factors include variable operative conditions, a variety of equipment and materials and tasks performed manually by different actors. The poor knowledge of the chemistry and reactivity during the experiment can contribute to undesired risk scenarios.

Chapter 3

Risk assessment techniques

Many different techniques can be used to develop a risk assessment study. This chapter describes the interaction matrix, the HAZOP and the LOPA analyses. These techniques identify potential hazards and risk scenarios in the process industry. However, in the present work, these techniques are adapted to the case of the pilot plant in the academic setting.

3.1 Hazard evaluation procedures

A complete hazard evaluation is the critical aspect of a successful risk assessment, but it has many limitations, such as completeness, reproducibility, inscrutability, relevance of experience and subjectivity [44]. It means that the experience of the analyst influences the risk assessment, so it is not objective and may be incomplete or difficult to understand.

The risk assessment depends on the objective of the process under consideration and its lifetime. For pilot plants, the objective is usually to investigate toxic waste management and to increase the knowledge of a specific reactive system (e.g., catalyst deactivation and behavior of the reactions involved) [44]. The pilot plants have peculiar features, including prominent manual operations, variable operating conditions, and issues due to documenting and addressing hazards, risks, and procedures.

To address a risk assessment study, different methodologies can be applied, such as:

- Interaction matrix;
- Checklist analysis;
- What-if analysis;
- FMEA (Failure Modes and Effects Analysis);
- HAZOP (Hazard and Operability Analysis);
- LOPA (Layer of Protection Analysis);
- Event tree analysis;
- Fault tree analysis.

While the tree-based techniques are quantitative, the other strategies above are qualitative and used to identify proper scenarios.

Typically, more than one of these techniques provide a robust and exhaustive hazard and risk assessment, including hazard identification methods and hazard assessment techniques based or non-based on scenarios [44].

3.2 Interaction matrix

The interaction matrix is a hazard identification method that analyzes the interaction between different chemicals, materials and operating conditions. The interaction matrix is a 2D matrix where one axis consists of all chemicals, utilities and intermediates involved in the process. In the other axes, all the previously listed chemicals must be indicated, and, in addition, normal and abnormal operating conditions that could lead to a hazardous scenario must be analyzed [44].

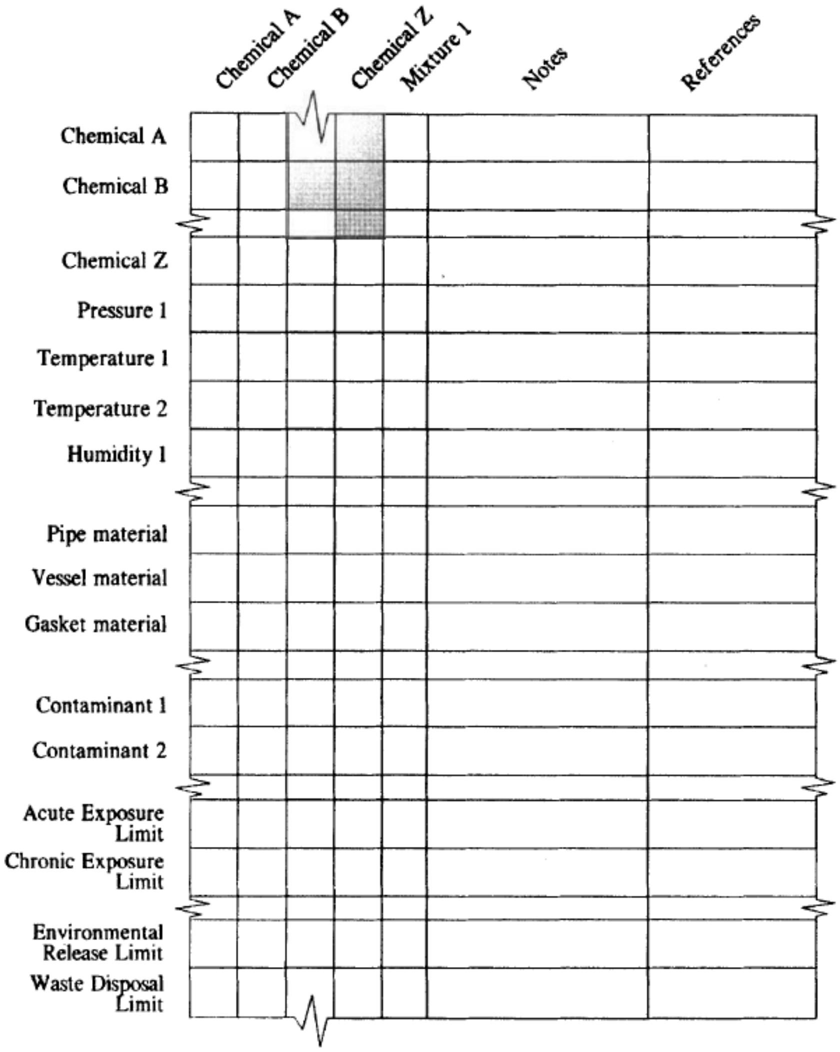


Figure 3.1: *Example of the structure of an interaction matrix [44].*

There are three main methods for determining whether or not the various interactions are compatible: personal knowledge, literature, and appropriate tools [45]. If incompatibilities are observed, the analyst should determine the better way to avoid or minimize them to work under safe conditions [44]. It is possible that the interaction between two chemicals or a chemical and an operating condition may not be reported in the literature. This could occur if the interaction is safe or if this combination has never been studied. The analyst's knowledge is crucial to recognize which of these two cases is being considered. If the interaction studied between two chemicals or between a chemical and an operating condition can be called *new*, a compatibility analysis should be performed, this only if it can be done safely; if this is not possible, the interaction should be avoided. If the interaction under study is between a chemical and a building material, the equipment manufacturer should be consulted.

Peculiar to pilot plants and research and development experimental apparatus is that molecules, materials and operating conditions can change in relation to different experimental campaigns performed. Moreover, variable boundary conditions can lead to new risk scenarios, especially when performing transient operations or modifying the experimental apparatus for research purposes.

3.3 Hazard and Operability Analysis (HAZOP)

The HAZOP analysis is one of the most commonly used techniques to analyze the chemical process and the possible hazards in a systematic way [46]. The main objective of the hazard and operability analysis is to define the risks associated with a specific operation and maintenance of the equipment [47]. In addition, the sources of deviation from the design intent are identified through HAZOP analysis. This technique can also be used to assess written procedures [44].

The HAZOP is usually applied during the review step [46]. Therefore, detailed plant information is necessary to obtain a complete risk assessment of the process. In addition to the process schematic in the form of a P&ID, the manuals for the equipment involved and the logic solvers for the controllers and programs used to manage the process should be provided [44].

The HAZOP study should be reviewed periodically to determine if the analysis needs to be updated with new comments. The analysis must also be reviewed when part of the process is changed to analyze whether new hazards can be observed or an initiating event can no longer occur [47].

3.3.1 Roles during the HAZOP

The HAZOP analysis is performed by a multidisciplinary team [44]. This analysis is usually initiated by a HAZOP leader responsible for governing the HAZOP. The study leader is responsible for many aspects of the study, such as the definition of the study team, the timing of the analysis, communication between the HAZOP team and the manager, and the proper application of the technique [47].

The study leader should identify different roles. In addition to the study leader, the list of possible roles in a team study is as follows:

- Specialists with extensive knowledge of the system. This role has limited participation.

- A designer who knows the design and process representation. Someone who can explain how the node and its systems should behave if a deviation occurs.
- A recorder (the study leader can cover this role). The recorder helps the study director to schedule meetings and manage administrative tasks.
- The user with knowledge of the operating conditions and consequences of a deviation from the design intent.
- Maintainer: someone responsible for the maintenance of the process equipment.

In addition to these roles, other people may be present during the meetings, such as stakeholders and suppliers [47].

3.3.2 Performing the HAZOP analysis

The HAZOP study can be divided into three steps: collecting all the necessary information for the review, performing the analysis, and documenting the results [44]. The study leader usually takes the first step [47] (Figure 3.2).

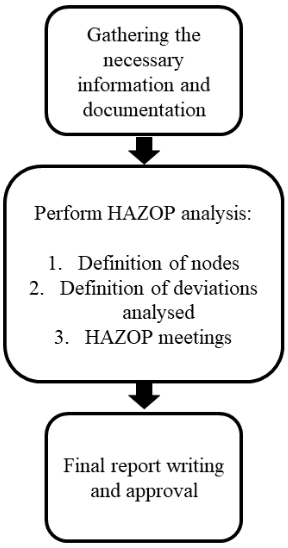


Figure 3.2: *HAZOP procedure*

The third step is also carried out by the study leader with the help of the recorder. The time required to carry out all these steps depends on the complexity of the plant being studied. Small processes may require within 4-12 days to carry out both steps two and three, the first step usually requiring less than 12 hours. On the other hand, complex processes may require more than 12 weeks, as each step requires 2-4 days, 2-6 weeks and 2-6 weeks respectively [44].

A HAZOP analysis is based on the definition of all the deviations from the ideal behavior of the plant (also defined as design intent), where a deviation is composed of a guideword and a parameter (Table 3.1) [46].

Table 3.1: *Example of guidewords, parameters and resulting deviations.*

Guideword	Parameter	Deviation
No	Flow	No Flow
Less	pressure	Less pressure
More	Temperature	More temperature
Reverse	Flow	Reverse flow
Before/After	Mixing	Before/After mixing

The first step of the HAZOP analysis is to divide the process into different nodes. A node is a plant section comprising one or more streams and equipment. Each node is analyzed chronologically [46]. In a node, an operation on a stream or substance is performed.

The analysis report is written, where all considerations about possible risk scenarios and their management must be discussed and recorded. The first step of the technique is the definition of the required guidewords, supervised by the study leader [47]. The HAZOP analysis is then performed.

Each node is analyzed, and the deviations are reported in a worksheet. This worksheet is not unique to all processes, but some common points are usually observed. The worksheet header usually consists of the following elements: title of study, sheet number, date of study, team members, section of plant/node, description of design intent and page number [47]. The table of the worksheet can be composed of the following minimum elements:

- Deviation number;
- Guide word;
- Parameter;
- Material involved;
- Deviation;
- Deviation causes;
- Deviation consequences;
- Presence of specific controls
- Comments;
- Safeguards.

In addition, some other information can be described, such as who defines the specific deviation [47] and the likelihood and severity of the specific deviation.

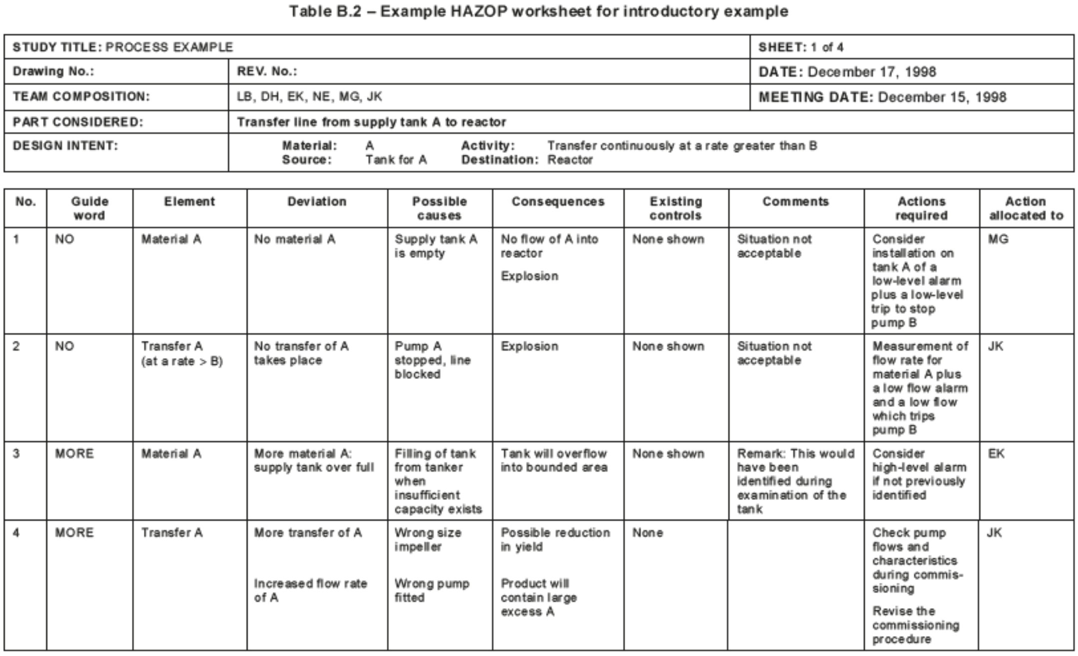


Table B.2 – Example HAZOP worksheet for introductory example

STUDY TITLE: PROCESS EXAMPLE		**SHEET:** 1 of 4
Drawing No.:	**REV. No.:**	**DATE:** December 17, 1998
TEAM COMPOSITION:	LB, DH, EK, NE, MG, JK	**MEETING DATE:** December 15, 1998
PART CONSIDERED:	**Transfer line from supply tank A to reactor**	
DESIGN INTENT:	**Material:** A **Activity:** Transfer continuously at a rate greater than B **Source:** Tank for A **Destination:** Reactor	

No.	Guide word	Element	Deviation	Possible causes	Consequences	Existing controls	Comments	Actions required	Action allocated to
1	NO	Material A	No material A	Supply tank A is empty	No flow of A into reactor Explosion	None shown	Situation not acceptable	Consider installation on tank A of a low-level alarm plus a low-level trip to stop pump B	MG
2	NO	Transfer A (at a rate > B)	No transfer of A takes place	Pump A stopped, line blocked	Explosion	None shown	Situation not acceptable	Measurement of flow rate for material A plus a low flow alarm and a low flow which trips pump B	JK
3	MORE	Material A	More material A: supply tank over full	Filling of tank from tanker when insufficient capacity exists	Tank will overflow into bounded area	None shown	Remark: This would have been identified during examination of the tank	Consider high-level alarm if not previously identified	EK
4	MORE	Transfer A	More transfer of A Increased flow rate of A	Wrong size impeller Wrong pump fitted	Possible reduction in yield Product will contain large excess A	None		Check pump flows and characteristics during commissioning Revise the commissioning procedure	JK

Figure 3.3: *Example of a HAZOP table [47].*

The study ends when all the nodes and their deviations have been analyzed and reported on the specific worksheet. Usually, all the information needed for the final report is given in the HAZOP worksheets. When the final report is written, it is reviewed by all the team members and should then be validated by them. If not all team members agree with the final report, this must be recorded. Then, the study leader and the manager must formally approve and sign off the final documents [47].

3.3.3 HAZOP drawbacks

HAZOP technique is used to study small and large processes. The results obtained from this analysis are related to the knowledge and experience of the study leader and the HAZOP team. There is no guarantee that all deviations and hazardous scenarios will be identified and analyzed. Deviations in one node can lead to consequences in downstream sections, which can not be analyzed when the process is complex. In addition, HAZOP analysis could be limited if only graphical representations are considered. The analysis does not consider actions and operations not reported in P&ID. Finally, when the resulting deviation scenario is too dangerous, the HAZOP study is not enough and other techniques are necessary, such as fault and event tree analysis, to provide quantitive information [47]. These last techniques are graphical models. FTA indicates the frequency of a top event when a system failure occurs.

ETA indicates the frequency of possible scenarios resulting from an initiating event, taking into account the probability of failure of specific layers of protection in the system [44].

In addition, HAZOP analysis requires in-depth knowledge of the process, and this could be a disadvantage when analyzing a pilot plant as all the necessary information may not be available. Another technique should be used, such as what-if analysis or the checklist method [5].

3.4 Functional safety and Layer of Protection Analysis (LOPA)

Many hazardous scenarios can occur in a process, but not all are unacceptable. The risk class must be defined and assigned to assess whether the resulting scenario is acceptable. Risk class is related to the severity of the outcoming scenario and its likelihood [48]. These parameters are studied and managed by functional safety discipline. The main objective of functional safety is to reduce the risk of hazardous scenarios by using safety systems called SIS (Safety Instrumented Systems), which are required to perform safety instrumented functions. (SIFs) [49]. All these systems are applied to obtain a final tolerable risk since zero risk can never be obtained [48]. The concept of tolerable risk is defined by a specific standard (as IEC 61511 [48,49]). It is a function of the severity (classified as *major*, *severe* or *minor*) and of tolerable frequency, which is defined in terms of (undesired) events per year (Table F.8 in [50]). The international standards for functional safety are the IEC 61508 and 61511 [48,49].

The Layer of Protection Analysis (LOPA) is a quantitative method to define the SIL required for a specific initiating event [48]. The list of initiating events is typically produced in a previous hazard identification step, e.g., using a HAZOP analysis.

3.4.1 Definitions

Many different definitions must be known in order to describe functional safety. The following definitions refer to safety systems within the functional safety framework:

- SIS: it is a safety instrumented system used to execute a safety function SIF [49].
- SIL: it is a safety integrity level that can be classified from 1 to 4. The level is assigned to the SIF in order to specify the SIS integrity requirement [49]. In essence, each order of magnitude of risk reduction that is required correlates with an increase in SIL, up to a maximum of SIL 4.
- SIF: it is a safety instrumented function performed by an SIS [49].
- IPL: it is an independent protection layer. The main objective of a protective layer is to decrease the likelihood of an undesired event. The protective layer has to be specific, auditable, independent, and reliable [34,48]. If at least one of these criteria is not met, it cannot be intended as an IPL.
- Safety interlock: it is a subclass of SISs. It consists of a SIF that protects against one or more specified harmful scenarios [48].

- BPCS: it is a basic process control system used to control and guide the response of the system. Usually, the final control element is a pneumatic, electronic or electrical system or a PES (Programmable Electronic System) [51].
- *MooN* (logic): it is an SIS composed of *N* independent detectors, with a minimum of *M* channels required to initiate the SIF operation [49]. This system is usually used when a redundant system is applied. It can have different configurations [48,52].

In addition, other definitions are used to define how much the safety system is reliable and terms related to LOPA, such as:

- ALARP: it is the acronym for *As Low As Reasonably Practicable,* and it is useful to define when a risk is tolerable or not [48].
- PFD: it is the probability of failure on demand [48,49,51]. It is a value that indicates the reliability of the equipment used, so the probability that the safety system does not respond when the hazardous scenario occurs [52]. It can also be given as PFD_{avg}, which is the average over the life of the SIF [48].
- MTTF: it is the mean time to failure [48]. It is a value that indicates the reliability of the equipment used.
- RRF: it is the risk reduction factor [48,52].
- UEF: unmitigated event frequency (UEL in [48]).

These definitions will be useful in understanding the LOPA analysis in Chapter 4.

3.4.2 The procedure of LOPA

The LOPA analysis is a quantitative method to define the SIL required to obtain a final frequency equal to or less tolerable [48].

Figure 3.4 shows the conventional procedure for carrying out a LOPA analysis. An H&RA carries out the first step, usually the HAZOP analysis [50]. When an initiating event is identified, its frequency should be defined by different available data in the literature [48]. Example data can be retrieved in [51] and [53]. The IPLs present must then be identified. These protective systems must have the four characteristics listed in §3.4.1, and the PFD is usually provided in the literature or by the manufacturer [51]. *Conditional modifiers* (Table 5.23 in [48]) are conditions, such as the ignition of a chemical with a low flash point, that should be considered to adjust the final frequency of the scenario [48].

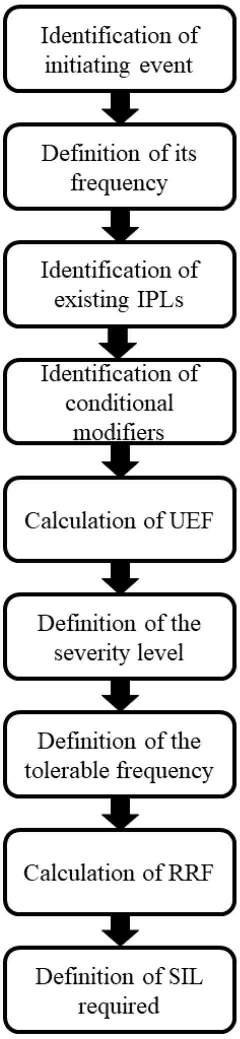


Figure 3.4: *Structured procedure of LOPA (adjusted from [48]).*

The UEF is defined by knowing the frequency of the initiating event. If there are IPLs, the initial frequency is multiplied by the different PFDs of the IPLs present and the final frequency is defined as the UEF. If no IPLs are present, the UEF is equal to the frequency of the initiating event. The definition of the severity class (Table C.2 in [34]) and of the tolerable frequency is crucial to obtaining the value of the desired RRF and, consequently, the required SIL according to Eq. (3.1) ([48]).

$$RRF = \frac{UEF}{Tolerable\ frequency} \tag{3.1}$$

Tolerable frequency is a function of the final scenario severity (Table F.8 in [50]). Different tables can be consulted [5,8] to define the SIL required, as reported in Table 3.2 and Table 3.3.

Table 3.2: *Allocation of the SIL as a function of likelihood and severity of a hazardous event and existing protection layers (adapted from* [50]*).*

N. of existing PLs	**Required SIL**								
3								**1**	**1**
2			**1**		**1**	**2**	**1**	**2**	**3**
1		**1**	**2**	**1**	**2**	**3**	**3**	**3**	**3**
Hazardous event likelihood	Low	Medium	High	Low	Medium	High	Low	Medium	High
	Minor			***Serious***			***Extensive***		
Hazardous event severity rating									

Table 3.3: *SIL targets expressed in terms of risk reduction factor (RRF) (adapted from* [48]*).*

SIL target	**Risk reduction factor (RRF)**
No SIF [3]	UEF ≤ tolerable frequency
SIL '*a*' [4]	RRF ≤ 10
SIL 1	10 < RRF ≤ 100
SIL 2	100 < RRF ≤ 1000
SIL 3	1000 < RRF ≤ 10000
SIL 4	10000 < RRF ≤ 100000

To determine if the SIL complies with the IEC 61511, Tables 4 and 5 of Ref. [49] have to be consulted. Once the required SIL has been determined, an appropriate IPL must be selected to reduce the final frequency of the event. If the IPL does not provide the same RRF indicated by the SIL classification, more than one IPL should be applied to achieve the required final risk reduction [49]. The risk reduction can be the required or the actual risk reduction. The required risk reduction is the one specified to achieve the tolerable frequency. The actual risk reduction is the one that gives a final frequency lower than the tolerable frequency, taking into account all possible layers of protection [34].

The LOPA analysis for the specific initiating event is terminated if the frequency of the hazard scenario is less than tolerable.

3.4.3 Limitations of LOPA

As HAZOP analysis, LOPA analysis presents some limitations [51]. These limitations are related to the fact that the LOPA technique must be used with an identification tool and is more time-consuming than qualitative methods such as HAZOP and what-if analysis [44]. Another limitation is the definition of the risk class. There are guidelines for defining the severity class of hazardous scenarios (Table C.2 in [34]). However, the experience and the interpretation of

---

[3] Table 5.13-5.14 in [48].

[4] The safety function does not need to be a SIF and need not comply with IEC 61508 and 61511 (Table 5.13 in [48]).

the analyst are crucial to obtaining robust and correct results. In addition, two PFD values for a particular IPL may not be the same because the IPL manufacturer may be different, or the data may not be from the same reference. So, the same LOPA analysis performed by two analysts could be different [44].

3.4.4 Human factor

In LOPA techniques, the human factor can be considered an IPL, but it has some limitations [48]. Human error is a possible initiating event in the LOPA and HAZOP analysis. The frequency of this type of event depends on how often the task is to be performed [34,51].

Table 3.4: *The initiating event frequency (IEF) for a task performed by an operator* [51].

Frequency of the task	IEF (yr^{-1})
Once per week (or more often)	1
Once per month (or more often)	0.1
Less than once per month	0.01

When the studied initiating event is due to a human operation, the human response from an alarm cannot be considered as an IPL [48].

The operator response to an alarm can be considered an independent layer of protection when two conditions are present. Firstly, the triggering event is not due to human error. Second, the triggering event is not due to a failure of the alarm system. In addition, several other conditions are required to define the operator response to an alarm as an IPL. One of these additional conditions is that the plant must be continuously monitored to respond to the specific alarm with sufficient time. The task required of the operator must not place the worker in a hazardous situation. If equipment shutdown is required, the operation should be autonomous from any other SIF that is shutting down the same equipment [48].

Figure 3.5 is helpful in understanding when an operator response may or may not be considered an IPL (this is also true for other types of possible IPLs). The alarm starts when the MSP is reached. If the operator's response is not faster than the time indicated as IRT, it cannot be considered an IPL. The process does not react immediately to the operator's corrective action but requires a certain amount of time. IRT is the time available to correct the process parameter because if it is not corrected within this time, it will exceed the *Never Exceed* value. PLT is the time the process requires to change the trend of the process parameter to return to “normal” operative conditions [48,51].

The effectiveness of the operator response depends on the level of experience of the operator itself [34]. An operator can be considered as an IPL only if he is trained. In addition, if the task is carried out once a day or once a week, the MTTF can be reduced from 1 per year to 1 per 10 years, depending on the operator's experience (Table G.3 in [34]).

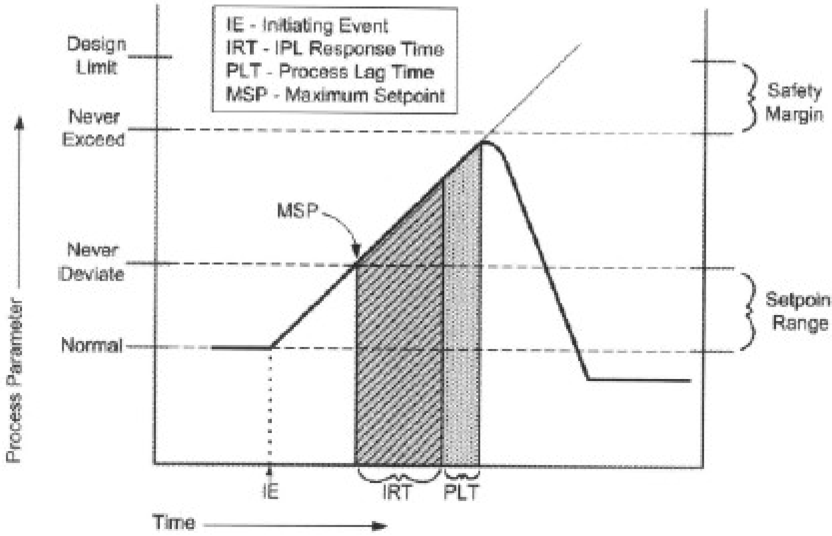


Figure 3.5: *Trend of the process parameter when the initiating event occurs (Figure 3.1 in [51]).*

In conclusion, the human factor is closely related to the plant's safety, as it can be fundamental to the execution of some key safety procedures. However, it can also be the initiating event of hazardous scenarios. Training the operator is the only way to observe more advantages than disadvantages of a human operation. This holds, especially in manual operations-rich settings where the operator is frequently asked to act on the equipment or procedures partially or totally rely on human actions. Academic research settings and related research infrastructures can be characterized by non-automatized contexts where the PI, researchers or students can be frequently asked to perform manual tasks. Moreover, routine and safety procedures can include relevant manual steps whose success strongly correlates with training and knowledge. Frequent manual operations and a framework with limited automatic supervision safety systems can lead to frequent and even severe undesired scenarios caused or concurrently caused by human error.

3.4.5 Equipment for pressure relief

One of the most common IPLs when the internal pressure of equipment increases or decreases are pressure relief devices, such as rupture disks, relief valves and vacuum breakers [51]. Pressure devices are useful to prevent the consequences of high or low pressures in the pilot plant. If a pressure increase is suffered, the consequences can include rupture, leakage, exposure to toxic or flammable substances, explosion and impact on a human target. This last consequence is usually due to an explosion, exposure to hazardous chemicals or fragment projections in the case of loss of equipment integrity. If the pressure is too low, especially when associated with vacuum conditions, the consequences could be the collapse of the equipment with possible ruptures, leaks and loss of containment. Sometimes, reverse flow is also a credible consequence determining contact between incompatible materials or uncontrolled flow to undesired locations. These two opposite behaviours result in hazardous scenarios that should be avoided. In addition, if one part of the system operates at low pressure and another is expected to operate at high pressure, a check valve (PFD = 0.1 [48]) should be added to prevent reverse flow [51].

The effectiveness of pressure relief systems depends on their sizing and fouling [48]. If a pressure relief device is to function as an IPL, it must be sized for the expected discharge scenario (API 520 [54,55]). It should be independent of other devices in the plant section under consideration. In addition, the material of the safety devices must be compatible with the chemicals involved, and the release of the substances must not result in hazardous conditions such as explosive and flammable mixtures in the atmosphere [48,51]. In this regard, the R&D setting can pose issues since the exact nature and composition of the stream can be unknown, especially when innovative experimental campaigns are performed or deviated process conditions are established, pushing side or unknown reactions.

The PFD of pressure relief devices can be considered between 0.1 and 0.01, depending on the number of devices installed. If more devices are required to manage the resultant scenario, the final PFD will have to be calculated with reference to the layout of the devices. Typically, a good PFD approximation when more than one pressure relief device is present is to consider the PFD equal to 0.1 [48,51].

3.4.6 Control loop, BPCS and safety interlock

The primary safety systems for a chemical plant are a control loop, BPCS and safety interlock. BPCS are basic process control systems; their definition is given in §3.4.1. BPCSs have previously been used as a synonym for control loop as they apply a defined control function. This safety system can apply its corrective action automatically or by operator action. This system comprises three components: an initiator, a control system embedding the SIF, and an actuator. The initiator measures the operating condition and sends a corresponding signal to the control system, which applies a corrective action only if the incoming signal indicates an abnormal condition. The corrective action is performed by an electrical or pneumatical system [51].

The control loops can be installed to obtain the best product quality and maintain safe working conditions in the plant. The control loop related to safety conditions can work continuously or in demand mode. The control loop is a subclass of the BPCS and can be classified as an IPL if it is independent of other BPCSs and the cause of the initiating event [48,51].

Interlocks are safety systems, such as BPCS interlocks, whose corrective action is to shut down a specific piece of equipment. Safety interlocks can have one or more SIFs, as different initiating events can activate them. The importance of the different SIFs could be related to the resulting hazardous scenario of the corresponding initiating event [48].

All these systems can be considered IPLs if they comply with IEC 61511 and the time required for the corrective action is so short that it does not lead to a hazardous scenario. All their PFDs are equal to 0.1 [48].

3.4.7 MooN structure

One of the strategies to improve the reliability of safety systems is based on a *MooN* structure. *MooN* systems consist of *N* detectors in contact with the desired SIF. If at least *M* detectors fail, the SIF is activated, and the safety function is initiated. Not all systems have the same target or the same PFD. Some examples are given in Table 3.5 [48,49,52].

Table 3.5: *Examples of MooN structures: objectives and PFDs (derived from Appendix F of [10]).*

Redundant architecture	Objective	PFD
1oo1	Base unit	0.001
1oo2	High-level of Safety	0.00002
2oo2	Maintaining output	0.002
2oo3	Safety and Availability	0.00007

The structure of these systems can vary according to the number of detectors and initiators required, but not all of them have the same weight in the final operation. Some sensors are more important than others because of their position. Therefore, when defining the *MooN* structure, the analyst must also consider the position and importance of the different initiators [48].

3.4.8 Ventilation system: Hood

The ventilation system is one of the most critical layers of protection in a chemical laboratory and pilot plant (Chapter 1). Ventilation systems can be classified according to their operating principle:

- Continuous ventilation systems can be divided into two sub-classes: those without performance monitoring (PFD = 0.1) and those with performance monitoring (PFD = 0.01).
- Discontinuous ventilation system: emergency ventilation triggered by safety controls, alarms and interlocks, known as SCAI (PFD = 0.1).

The difference between the first and second ventilation systems is the ability to define the hood performance. The system measuring the hood's performance helps determine whether the ventilation system works properly. A hood with such a system is connected to a safety interlock or an alarm to prevent dangerous scenarios and not put the operators at risk. SCAI, considered a BPCS, is a discontinuous ventilation system connected to toxic or combustible gas detectors. When the detection system detects at least one of the hazardous gases, the ventilation system is activated to reduce the gas concentration below the safety limit. These systems may be unreliable during a power failure unless provided with a backup utility supply [51].

In R&D settings and academic laboratories, a hood is typically present in chemical or biological laboratories and used when operations occur. It is pretty always continuous and typically without performance monitoring, while discontinuous safety ventilation (SCAI) is rare.

3.4.9 Useful IPLs: AutoStart of standby equipment and Backup utility supplies

If a power failure occurs and the existing protective layers are not sufficient to reduce the frequency of the scenario, two possible IPLs can contribute to the required risk reduction target:

- Automatic start of standby equipment (such as a standby generator or standby pumps);
- Backup utility supplies.

These two systems are used for voltage drop and other scenarios such as utility loss or equipment inefficiency. Certain conditions must be met for the AutoStart system to work as expected. Firstly, the equipment must be maintained in the conditions required to operate as expected and in automatic mode. The standby equipment starts working when the specific signal is received. Some examples of this type of signal are an increase in voltage and high or low pressure. When all these conditions are present, the system can be considered an IPL [48].

The second IPL is a backup utility supply usually associated with a LESS deviation, such as a decrease in voltage or less flow rate of a utility stream. It can be considered independent if activated autonomously and not by operator action, i.e., manual activation is not contemplated. In addition, this system must be able to manage the scenario, and the time required to be online is short enough and less than the IRT (Figure 3.3). The PFDs of these two IPLs are equal to 0.1 [48].

Chapter 4

Case study: the Fischer-Tropsch synthesis

This chapter discusses the risk assessment of the Fischer-Tropsch (FT) pilot plant for research installed at the Università degli Studi di Milano, Italy. The main objective of this plant is to study the production and composition of liquid fuels obtained from hydrogen and carbon monoxide or carbon dioxide via FT synthesis. The P&ID and detailed information on the equipment used and the operating conditions are given in the Appendix (§A.1-5).

The chapter begins with a brief introduction to FT synthesis, followed by a description of the pilot plant and a discussion of the results obtained from the three different techniques used, namely the interaction matrix, the HAZOP and the LOPA analysis. These techniques have been illustrated in Chapter 3.

4.1 The Fischer-Tropsch synthesis

The goal of the Fischer-Tropsch process is to obtain liquid fuels by the combination of hydrogen and carbon monoxide or carbon dioxide (syngas). Syngas can be available by different processes, which come from biomass, wood and lignocellulosic materials. In the early 1900s, Sabatier and Senderens obtained methane from hydrogen and carbon monoxide in the presence of a nickel catalyst [56]. However, FT synthesis takes its name from two German researchers who studied it in the first half of the 1920s. The initial process required high-pressure conditions, but later, the synthesis was further developed in order to also work with mild pressure. Initially, the process was used by countries with difficult access to crude oil. Natural gas and biomass can be used as suitable raw materials for the production of syngas [56,57].

The FT process can involve a first section to produce syngas from available raw materials, followed by the synthesis section and fractionation.

The reactions involved in the process are reported below (R.1-5):

$$n\,CO + (2n+1)\,H_2 \rightarrow C_nH_{2n+2} + n\,H_2O \qquad \Delta H^{\circ}_{298} < 0 \qquad \text{(R. 1)}$$

$$n\,CO + 2n\,H_2 \rightarrow C_nH_{2n} + n\,H_2O \qquad \Delta H^{\circ}_{298} < 0 \qquad \text{(R. 2)}$$

$$CO + H_2O \rightleftharpoons CO_2 + H_2 \qquad \Delta H^{\circ}_{298} = -41\ kJ/mol \qquad \text{(R. 3)}$$

$$n\,CO + 2n\,H_2 \rightarrow H(CH_2)_nOH + (n-1)\,H_2O \qquad \Delta H^{\circ}_{298} < 0 \qquad \text{(R. 4)}$$

$$2\,CO \rightarrow C + CO_2 \qquad \Delta H^{\circ}_{298} = -172\ kJ/mol \qquad \text{(R. 5)}$$

R.1 and R.2 are the main reactions of the process and are exothermic. In contrast, R.3-5 are side reactions of the process [57]. The plant can have different designs depending on the equipment and catalyst used. FT synthesis is usually carried out with an iron or cobalt-based catalyst, but other metals, such as nickel and ruthenium, can also be used as catalysts [56].

Iron and cobalt require different operating conditions, and their use depends on the raw material of the synthesis gas. When coal is used, an iron-based catalyst is preferred, which is different when natural gas is the available feedstock. The pressure range of the reactor is between 15 and 30-50 bar, depending on the type of reactor used. The temperatures required by the process are usually in the range of 200-350°C, but the plant with a cobalt-based catalyst operates at a lower temperature (200-240°C) than the one with an iron-based catalyst. On the contrary, the ratio of hydrogen to carbon monoxide is higher. The final composition is also different, as the activity of the catalyst is lower for the iron-based catalyst. When a cobalt-based catalyst is used, the composition of the final mixture is made up of a higher proportion of diesel and waxes than when an iron-based catalyst is used [56,57].

Different technologies for the reactor are available, including the slurry-phase reactor, the multitubular fixed bed reactor, the fixed fluidized bed reactor and the circulating fluidized bed reactor. The efficiency of these reactors is based on the capability of cooling the system to remove the heat generated by the reactions involved, which are exothermic. If the temperature is too low compared to the design intent (< 200°C), the product mixture becomes more viscous, hindering the desired target. On the contrary, if it is too high (> 350°C), carbon deposition on the catalyst and deactivation of the latter is expected. The deactivation of the catalyst cannot be avoided, so at a certain point in time, the catalyst should be replaced or regenerated with hydrogen in accordance with R.6 [57].

$$C + 2\,H_2 \rightarrow CH_4 \qquad \Delta H°_{298} = -75\ kJ/mol \qquad \text{(R. 6)}$$

The replacement or the regeneration of the catalyst depends on the reactor used [56,57].

In conclusion, the product composition of an FT synthesis depends on the following:

- The catalyst;
- The reactor;
- The operative conditions, i.e. the temperature and pressure;
- The efficiency of the cooling system.

The combination of these components should, therefore, be the one that gives the desired final composition of the product mix, which will be composed of methane, short-chain (C_2-C_4) alkanes and alkenes; long-chain products such as gasoline, diesel and waxes (C_{19+}); by-products as oxygen compounds [57].

4.2 Description of the FT pilot plant

The pilot plant considered in this study is shown in Figure 4.1 and is located in an academic laboratory. All the pieces of the equipment are under a fume hood, but others are not, i.e. T-01 to T-04 and valves 1-5, which are located in a separate room.

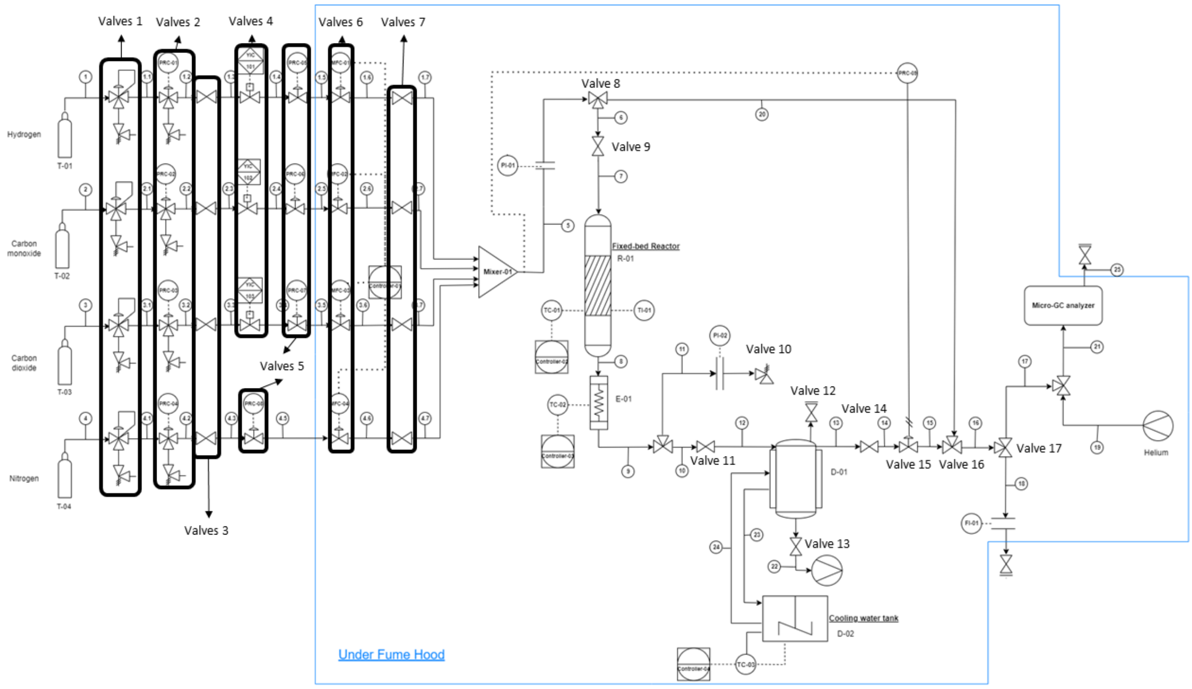


Figure 4.1: *Instrumented process flow diagram of the pilot plant for Fischer-Tropsch synthesis (see §A.1 for a full page view)*

The equipment is usually run by one or two people (PhD and undergraduate students) under the supervision of a PI or professor. As discussed in Chapters 1 and 2, pilot plants can have several intrinsically hazardous properties. In the plant under consideration, these properties are:

- Chemicals involved, which are toxic and flammable (§A.5, §A.8);
- Manual operations (e.g.; start-up and shut-down, §A.4);
- Second-hand equipment (§A.2-3);
- No written procedures available for the entirety of the operations performed;
- Variability in operating conditions which depend on the experimental campaign performed (e.g., temperature, pressure, composition of reactant mixture and catalyst);
- Series of valves (see §A.2, discussed later).

Different precautions should be taken to manage these properties. As the chemicals involved are both toxic and flammable, in-depth knowledge is required to manage these substances safely (§A.8). In addition, a compatibility analysis between the chemicals and the materials involved is essential (§4.3, §A.6-7) in order to avoid dangerous scenarios such as irreversible damage to the equipment. Unfortunately, this is not always possible because the equipment used is "second-hand", and the technical specifications may no longer be available or may be altered.

This compatibility analysis should also be carried out between the different chemicals and operating conditions, as discussed in §3.2. It should be noted that the valves' series could lead to abnormal pressure conditions since if one of them fails, the pressure in the downstream sections will be modified, and different consequences can be led (see §A.9 to understand which are the main consequences).

One of the most critical aspects of the pilot plant under consideration is the lack of written procedures that could affect good operator performance in manual operations. The most common manual operations required for this pilot plant are:

- Start-up (see Table A.4.2 in §A.4);
- Shut-down (see Table A.4.2 in §A.4);
- Cleaning of R-01 and D-01.

The start-up and shut-down procedures of the system require the manual setting of the PRC-09 and various controllers (Controllers -01 and -02). In addition, during start-up, the operator must close the shut-off valves (valves 7) in order to open and clean R-01 and D-01. Typically, the operator carries out the cleaning of R-01 and D-01 autonomously, as well as the start-up and shut-down operations. The frequency of these operations is the main problem of the pilot plant since the probability of a human error for a task performed once a week is equal to 1 time a year [51]. The consequences of possible mistakes in these procedures are analyzed and discussed in §4.4 and §4.5.

4.3 Interaction matrix

The interaction matrix is helpful in identifying hazardous situations due to incompatibilities between chemicals, materials and operating conditions (normal and abnormal). In this study, the interaction matrix was divided into two different matrices:

- Chemicals vs. Materials;
- Interaction matrix without materials.

Therefore, the compatibility is assessed not only among chemicals but also with construction materials of the experimental setup.

4.3.1 Compatibility between Chemicals and Materials

Table A.6.1 (§A.6) and Table 4.1 show the interaction matrix between chemicals and materials. The materials considered are those of the leading equipment such as pipes, valves, seals, gaskets, M-01, R-01, E-01, D-01, pressure and flow indicators.

Two standards are used to analyze the compatibility between gases and equipment materials: EN ISO 11114-1:2020 [58] and EN ISO 11114-2:2021 [59]. The remaining interactions have been analyzed from other sources [60][61][62].

Table 4.1: *Compatibility between chemicals and materials (white: not found; green: compatible; red: incompatible; orange: could be incompatible). Further details are provided in Table A.6.1.*

	SS316	SS304	Brass	PCTFE	Elastomer	PTFE	FKM	BunaN	Aluminum	Glass
H_2	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	
CO	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	
CO_2	🟩	🟩	🟩	🟩	🟧	🟩	🟥	🟥	🟩	
N_2	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	
SiO_2										
Mineral wool										
Catalyst										
Water	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
CFC	🟩	🟩	🟩	🟩	🟧	🟩	🟩	🟩	🟩	
He	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	
Acetone	🟩	🟩	🟩	🟩 **T < 37°C**	🟧	🟩	🟥	🟥	🟩	🟩
C_7-C_{30}	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
C_2-C_6	🟩	🟩	🟩	🟩	🟧	🟩	🟩	🟩	🟩	🟩
Incondensable gases	🟩	🟩	🟩	🟩	🟧	🟩	🟥	🟥	🟩	
Oxygen compounds	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩

Table A.6.1 and Table 4.1 show that elastomer materials could not be compatible with different chemicals, depending on the elastomeric material. To avoid this margin of error, it is necessary to consult the manufacturer to know the material in question and its compatibility. In addition, FKM (fluorinated elastomers) and Buna N (nitrile rubber) should be avoided since they are incompatible with carbon dioxide.

4.3.2 Compatibility among Chemicals

Table A.7.1 (§A.7) analyses the compatibility between the different chemicals, but also the compatibility between chemicals, environment, and deviated operating conditions, such as:

- Very high (MORE) temperature;
- Very high (MORE) pressure.

The incompatibilities are due to the presence of flammable gases, pyrophoric catalysts and the formation of corrosive materials. Altered process conditions leading to undesired temperature values can provide additional risk scenarios mainly related to the ignition of flammable mixtures and the effect on the flammability limits. Moreover, the pressure affects the flammability limits as well, enlarging the potential flammable range. The correct management of the substances and setting proper operating conditions to ensure an experimental run out of the flammability limits is fundamental to avoid incompatibilities and hazardous consequences [63,64].

4.4 Hazard and Operability Analysis (HAZOP)

To develop the HAZOP analysis, the pilot plant has been divided into four nodes, which are shown in Figure 4.2.

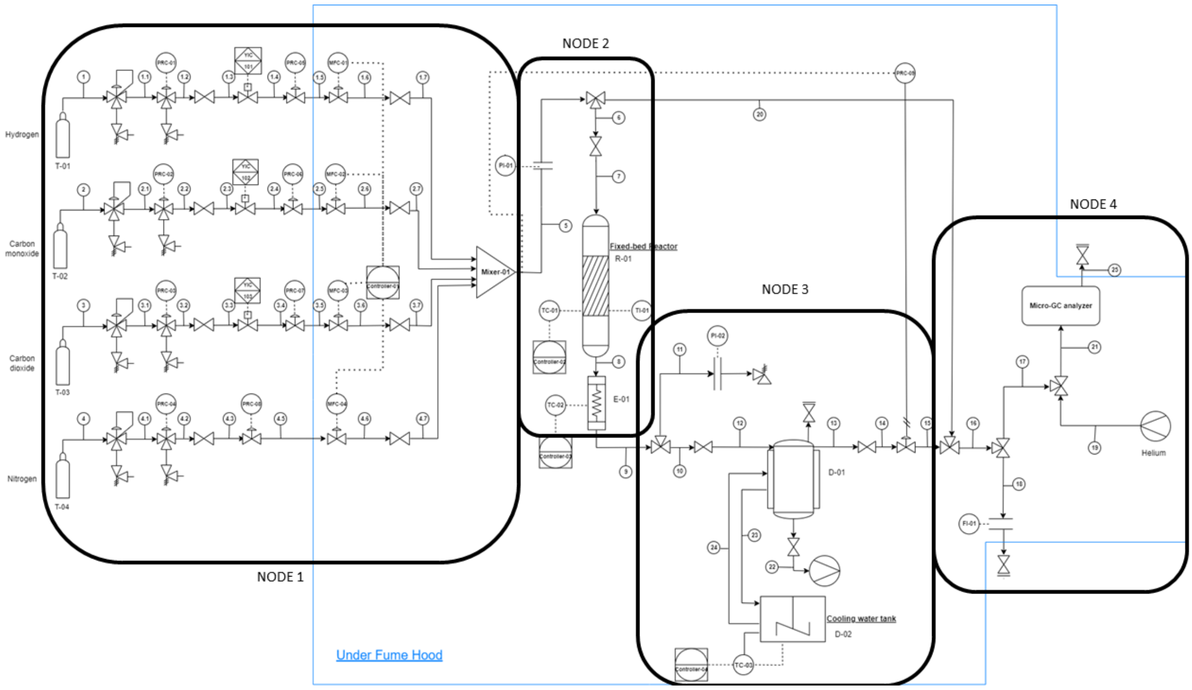


Figure 4.2: *Definition of the four nodes for the HAZOP analysis.*

The different sections have different objectives, which can be summarized as follows:

- Node 1: Feeding section, where four feeding lines are mixed.
- Node 2: Reaction section, where the synthesis occurs in a dedicated reactor.
- Node 3: Separation section, where the products are separated from the mixture.
- Node 4: Gas phase analysis, where the quality of the products is assessed.

Once the nodes have been defined, the deviations to be analyzed along the HAZOP have been defined (Tables A.9.1-2). The plant runs continuously for five days per week, and it is stopped for cleaning and emptying operations on R-01 and D-01. The frequent start-ups and shut-downs require a HAZOP study with respect to both continuous and transient states of the process. The transient analysis is limited to the procedure regarding the start-up and shutdown of the process. Table A.9.1 shows the deviations studied when the plant is operating as a continuous process. On the other hand, Table A.9.2 shows the deviations that an incorrect start-up or shut-down of the plant can cause.

Deviations with a high-risk classification (i.e. risk classes A, B, C) are listed in Table 4.2. They are further discussed and analyzed in §4.5.

Table 4.2: *Main hazardous events emerged from the HAZOP analysis (L: likelihood; S: severity; R.C.: risk class).*

Node	Initiating event	Characteristics of the basic event	Deviation	S	L	RC
1	Set a wrong set point in at least one of MFC-01/02/03/04	Human error	MORE pressure or flow rate	E3	W4	C
	A power outage	System failure	NO/LESS electric voltage-current	E3	W4	C
2	Wrong value at PI-01	System failure	MORE pressure	E3	W4	C
	Reactor too packed	Human error	MORE pressure	E3	W4	C
	Wrong set point in PRC-09	Human error	MORE pressure or flow rate	E3	W4	C
	Wrong set point in TC-01	Human error	MORE temperature/reaction rate	E3	W4	C
	Wrong set point of temperature (start-up)	Human error	MORE temperature	E3	W4	C
	Leakage/defective connection	System failure	LESS pressure, LESS/NO flow	E4	W3	C
	Reactor opening before closing the feed line(s)	Human error	TOO EARLY opening of the reactor	E3	W4	C
	Reactor closing after opening the feed line(s)	Human error	TOO LATE closing of the reactor	E3	W4	C
	A power outage	System failure	LESS/NO electric current/voltage	E3	W4	C
	Catalyst poisoning (not required)	System failure/human error	LESS/NO reaction rate or catalytic activity	E4	W3	C
3	Wrong set point in PRC-09	Human error	MORE pressure or flow	E3	W4	C
	PI-02 failure	System failure	MORE pressure	E3	W4	C
	Power outage	System failure	LESS/NO electric voltage	E3	W4	C

Table 4.3: *Example of a HAZOP table based on the deviation MORE flow rate in Node 1 (feed section).*

Deviation name: Increasing Flow

Node description (design intent): feeding of reactants and mixing to the desired composition (which could change depending on the experimental test performed).

Cause	Consequence	Safeguards	Recommendations	S	L	RC
1.Wrong set point at the mass flow controller	Potential increase in pressure [5] and changes in the final composition with loss of the experimental test.	Hood. Sensor for leakages. Sensors for pressure. Alarmed high-pressure sensor (PIAH).	Periodic check of the set-point of the mass flow controller. Proper procedures.	E2/E3	W4	**D/C**
2.…						

---

[5] Refer to the associated deviation MORE pressure in the HAZOP analysis.

All HAZOP deviations analyzed are reported in §A.9, and the structure of the tables is the same as of Table 4.3. The definitions of severity (S), likelihood (L) and risk class (R) are reported in Tables 4.4-7.

Table 4.4: *Classification of severity (S) for evaluating the risk R of a scenario.*

Severity class (S)	Description
E1	**NOTICEABLE** People: Recoverable injuries for which FIRST AID is necessary. No sick leave. Environment: No significant environmental damage.
E2	**GREAT** People: Recoverable injuries with sick leave. Environment: Environmental damage without lasting effects.
E3	**SERIOUS** People: Irreparable injuries involving one individual. Possibly minor release of hazardous material. However, the effects on people manifest only in the place where the calamity occurs. Environment: There is a significant release of a dangerous product, environmental damage noticeable in the immediate surroundings of the calamity, with possible permanent local effects.
E4	**VERY SERIOUS** People: Irreparable injuries for multiple individuals within the plant. Possibly significant release of hazardous product. However, the effects on individuals manifest only within the plant. Environment: There is a significant release of hazardous material and environmental damage in the wide surroundings of the calamity within the plant, with possible permanent local effects within the plant.
E5	**CATASTROPHIC** People: Irreparable injuries for multiple individuals within the plant. Possibly significant release of a hazardous material. Effects on individuals may also manifest outside the plant. Environment: There is a significant release of hazardous material and environmental damage in the surrounding area outside the plant, with potential permanent effects outside the plant.

Table 4.5: *Classification of likelihood (L) for evaluating the risk R of a scenario.*

Likelihood class (L)	Description
W1	**UNLIKELY** Since the start of the exploitation of the installation, a record of all accidents was kept in an incident-accident system. As no accidents have occurred in the last 20 years, it seems unlikely that an accident will occur during the further exploitation of this installation.
W2	**RARE** This cause is unlikely but not excluded during the period of exploitation. However, the situation has not yet occurred in this installation.
W3	**PROBABLE** This cause might occur during the period of operation and has already occurred in the past in installations in the company or similar installations elsewhere.
W4	**EXPECTED** No experience with the installation, e.g., new installations, or no assessment possible. For existing installations, this cause has already occurred frequently.

Table 4.6: *Matrix for evaluating the risk class (RC) of a scenario, combining the likelihood (L) and severity (S) classes.*

		1 per 1000 years	1 per 100 years	1 per 10 years	1 per 1 years
		W1	**W2**	**W3**	**W4**
		Unlikely	*Rare*	*Probable*	*Expected*
E1	*Noticeable*	F	F	F	E
E2	*Great*	F	F	E	D
E3	*Serious*	F	E	D	C
E4	*Very serious*	E	D	C	B
E5	*Catastrophic*	D	C	B	A

Table 4.7: *Risk classification*

Risk class (RC)	**Description**
F	**Noticeable Risk** No additional risk measures are required.
E	**Moderate Risk** Technical or organisational risk-reducing measures may be required.
D	**Severe Risk** Active or passive barriers as risk-reducing measures may be required.
C	**Very severe Risk** Active or passive barriers as risk-reducing measures are required.
B	**Catastrophic Risk** Active or passive barriers as risk-reducing measures are required.
A	**Extreme Risk** Passive barriers as risk-reducing measures are required. Redesign is recommended.

In order to determine the likelihood of the different initiating events (indicated as causes in Table 4.3), values from the literature have been used [34,48,50,51,65]. In Table 4.3, it can be observed that the severity class, and consequently the risk class, is not always unique. This is because the final scenario could be classified in both classes. However, during the LOPA analysis (§4.5), the conservative approach was used (e.g., the risk class of cause 1 in Table 4.3 is considered equal to C).

4.5 Case study: LOPA

In the present work, the risk classification involves three different classes:

- Risk class A (extreme risk): risk-reducing measures can only be passive technical measures where redesign is strongly recommended.
- Risk class B (very big risk): risk-reducing measures can only be active or passive technical measures with a slight preference for the use of passive measures.

- Risk class C (big risk): risk-reducing measures can only be active or passive technical measures with a slight preference for the use of passive measures.

This classification can be obtained by combining the likelihood and severity of the final events, i.e. the Top Events, that emerged from the HAZOP analysis. The relevant Top Events are discussed in the following sections, and the functional safety approach (discussed in §3.4) is implemented to identify and quantify proper protective measures and recommendations. These sections are structured to provide a clear analysis of the initiating events and how adding specific protective layers can reduce their frequency of occurrence.

The possible initiating events have been obtained from the HAZOP analysis (see §A.9).

Top Events listed in Table A.10.1 are the initiating events with a high probability and a risk class higher than C, i.e. at least very severe risk scenarios.

It can be noted that the majority of Top Events occur in Node 2 and are primarily due to human error. Incidentally, operating on the reactor is critical, and many actions on the pilot plant are performed manually. Other initiating events are due to system failures, which are described in §4.5.2.

The LOPA is performed according to BS EN 61511-1:2017+A1 [49], BS EN 61511-2:2017 [50] and BS EN 61511-3:2017 [34]. According to Table F.8 of [50], the tolerable frequency of a hazardous event (expressed in events/year) is defined. Since the resulting risk class is C (very severe) for all the considered events, the tolerable occurrence frequency[6] is equal to 10^{-4} yr^{-1}. The procedure discussed in Figure 3.4 has been followed to perform the analysis. When the intermediate frequency is lower than the tolerable frequency, the procedure is finished.

When this final frequency is calculated, the resulting reduced final risk class is represented in a contour plot and compared to the initial state (Figure 4.3 [66]). Equations 4.1 and 4.2 define the mean probability of failure (P_f) and the severity (*D,* It has a different definition than S in HAZOP) of the specific event [66]. The time assumed for the analysis (t) is 10 years, which is considered consistent with the lifetime of an experimental setup for academic research, and the frequency is specified for each event. The C (cost of damage) is estimated to calculate the severity using the values given in Table 4.8 [66].

$$P_f = \frac{t - 1/f(1 - \exp(-ft))}{t} \tag{4.1}$$

$$D = \frac{\log(c)}{\log(c_{max})} \tag{4.2}$$

---

[6] The correction factor required from Note 1 of Table F.8 [50] is already considered.

Table 4.8: *Classification of the severity of a given hazardous initiating event, considering the cost of damage (C) and the severity (D)* [66].

Rank	**Assets**	**C** [€]	**D** [-]
1	No damage	1	0
2	Slight (< 100 €)	10	0.2
3	Minor (> 100 € and < 1,000 €)	10^2	0.4
4	Localized (> 1,000 € and < 10,000 €)	10^3	0.6
5	Major (> 10,000 € and < 100,000 €)	10^4	0.8
6	Extensive (> 100,000 €)	10^5	1

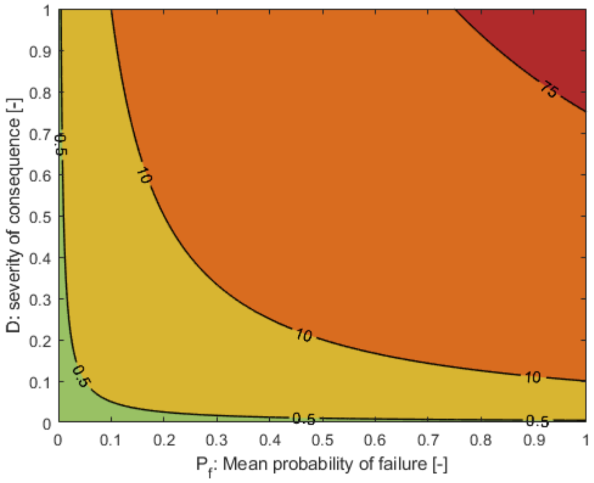


Figure 4.3: *Contour plot to define the risk class of the scenario (adjusted from [66])*

The contour plot reported in Figure 4.3 is useful to understand the classification of the risk class for each considered event. The risk class is classified as reported in Table 4.9, and the value of the resulting risk R is calculated by Eq. 4.3.

$$R = 100 \cdot D \cdot P_f \tag{4.3}$$

Table 4.9: *Risk classification criterion.*

Risk level	**Classification**
$0 \leq R < 0.5$	*Low*
$0.5 \leq R < 10$	*Moderate*
$10 \leq R < 75$	*High*
$75 \leq R \leq 100$	*Unacceptable*

Since the risk assessment is based on the experience of the analyst, the classification shown in Table 4.9 may be different depending on alternative criteria decided by the HAZOP and LOPA team. The events analyzed in the present work are classified as *unacceptable* or *high.*

4.5.1 Deviations due to a human error

The primary deviations induced by human error are the following:

- MORE pressure,
- MORE flow,
- MORE temperature or reaction rate (higher reaction magnitude),
- TOO EARLY opening of the reactor,
- TOO LATE closing of the reactor.

MORE pressure is usually combined with MORE flow. This can be explained by the fact that an increase in flow accompanies an increase in pressure, as the reactants are gases in isothermal conditions.

MORE pressure or flow can induce various consequences, including:

- MORE conversion of CO and consequent loss of an experimental test;
- LESS separation in D-01 and consequent loss of an experimental test;
- Establishment of the maximum pressure of the equipment, i.e., in pipes, in the mixer, in the reactor;
- Basic damage to sealings and fittings;
- Leakages and ruptures from the pilot plant equipment;
- Loss of containment of flammable or toxic material(s);
- Fire, explosion or exposure to toxic.

It is worth noting that a deviation of MORE flow affects the final composition of the mixture, leading to the loss of the experimental test. Increasing the flow in streams 5, 6 or 7 will not change the final composition of the mixture but will change the flow rates of the streams after R-01 (streams 8 to 17), resulting in possible condensation of products in streams 9, 10 and 11 and less separation in D-01. If the flow rate is changed by only one of the reactants, the final composition will change as reported in §4.5.3.1.

The substances involved are flammable and poisoning, and some protection layers are required in the case of a loss of containment, as will be discussed later in the section.

In the HAZOP analysis, the safeguards indicated for these deviations are:

- hood;
- pressure sensor(s);
- leakage monitoring system;
- high-pressure indicator and alarm (PIAH), i.e., a sensor providing an alarm once the pressure is above a set threshold.

According to the functional safety approach, the effectiveness of the layers of protection needs to be assessed according to the risk reduction criteria.

Concerning the consequences of the initiating event these are classified into three categories: acceptable, undesired and unacceptable (Table 4.10). Acceptable consequences also refer to minor consequences which are related to operational issues or transient scenarios. Unacceptable consequences can involve an effect on a human target.

Table 4.10: *Categories of consequences.*

Classification	Consequences
Acceptable	MORE conversion LESS separation Loss of an experimental test
Undesired	Establishment of the maximum pressure Damage to sealings and fittings General leakages and ruptures
Unacceptable	Loss of containment of flammable or toxic material(s) Fire, explosion or exposure to toxics.

For each undesired or unacceptable consequence, Table 4.11 indicates which are the possible preventive or mitigative actions or systems.

Table 4.11: *Preventive or mitigative actions in the case of undesired or unacceptable consequences associated with an initiating event.*

Classification	Consequences	Preventive/mitigative actions
Undesired	Establishment of the maximum pressure	BPCS, safety devices (pressure relief devices)
	Damage to sealings or fittings	Hood, leakage monitoring system acting on isolation valves
	Leakages and ruptures	Hood, leakage monitoring system acting on isolation valves
Unacceptable	Loss of containment of flammable or toxic material(s)	Hood, leakage monitoring system acting on isolation valves
	Fire, explosion, exposure to toxics	No ignition sources, hood, or leakage monitoring system acting on isolation valves reducing the amount released

The pressure relief devices should be compliant with the regulations, such as API 520 [54,55] or EN 764-7:2002 [67].

A deviation of MORE temperature is usually correlated to MORE reaction rate, and the main consequences of these deviations are classified in Table 4.12.

Table 4.12: *Deviation of MORE temperature or reaction rate: classification of consequences.*

Classification	Consequences
Acceptable	Altered final composition of the mixture Loss of the experimental test
Undesired	Pressure increase (§1.2.1) Damage to the catalyst Leakages and ruptures
Unacceptable	Major loss of containment, fire, explosion or exposure to toxics

These safeguards are similar to those assigned to the deviation of MORE pressure deviation since the temperature is strictly correlated to the system's pressure. As the temperature increases, so does the reaction rate of R.1-5, and a higher carbon deposition can be expected. If the carbon deposition fouls the catalyst, hot spots can also arise. Moreover, the internal pressure in the system may increase, with the associated consequences since an increase in temperature increases the volume of the gaseous phases and the final pressure.

The pilot plant operates continuously but is stopped every week for cleaning and emptying operations on the main equipment (R-01 and D-01). The start-up and shut-down of the plant require to change the set-point of the following controllers:

- PRC-09;
- MFC-01; -02; -03; -04;
- TC-01; -02;

When the flow in the system is zero, R-01 and D-01 are opened by the operator and cleaned with acetone. The shut-down and the start-up of the system are performed manually by a single operator (no written procedure is available), so it is reasonable to consider a high frequency of human error (§3.4.4). In this regard, two credible hazardous scenarios can be obtained when the procedure is not applied correctly:

- the reactor is opened TOO EARLY;
- the reactor is closed TOO LATE.

Independently on the scenario, the following consequences can occur: loss of containment of flammable or toxic materials, fire, or explosion (upon effective ignition source and provided the quantity of released material can sustain an explosion). Such a set of consequences is unacceptable, and proper layers of protection are required. These include suitable sensors (as detectors for hazardous gases) and the hood.

4.5.2 System failure

The system failure considered in this analysis includes:

- a power outage,
- a failure of a sensor or an indicator of a process variable,

- leakages or defective connections.

These initiating events can lead to hazardous scenarios, and the associated deviations are the following:

- MORE or LESS pressure (§4.5.1);
- MORE or LESS flow (§4.5.1);
- LESS or NO voltage.

If there is LESS or NO voltage, the equipment (such as R-01, D-01, controllers -01 to -04) may not respond as it should. In this scenario, the solenoid valves (valves 4, Figure A.1.1) will fail closed, and the process will no longer be supplied with reactants (all the valves in the plant behave as FC). The reactor (R-01) will stop running appropriately as its temperature control (Control-02) will stop working. Control-02 is a feedback controller with a temperature indicator. It adjusts the furnace power as the temperature inside R-01 rises. If the power is switched off, valves will fail close, and some reactants may remain in the reactor, which will take some time to reduce its temperature. During this time, the temperature inside the reactor is no longer controlled, and the residues inside R-01 could lead to some hot spots and consequently increase the reaction rate (§4.5.1), potentially damaging the catalyst bed. Finally, in the event of a power failure, controllers -03 and -04 will also stop working, resulting in the following:

- LESS separation in D-01 because the temperature in D-01 is not equal to 5°C, and not all heavy products could condensate;
- Blockage of E-01 because the temperature can be lower than 60÷80°C, and some products, including waxes, can condense before D-01.

Such scenarios can be prevented by adopting an independent emergency power supply with the characteristics described in §3.4.9.

4.5.3 Deviations in Node 1: Feeding section

The purpose of Node 1 is to feed the process and maintain the composition of the mixture fed to the reactor. The node consists of four streams carrying respectively hydrogen, carbon monoxide, carbon dioxide and nitrogen. All these chemicals are pure, and the equipment is listed in Table A.10.2. It can be seen from Figure 4.1 that the valves of each stream have the same number. This does not mean that the same valve manages four different streams but that these valves have the same characteristics for each stream (e.g., valve 1 for the hydrogen stream has the same characteristics as valve 1 for the CO stream).

The hazardous initiating events of Node 1 reported in Table A.10.1 are the following:

- Wrong set point in at least one of MFC-01, 02, 03 or 04;
- A power outage.

These initiating events are analyzed respectively in Sections §4.5.3.1-2.

4.5.3.1 Mass flow controllers: MFC-01, -02, -03, -04.

Setting the MFC-01/02/03/04 is a manual operation done by a student or a researcher every week, so the possibility of incorrect setting has a frequency of 1 per year [51]. When at least one set point is wrong, a deviation of MORE pressure or flow can occur (§4.5.1).

The safeguards indicated in the HAZOP analysis are the adoption of the hood, a sensor for leakages and a high-pressure alarm and indicator (PIAH).

In this regard, the hood and detectors for reactants and methane are already installed. The increasing pressure will be expected downstream of valve 6, so the existing protection layers are the hood and valve 4. As the nitrogen stream (stream 4) does not have a solenoid valve (valve 4 in the other streams), this valve cannot be considered for managing an incorrect nitrogen set-point.

When at least one of the flow rates is set incorrectly, the ratio between the reactants and the inert fed to the pilot plant changes. The resulting scenarios are illustrated in Table 4.13.

Table 4.13: *Deviations induced by errors in the setting of mass flow controllers. Details on the consequences due to the deviated ratio of reactants.*

Substance	Deviation	Consequence
Hydrogen	MORE flow rate	Altered selectivity and conversion, i.e., a higher quantity of short-chained products is produced (e.g., liquefied petroleum gas)
	LESS flow rate	Altered selectivity and conversion, i.e., a higher quantity of long-chained products is produced (e.g., waxes)
	NO flow rate	R.1-4 do not occur
	LESS ratio with CO or CO_2 (< 1)	No reactions occur
Carbon monoxide	MORE flow rate	Altered selectivity and conversion, i.e., a higher quantity of long-chained products is produced (e.g., waxes)
	LESS flow rate	Altered selectivity and conversion, i.e., a higher quantity of short-chained products is produced (e.g., liquefied petroleum gas)
	NO flow rate	R.1-5 do not occur
Carbon dioxide	MORE flow rate	Altered selectivity and conversion, i.e., a higher quantity of long-chained products is produced (e.g., waxes)
	LESS flow rate	Altered selectivity and conversion, i.e., a higher quantity of short-chained products is produced (e.g., liquefied petroleum gas)
	NO flow rate	R.1-5 do not occur
Nitrogen	NO flow rate	GC composition measurement not correct

Table 4.13 shows that a change in the initial composition affects the final composition of the mixture resulting from the FT synthesis. More in detail, an altered quantity of H_2, CO or CO_2 will affect selectivity towards short of long chain products.

Another possible operator error is the swapping of carbon monoxide operating conditions for carbon dioxide in MFC-01, -02, -03 and -04. The consequences are illustrated in Table 4.14.

Table 4.14: *Deviations induced by substitution of substances. Details on the consequences.*

Deviation	Consequence
AS WELL AS flow rate of CO (CO fed instead of CO_2)	If CO is fed instead of CO_2, a higher conversion of CO will be observed since CO is more reactive than CO_2. The product mixture will be rich in long-chain hydrocarbons. Faster FT catalyst deactivation.
AS WELL AS flow rate of CO_2 (CO_2 fed instead of CO)	If CO_2 is fed instead of CO, a lower conversion of CO_2 will be observed as CO is more reactive than CO_2, and the temperature of R-01 is lower than that required for CO_2. The product mixture will be rich in short-chain hydrocarbons.

In summary, if the wrong reactant is added, an experimental test is lost.

To control the eventual consequences of deviations related to the hydrogen feed line (e.g., leakages), the following IPLs are provided:

- Valve 4: This solenoid valve is connected to detectors of CO, CO_2, CH_4 and H_2. This valve acts as FC, i.e., if any detector detects at least one of the abovementioned chemicals or when there is a decrease in the voltage of supplied equipment, the valve will block the flow.
- Hood, which can be considered as an IPL since the increase in pressure starts from stream 1.5;

The effect of these protection layers on the frequency of events is reported in Table 4.15.

Table 4.15: *Existing independent protection layers (IPLs) to manage a deviation induced by a wrong set-point in MFC-01/-03.*

Initiating event	Frequency (yr^{-1})	Independent protection layer 1 Solenoid valve	Independent protection layer 2 Hood (Passive IPLs)	Intermediate frequency (yr^{-1})	Tolerable frequency (yr^{-1})
Wrong set point (MORE pressure or flow)	1 (7,8)	0.028	0.1	$2.8 \cdot 10^{-3}$	$1 \cdot 10^{-4}$

---

[7] From Table 4.3 of [51].

[8] From Table G.3 of [34].

This intermediate frequency is higher than tolerable, so additional IPLs are required. The risk reduction factor (RRF) obtained by eq. (3.1) equals 28, and a SIL 1 is required. The SIL 1 IPL needs to be added to the existing protection layers, i.e., the solenoid valve and hood.

Table 4.16: *Additional independent protection layer (IPL) to manage a deviation induced by a wrong set-point in MFC-01/-03.*

Initiating event	**Frequency (yr^{-1})**	**IPLs**			**Intermediate frequency (yr^{-1})**	**Tolerable frequency (yr^{-1})**
		1	**2**	**3**		
		SIL 1	**Solenoid valve**	**Hood (Passive IPLs)**		
Wrong set point (MORE pressure or flow)	1	0.1 (9)	0.028	0.1	$2.8 \cdot 10^{-4}$	$1 \cdot 10^{-4}$

The resulting intermediate frequency is higher than the tolerable threshold, and additional layers of protection are required. However, the necessary reduction factor is RRF = 2.8. Hence, a SIL “a” (RRF < 10) is required. It does not need to be a SIF, and it is not necessary to comply with IEC 61508 and 61511. In this regard, maintenance practice and control of equipment wear out are helpful to reduce further and control the frequency.

In any case, provided that the initiating event is due to a human error, the operator response cannot be considered an IPL, as the same person who initiated the event is likely to respond to an alarm [48].

Table 4.17: *Safety and pressure relief device as independent protection layers (IPLs) to manage a deviation induced by a wrong set-point in MFC-01/-03.*

Initiating event	**Frequency (yr^{-1})**	**IPLs**				**Intermediate frequency (yr^{-1})**	**Tolerable frequency (yr^{-1})**
		1	**2**	**3**	**4**		
		Safety device	**Pressure relief device**	**Solenoid valve**	**Hood (Passive IPLs)**		
Wrong set point (MORE pressure or flow)	1	$1 \cdot 10^{-4}$ (10)	0.1 (11)	0.028	0.1	$2.8 \cdot 10^{-8}$	$1 \cdot 10^{-4}$

Adding a safety device and a pressure relief device decreases the frequency of the hazardous event to a value of $< 10^{-4}$. The safety device indicated as IPL 1 is an I/O system and is a digital input channel used to limit the possible setpoint range. In particular, this device can be classified as a “maximum physical value limiter”, where a maximum value for the flowrate is set by an

---

[9] From Table 5.14 of [51].

[10] http://silsafedata.com/ [53], expressed as a digital input channel.

[11] From Table 4.5 of [48].

authorized operator, in this case, the principal investigator of the pilot plant or the maintenance manager [68].

The pressure relief device should be placed before valve 7 (stream 1.6) (Figure 4.4) since Node 1 can be isolated via valve 7 if the pressure or flow is higher than the design intent.

The safety device is implemented such as to fix an operating range that an operator can not modify.

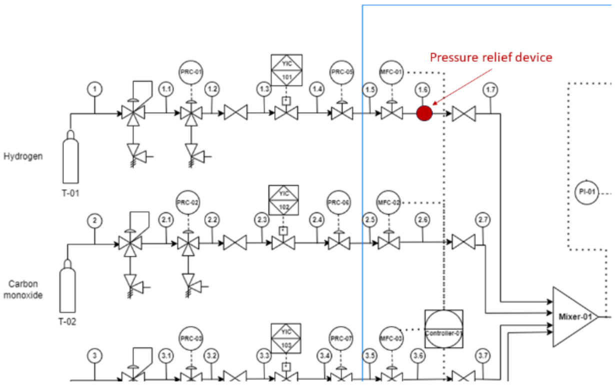


Figure 4.4: *Position of the pressure relief device along the hydrogen stream*

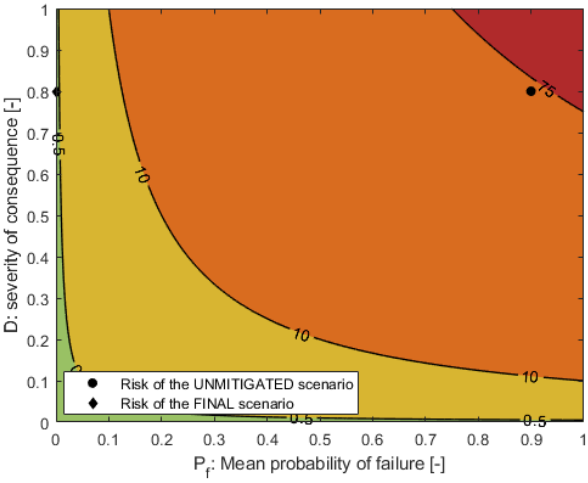


Figure 4.5: *Risk class when the set-point of MFC-01/-03 is incorrect (Node 1) (D = 5).*

The final risk class of the present scenario for the hydrogen stream is reduced to *low* after implementing the proposed independent protection layers.

The considerations made for hydrogen streams can also be implemented for carbon monoxide and carbon dioxide streams since the existing protection layers used to manage the resulting scenarios are the same. So, the additional IPLs required are the safety device and the pressure relief device.

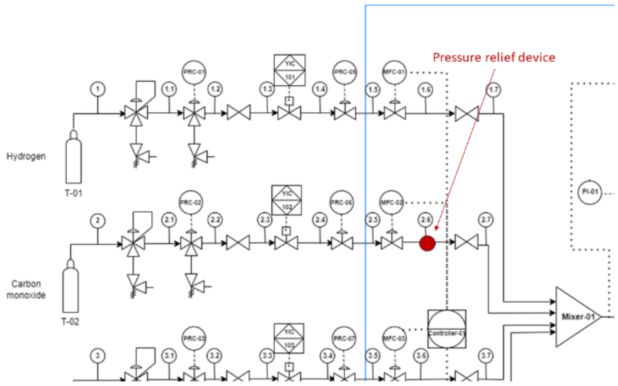


Figure 4.6: *Position of pressure relief device along the carbon monoxide stream.*

Figures 4.6 and 4.7 indicate the position of the pressure relief device to accommodate eventual deviations as emerged from the HAZOP analysis. The final and the initial risk classes are equal to the one represented in Figure 4.5, so the final classification is equal to *low* for both the considered streams.

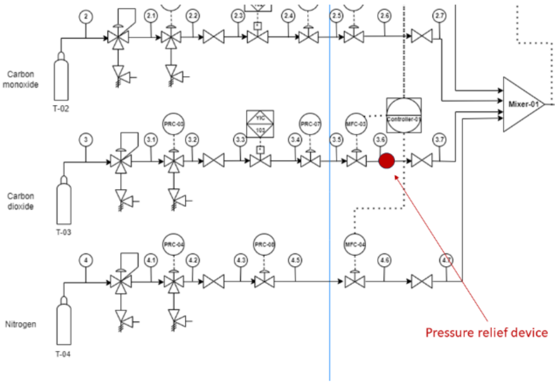


Figure 4.7: *Position of pressure relief device along the carbon dioxide stream.*

The nitrogen stream has a similar structure to the previous streams but does not have the solenoid valve. The properties of N_2 are less hazardous than H_2 and CO, so the classification of the HAZOP risk class is D, and the LOPA analysis is not required.

However, a possible final configuration of the IPLs is shown in Table 4.18, where the assumptions of the two additional protective layers (IPLs 1 and 2) are the same as the one discussed for the hydrogen stream.

Table 4.18: *Independent protection layers required to manage a wrong set-point in MFC-04.*

Initiating event	Frequency (yr^{-1})	IPLs			Intermediate frequency (yr^{-1})
		1	**2**	**3**	
		Safety device	**Pressure relief device**	**Hood (Passive IPLs)**	
Wrong set point (MORE pressure or flow)	1 (12,13)	$1\cdot10^{-4}$ (14)	0.1(15)	0.1 (16)	$2.8\cdot10^{-6}$

The position of the pressure relief device is reported in Figure 4.8.

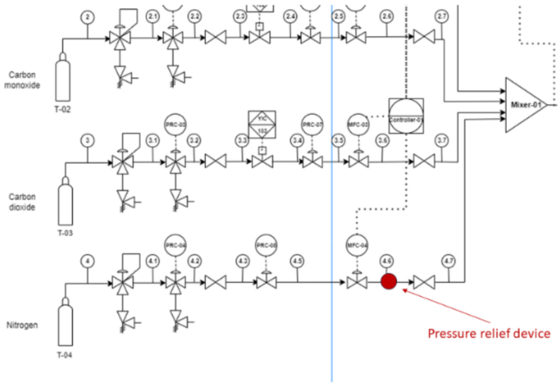


Figure 4.8: *Position of pressure relief device in Nitrogen stream.*

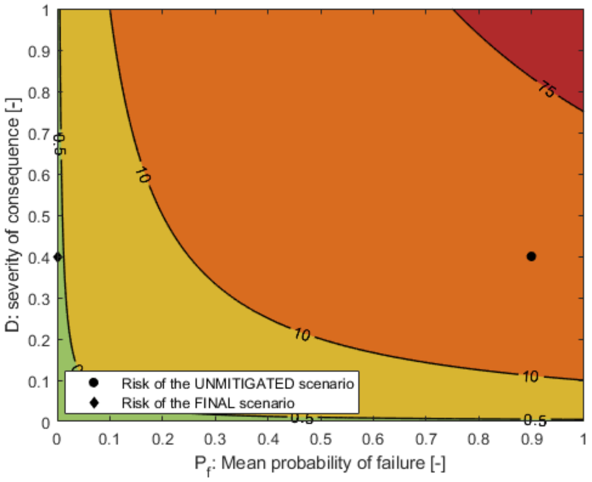


Figure 4.9: *Risk class when the set-point of MFC-04 is incorrect (Node 1) (D = 3), before and after implementing the protection layers.*

---

[12] From Table 4.3 of [51]

[13] From Table G.3 of [34]

[14] http://silsafedata.com/ [53]: Digital input channel

[15] From Table 4.5 of [48]

[16] From Table 5.37 of [51]

From Figure 4.9, the initial risk class (the existing IPLs are not considered) is *high,* and the final risk class (considering the existing and the additional IPLs) is *low*.

4.5.3.2 Electrical system: a power outage

A power outage, intended among the different initiating events, can determine a trip scenario leading to undesired outcomes. Other causes inducing such an occurrence include a short circuit and a spurious trip of electrical protective systems.

If there is a power outage, the solenoid valves will act fail close (FC). Without proper management of the inflow, this gives a possible increase in the pressure upstream of valve 4, especially if this is a manual step requiring monitoring. Other expected consequences affecting the downstream nodes include a pressure decrease, decreasing/no flow to the reactor and the loss of an experimental test (see §4.5.2). The hazardous scenario is related to the increasing pressure consequences. The existing protection layers are the hood, solenoid valve, and two pressure relief valves connected to valves 1 and 2.

Table 4.19: *Existing independent protection layers required to manage a power outage in Node 1.*

Initiating event	**Frequency (yr^{-1})**	**IPLs**				**Intermediate frequency (yr^{-1})**	**Tolerable frequency (yr^{-1})**
		1	**2**	**3**	**4**		
		Pressure relief valve	**Pressure relief valve**	**Solenoid valve**	**Hood (Passive IPLs)**		
Power outage (LESS/NO electric voltage)	1 (17)	0.01 (18)	0.01	0.028	0.1	$2.8 \cdot 10^{-7}$	$1 \cdot 10^{-4}$

The resulting scenario is classified with severe consequences, so the tolerable frequency is equal to 10^{-4} yr^{-1}, higher than the intermediate frequency.

---

[17] From personal communication with the operators of the pilot plant. Such a scenario has been experienced statistically one time per year.

[18] Table G.7 of [34]

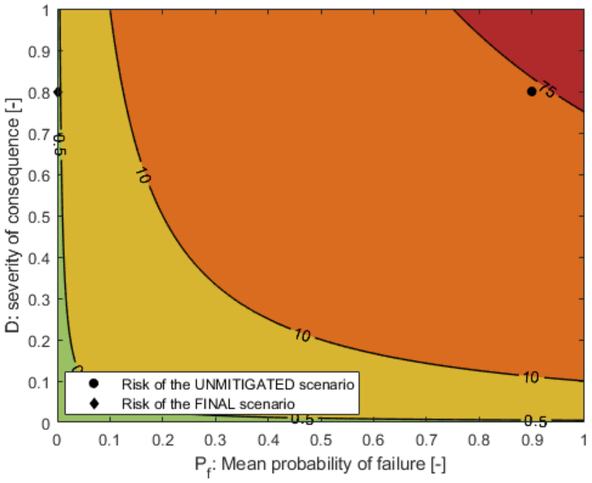


Figure 4.10: *Risk class for the event power outage in Node 1 (D = 5).*

In conclusion, no additional protection layers are required, and the risk classification is *low*.

4.5.4 Deviations in Node 2: the reaction section

Node 2 converts the reactants to products according to the desired conversion and selectivity. The aim is to obtain a heavy phase consisting of C_7-C_{30}. A by-product of the main reaction is water. The E-01 is the heat exchanger downstream of the reactor, and it keeps stream 8 in a gaseous phase. The composition of stream 8 depends on the composition of stream 7, where the ratios between the different reactants are fundamental to the occurrence of R.1 and R.2 (Tables 4.13-14).

The solenoid valves (valve 4) connected to the detectors (Node 1) fail close and act if at least one of CO, CO_2, CH_4 or H_2 is detected in the laboratory. However, for the LOPA analysis of Node 2, Valve 4 is not considered an IPL as it is equipment of node 1.

4.5.4.1 Failure of PI-01

If PI-01 fails or malfunctions, the pressure indicated can be wrong. The pressure inside the pilot may increase without supervision by the operator. Additionally, an increasing flow is possible. The consequences of these deviations are listed in Table 4.20.

Table 4.20: *Deviations of MORE pressure or flow in the pilot plant and associated safeguards.*

Deviation	Possible Safeguards	Comments
MORE conversion of carbon monoxide	Temperature control loop, pressure control loop	In the case of PI-01 failure, the operator can wrongly set the pressure. If the resulting deviation is LESS pressure, the resulting consequence is LESS conversion, and the system is more prone to light products. On the contrary, MORE pressure pushes the conversion to long-chain hydrocarbons.
AS WELL AS outlet composition	Temperature control loop, pressure control loop	See Table 4.14
MORE Temperature in E-01 and R-01	Temperature control loop Sensors for pressure	See § 4.5.1
Leakages or rupture	Sensors for leakages Sensors for pressure Hood	There is a release of toxic or flammable materials, so additional protective layers are required.
Loss of containment and additional final events	Sensors for leakages Sensors for pressure Hood	There is a release of toxic and flammable materials, so additional protective layers are required.

The safeguards indicated in the HAZOP analysis are a hood, a sensor for leakages, a sensor for pressure and an alarmed high-pressure indicator (PIAH). Two existing protection layers are present, i.e., the hood and valve 10. Valve 10, although related to node 3, can handle a deviation of MORE pressure originating in node 2.

Table 4.21: *Existing independent protection layers to manage the failure of PI-01 in Node 2.*

Initiating event	Frequency (yr^{-1})	IPLs 1 Valve 10 (Rupture disk)	IPLs 2 Hood (Passive IPLs)	Intermediate frequency (yr^{-1})	Tolerable frequency (yr^{-1})
PI-01fails (MORE pressure)	~ 1 (19)	0.01 (20)	0.1	$1 \cdot 10^{-3}$	$1 \cdot 10^{-4}$

Intermediate frequency is higher than tolerable. The risk reduction factor equals 10, so a SIL 1 is required.

---

[19] Table 11-1 of [65]

[20] Table 5.21 of [51]

Table 4.22: *Additional independent protection layers required to manage the failure of PI-01 in Node 2.*

Initiating event	Frequency (yr^{-1})	IPLs			Intermediate frequency (yr^{-1})	Tolerable frequency (yr^{-1})
		1	**2**	**3**		
		SIL 1	**Valve 10 (Rupture disk)**	**Hood (Passive IPLs)**		
PI-01fails (MORE pressure)	≈ 1	0.1	0.01	0.1	$1\cdot10^{-4}$	$1\cdot10^{-4}$

Since the initiating event is not related to a human error but is due to misoperations, the alarmed high-pressure indicator with an operator response could be considered an independent layer of protection if the operator has been trained to act upon an alarm. Alarms with operator response can be assigned PFD = 0.1 if the independence requirements are met. More in detail, the alarmed system must be independent of the BPCS (i.e., the hardware associated with the initiating cause is not associated with the alarm), and the initiating cause does not involve an operator error.

Concerning this topic, it is worth noting that the operator's response to the alarm must be feasible and independent (see §3.4.4).

The pilot plant is not continuously monitored. Therefore, the operator action coupled with the alarm cannot be considered an independent protection layer.

Table 4.23: *Independent protection layers required to manage PI-01 failure in Node 2.*

Initiating event	Frequency (yr^{-1})	IPLs			Intermediate frequency (yr^{-1})	Tolerable frequency (yr^{-1})
		1	**2**	**3**		
		2oo3 Redundant scheme	**Valve 10 (Rupture disk)**	**Hood (Passive IPLs)**		
PI-01fails (MORE pressure)	≈ 1	$3.5\cdot10^{-5}$ (21)	0.01	0.1	$3.5\cdot10^{-8}$	$1\cdot10^{-4}$

The additional layer of protection can be a redundant pressure sensor with a suitable *MooN* scheme, such as 2oo3 (discussed in §3.4.7), where the three initiators should be placed at streams 5, 7 and 8 (Figure 4.11). This scheme is a symmetrical architecture that successfully tolerates a short circuit or an open circuit failure. If a short circuit occurs, the 2oo3 structure becomes a 2oo2 system. On the other hand, if a unit fails as an open circuit, the redundant scheme goes from a 2oo3 structure to a 1oo2 structure [52].

---

[21] Table F-10 of [52]

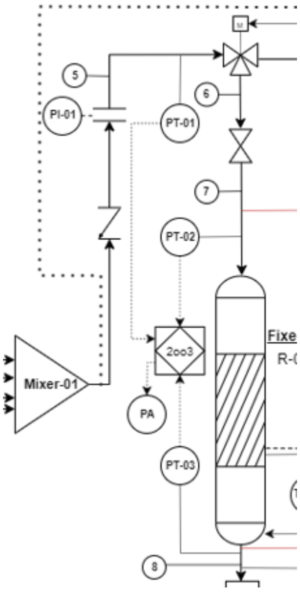


Figure 4.11: *Independent protection layer based on 2oo3 redundant scheme working on 20 bar sensors (PT-01, PT-02, PT-03, SIL3 2oo3, PA). When the pressure is above 20 bar, the alarm is provided.*

The 2oo3 architecture will fail dangerously only if two units fail simultaneously [52]. In this case, when two sensors fail, an alarm is provided.

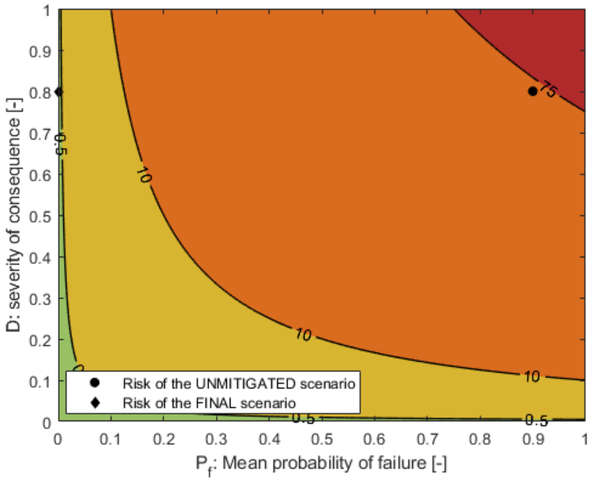


Figure 4.12: *Risk class for the event PI-01 failure in Node 2 (D = 5).*

Use the 2oo3 scheme instead of PI-01 to reduce the risk class from *high* to *low*.

4.5.4.2 Incorrect reactor packing (R-01)

When the pilot plant is shut down, the reactor is emptied, and the catalyst is entirely replaced. Previous tests showed that if the catalyst is too fine or active, the pressure inside R-01 will increase, and the equipment undergoes dangerous vibration. Possible leakages from the inlet or outlet connections can occur. In order to avoid this scenario, the following catalyst's characteristics are already adjusted:

- Catalyst size (100-150 μm);
- Addition of an inert to the catalyst, such as SiO_2 or mineral hood.

The consequences listed in the HAZOP analysis for an incorrect reactor packing are classified as reported in Table 4.24.

Table 4.24: *Classification of consequences for the event of reactor overpacking.*

Classification	Consequences
Acceptable	More conversion of CO Altered composition of products Loss of a test
Undesired	Leakages Rupture of the reactor (the reactor no longer works as expected)
Unacceptable	Explosion, injury or death

Since the hazardous scenario is related to an increase in pressure, the safeguards are the following: hood, sensor for leakages, sensors for pressure, alarm sensor set at high pressure (PIAH).

The PIAH cannot be used as an independent layer of protection since the initiating event is related to a human error (§3.4.4). Since the existing protection layers are the same as in §4.5.4.1 (hood and valve 10) and the classification of the hazardous scenario is preserved, final calculations are reported in Table 4.25.

Table 4.25: *Independent protection layers required to manage an incorrect reactor packing in Node 2.*

		IPLs				
		1	2	3		
Initiating event	**Frequency (yr^{-1})**	**Basic process control system (BPCS)**	**Valve 10 (Rupture disk)**	**Hood (Passive IPLs)**	**Intermediate frequency (yr^{-1})**	**Tolerable frequency (yr^{-1})**
Incorrect reactor packing: overpacked reactor (MORE pressure)	1 (22,23)	0.1	0.01	0.1	$1 \cdot 10^{-4}$	$1 \cdot 10^{-4}$

---

[22] From Table 4.3 of [51]

[23] From Table G.3 of [34]

Without the independent layer of protection, the intermediate frequency is higher than the tolerable frequency. A control loop (BPCS) has to be added in order to decrease the frequency of the resulting scenario. The control loop should be composed of a pressure sensor measuring the process variable in stream 8, which is connected to a motorized three-way valve, as in Figure 4.13 (valve 8 should be changed with a motorized three-way valve).

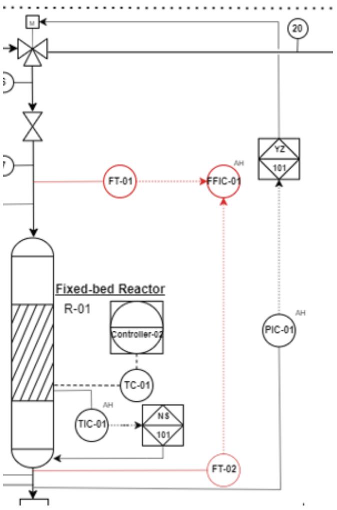


Figure 4.13: *Independent protection layer based on a BPCS (PIC-01, YZ-101, motorized three-way valve). When the pressure is above 20% of the operating pressure, the motorized three-way valve changes the direction of the flow from stream 6 to stream 20.*

When the pressure in stream 8 is higher than the one fixed for safety reasons, the new valve 8 automatically deviates the feeding mixture to the by-pass line.

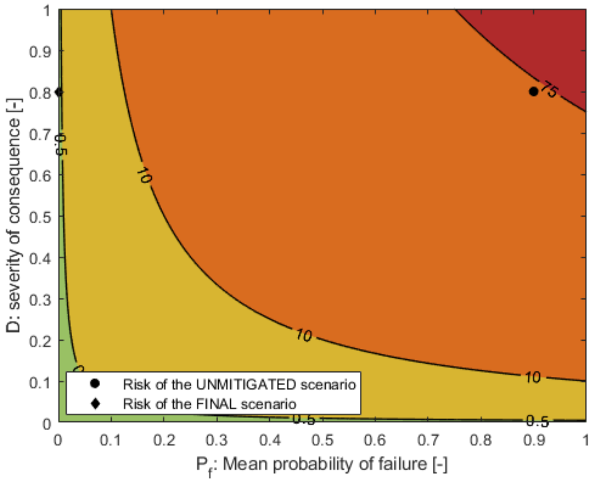


Figure 4.14: *Risk class for the event of reactor overpacking in Node 2 (D = 5).*

The final risk class is low when adding the BPCS as an independent layer of protection.

4.5.4.3 Incorrect setting of PRC-09

Selecting the set-point of PRC-09 is a manual operation done weekly. Periodic checking and recording of the setpoint should be done at least twice daily.

If the set-point is wrong, two primary deviations can be observed from R-01: MORE or LESS pressure. If the pressure increases, the flow will have the same trend (MORE flow rate), and the same is true for decreasing pressure (NO or LESS flow). When there is a decrease in pressure, the conversion of CO decreases. The main deviations are MORE flow and pressure (discussed in §4.5.1).

The existing independent protection layers (IPLs) are the following:

- Valve 10;
- Hood.

The intermediate frequency of the initiating event without additional IPLs is higher than the tolerable one, so a SIL1 is required. Table 4.26 provides the final analysis related to an increase in pressure and flow due to a wrong set-point of PRC-09.

Table 4.26: *IPLs required to manage a wrong set-point of PRC-09*

Initiating event	**Frequency (yr^{-1})**	**IPLs**			**Intermediate frequency (yr^{-1})**	**Tolerable frequency (yr^{-1})**
		1	**2**	**3**		
		Basic process control system (BPCS)	**Valve 10 (Rupture disk)**	**Hood (Passive IPLs)**		
Wrong set point of PRC-09 (MORE pressure or flow)	1 (24,25)	0.1	0.01	0.1	$1 \cdot 10^{-4}$	$1 \cdot 10^{-4}$

The additional control system has the same characteristics as discussed in §4.5.4.2, and it is represented in Figure 4.13. The resulting risk class is *low*.

---

[24] From Table 4.3 of [51]

[25] From Table G.3 of [34]

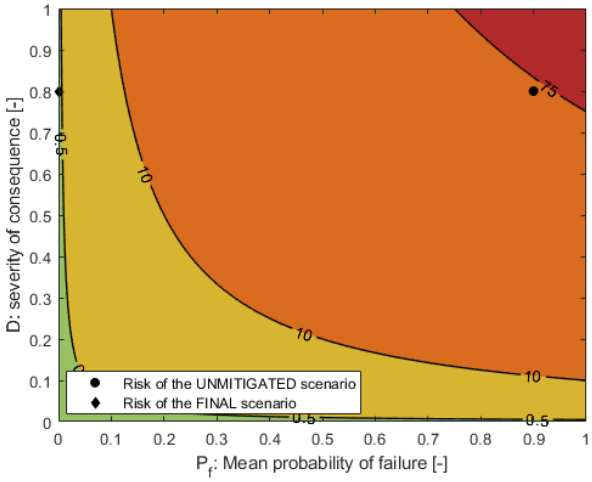


Figure 4.15: *Risk class when the set-point of PRC-09 is wrong in Node 2 (D = 5).*

4.5.4.4 Incorrect setting of TC-01

Set the set-point of TC-01 is a manual operation done almost daily, with an estimated failure frequency of 1 yr^{-1}. The temperature inside the reactor follows a ramp, which is already defined (Figure 4.16). The resulting hazardous scenarios are related to a higher set-point of TC-01.

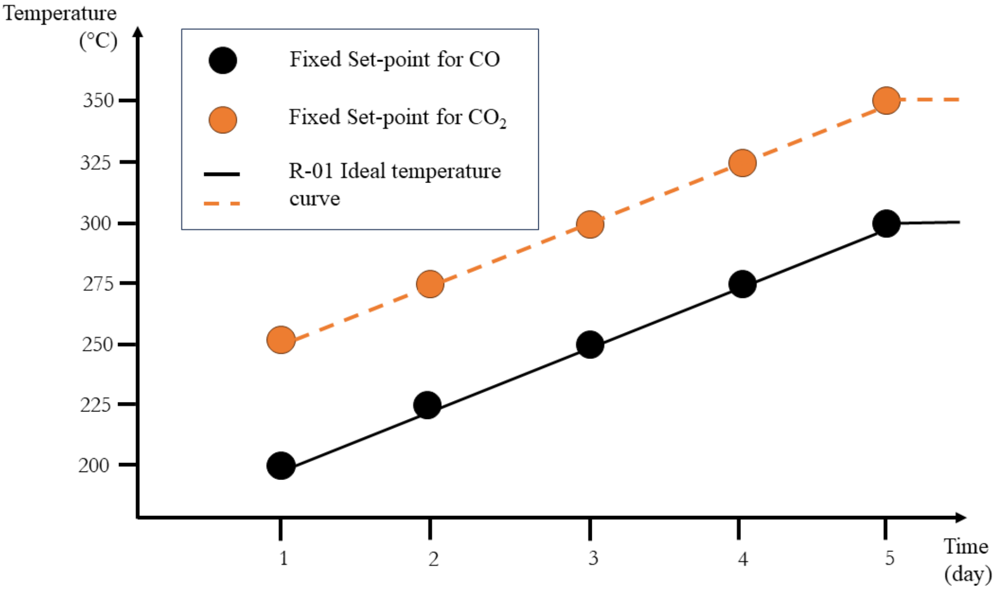


Figure 4.16: *Temperature ramp in R-01 for CO and CO_2.*

The consequences related to this occurrence are reported below and discussed in §4.5.1:

- MORE temperature, i.e., a higher amount of energy and a higher temperature than required, variation in the final composition, loss of the experimental test, higher pressure, possible leakages or ruptures, loss of containment and subsequent release of a flammable/toxic mixture, and damage to the catalyst.
- MORE reaction rate, i.e., a higher temperature, variation in the composition of the reactive mass, loss of the experimental test, increase in the heavy phase, and damage to the catalyst.

The protective layers already present are the hood and valve 10.

Table 4.27: *Existing independent protection layers to manage an incorrect setting of TC-01.*

Initiating event	Frequency (yr^{-1})	IPLs 1 Valve 10 (Rupture disk)	 2 Hood (Passive IPLs)	Intermediate frequency (yr^{-1})	Tolerable frequency (yr^{-1})
Wrong set point of TC-01 (MORE temperature)	1 (26,27)	0.01	0.1	$1{\cdot}10^{-3}$	$1{\cdot}10^{-4}$

The most critical scenario is related to increased pressure and temperature, which are correlated since the mixture is in the gaseous phase. The SIL required to reduce the frequency of this peak event is 1. The possible protection layer is a safety interlock consisting of a temperature sensor connected to the reactor furnace. This sensor detects the temperature inside the reactor, and if the temperature is higher than the safety set-point (such as 400°C), the furnace is shut down.

Table 4.28: *Independent protection layer required to manage an incorrect setting of TC-01.*

Initiating event	Frequency (yr^{-1})	IPLs 1 Safety interlock	 2 Valve 10 (Rupture disk)	 3 Hood (Passive IPLs)	Intermediate frequency (yr^{-1})	Tolerable frequency (yr^{-1})
Wrong set point of TC-01 (MORE temperature)	1	0.1(28)	0.01	0.1	$1{\cdot}10^{-4}$	$1{\cdot}10^{-4}$

---

[26] From Table 4.3 of [51].

[27] From Table G.3 of [34].

[28] From Table 5.13 of [51].

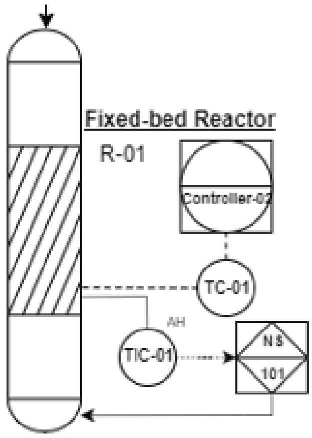


Figure 4.17: *Independent protection layer based on a safety interlock (TIC-01, NS-101). The safety interlock shuts-down the furnace when the temperature measured in R-01 is above 400°C.*

The resulting intermediate frequency is smaller than the tolerable one.

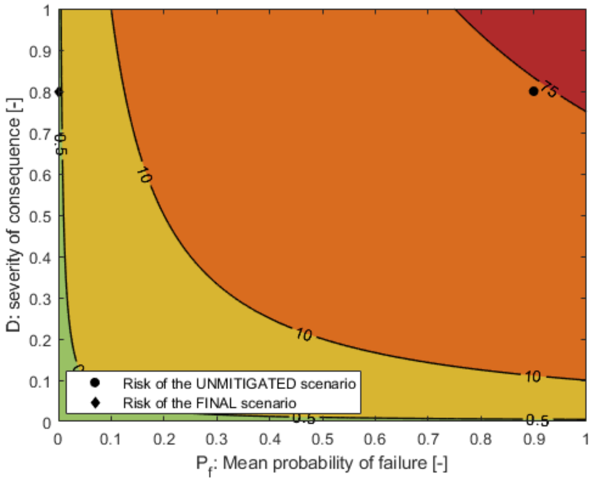


Figure 4.18: *Risk class when the setting of TC-01 is incorrect in Node 2 (D = 5).*

The existing independent protection layer and the addition of the safety interlock results in a *low*-risk classification.

4.5.4.5 Incorrect setting in R-01 and TC-01 during start-up

During the start-up, the temperature inside the reactor increases following a defined temperature ramp (Figure 4.19, Table 4.29).

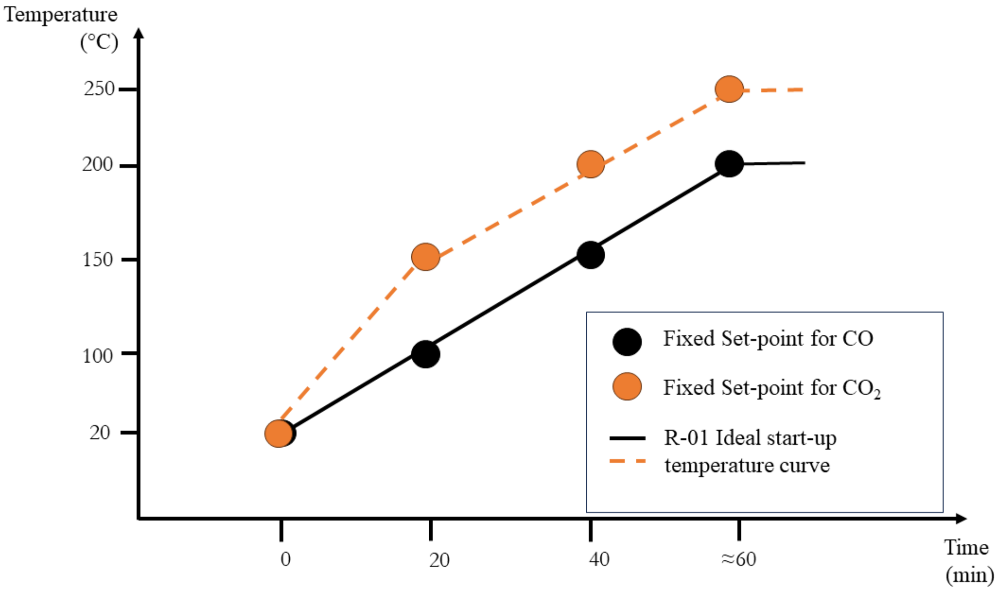


Figure 4.19: *Temperature ramp during the start-up of the reactor (graphical profile).*

Table 4.29: *Temperature ramp during the start-up of the reactor (Table).*

Set point of temperature (CO)	**Set point of temperature (CO$_2$)**	**Duration of the temperature step**
20°C (ambient temperature)	20°C (ambient temperature)	Initial step
100°C	150°C	0
150 °C	200 °C	20 min
200°C	250°C	40 min [29]

The temperature profile is adjusted through a manual operation every week. Provided this time frame, the frequency of setting the wrong temperature set point is set to 1 yr^{-1}.

This occurrence can lead to a deviation of MORE temperature inside the reactor, inducing possible damage to the catalyst (the catalyst loses its structure at temperatures above 400°C), MORE pressure, different product composition and the loss of the experimental test. According to the HAZOP analysis, the safeguards indicated are the following: a hood, a sensor for leakages, a sensor for pressure, and an alarmed high-pressure indicator (PIAH).

---

[29] When the set-point is achieved the operative steady-state condition starts.

Table 4.30: *Independent protection layer required to manage an incorrect setting of TC-01 during the start-up.*

Initiating event	Frequency (yr^{-1})	IPLs 1	IPLs 2	IPLs 3	Intermediate frequency (yr^{-1})	Tolerable frequency (yr^{-1})
		Safety interlock	**Valve 10 (Rupture disk)**	**Hood (Passive IPLs)**		
Set wrong temperature during the start-up (MORE temperature)	1	0.1[30]	0.01	0.1	$1 \cdot 10^{-4}$	$1 \cdot 10^{-4}$

The safety interlock has the same characteristics as the one discussed in §4.5.4.4 (Figure 4.17). The risk of the mitigated event is classified as *low* (Figure 4.18).

4.5.4.6 Failure of R-01 connections

Two primary connections are present on R-01, which could represent a source of leakage. The safeguards include a hood and a sensor for leakages. Only a single protection layer is provided (hood). According to Table 4.31, the resulting intermediate frequency is unacceptably high.

Table 4.31: *Existing independent protection layers to manage potential leakages from R-01 junctions.*

Initiating event	Frequency (yr^{-1})	IPLs 1	Intermediate frequency (yr^{-1})	Tolerable frequency (yr^{-1})
		Hood (Passive IPL)		
Leakages/defective connections (LESS/NO pressure or flow)	1([31])	0.1	$1 \cdot 10^{-1}$	$1 \cdot 10^{-4}$

To achieve the tolerable frequency (10^{-4}), SIL 3 is required (Table 4.32). In this regard, it should be noted that such a SIL performance is pretty high, requiring sophisticated strategies. Moreover, more than one layer of protection can be assigned, provided such layers of protection are independent.

---

[30] From Table 5.13 of [51].

[31] No data are found (conservative approach).

Table 4.32: *Additional independent protection layers required to manage potential leakages from R-01 junctions.*

Initiating event	Frequency (yr^{-1})	IPLs		Intermediate frequency (yr^{-1})	Tolerable frequency (yr^{-1})
		1	2		
		SIL 3	Hood (Passive IPL)		
Leakages/ defective connections (LESS/NO pressure or flow)	1	10^{-3}	0.1	$1 \cdot 10^{-4}$	$1 \cdot 10^{-4}$

A suitable device could be a ratio control loop connected to a high alarm. The ratio control loop consists of two mass flow transmitters arranged across R-01 and connected to a ratio controller. The ratio controller compares the two flow rate signals, and if the ratio is greater than 1.2, the signal is activated, and the operator must initiate an appropriate procedure to shut down the equipment. An increasing differential value measured is indicative of a leakage from the plant section. This control loop should be switched on and off every week, as it must only be active when the process is in continuous operation. In fact, during transients (i.e. start-up and shut-down) can be detrimental.

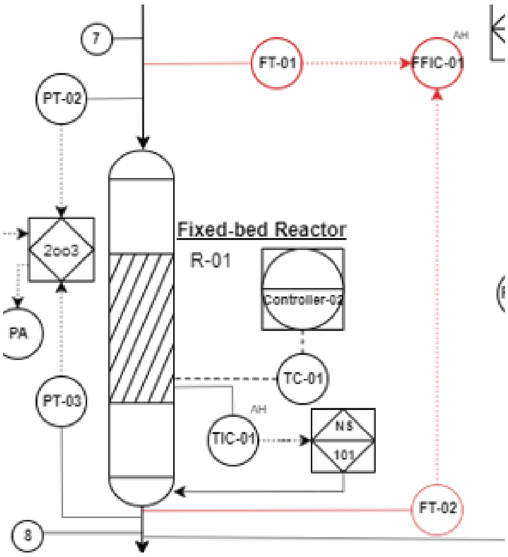


Figure 4.20: *Protection layer based on a ratio controller with a high alarm (FT-01, FT-02, FFIC-01). The alarm is activated when the ratio between the signal from FT-01(mass-flowrate) and the signal from FT-02 (mass-flowrate) is above 1.2.*

According to the proposed features, this control loop and operator response cannot be considered an independent protection layer since the operation is not monitored 24 hours a day. In addition, there could be an additional source of human error when activating the proposed procedure. According to the LOPA approach, the initiating event discussed can not be adequately managed under the current framework, and the resulting frequency is above the tolerability limit (Table 4.31).

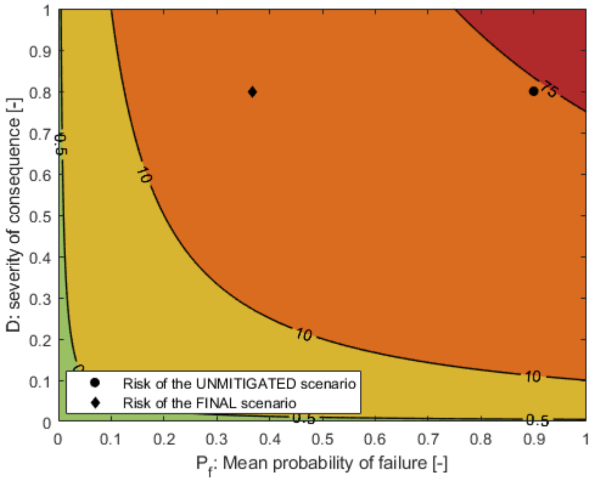


Figure 4.21: *Risk class in the case of the failure of R-01 primary connections in Node 2 (D = 5). According to the LOPA analysis, in the current framework the scenario is still unprotected.*

4.5.4.7 Deviations related to transients of R-01 (start-up or shut-down)

The experimental apparatus is shut down weekly. On that occasion, the reactor is emptied to replace the deactivated catalyst with a new one. The following two hazardous events could result from a human error in performing the requested tasks:

- TOO EARLY reactor opening before the feed is closed. This can lead to a loss of containment with subsequent severe final scenarios, including releasing a flammable or toxic material.
- TOO LATE reactor closure after the feed is opened. Similarly to the previous event, this induces a loss of containment of hazardous materials.

These two events can only be ascribed to a human error. The occurrence frequency is equivalent since the two events are correlated. In addition, both scenarios give a loss of containment, so they are analyzed similarly. According to the HAZOP analysis, possible safeguards include a hood and a sensor system. A single independent protection layer is already provided, i.e., the hood.

Table 4.33: *Existing independent protection layers to manage leakages during transients of R-01 (start-up or shut-down)*

Initiating event	Frequency (yr^{-1})	IPLs 1 Hood (Passive IPL)	Intermediate frequency (yr^{-1})	Tolerable frequency (yr^{-1})
TOO EARLY reactor opening/ TOO LATE reactor closure [32]	1	0.1	$1 \cdot 10^{-1}$	$1 \cdot 10^{-4}$

The resulting RRF is equal to 1000, so a SIL3 is required.

Table 4.34: *Additional independent protection layers to manage leakages during transients of R-01 (start-up or shut-down)*

Initiating event	Frequency (yr^{-1})	IPLs 1 SIL 3	 2 Hood (Passive IPL)	Intermediate frequency (yr^{-1})	Tolerable frequency (yr^{-1})
TOO EARLY reactor opening/ TOO LATE reactor closure	1	10^{-3}	0.1	$1 \cdot 10^{-4}$	$1 \cdot 10^{-4}$

Under the current configuration, it is impractical to add independent protection layers to manage leakages during transient operations. The resulting risk class is equivalent to that reported in Figure 4.21. It should be considered that there are detectors connected to solenoid valves (valves 4) in the same room, which are FC (fail closed) when at least one of the following gases is detected: H_2, CO, CO_2 or CH_4. The detection system can be intended as the sole protection layer able to manage the initiating events under consideration. According to what is stated in §4.5.4, it can not be considered an independent layer of protection.

4.5.4.8 Deviations related to an electrical power outage

When there is a power outage, the process could behave differently than expected. As said in §4.5.2 and §4.5.3.2, when a voltage or power variation is experienced, valves 4 close, and the consequences listed in Table 4.35 can be observed.

---

[32] Too early refers to opening the reactor R-01 without interrupting the feeds to the experimental setup. Too late refers to closing the reactor R-01 after the feeds have been opened.

Table 4.35: *Equipment involved and primary consequences in the case of a power outage.*

Equipment	**Consequences**
Streams: 1.3, 2.3, 3.3	MORE pressure (§4.5.1).
Streams from: 1.4, 2.4 and 3.4	LESS pressure (R-01, E-01, D-01).
Reactor R-01	LESS pressure and temperature: the furnace of R-01 does not work. LESS reaction rate is an associated consequence.
Heat exchanger E-01	LESS pressure and temperature: E-01 does not heat the product mixture. Partial condensation of streams 8, 9, 10, 11 and 12 is an associated consequence. Moreover, a blockage in the piping can be expected. An escalating scenario involves a credible loss of containment.
D-01 (Node 3)	LESS pressure and temperature: the temperature of 5°C is not maintained. Partial condensation of hydrocarbons is an associated consequence (poor separation during an experimental test).

Since one of the possible consequences is the loss of containment, especially when the power outage affects the heat exchanger E-01, the hood can be considered an independent protection layer.

Table 4.36: *Existing independent protection layers to manage a scenario of power outage.*

Initiating event	**Frequency (yr^{-1})**	**IPLs** **1** **Hood (Passive IPL)**	**Intermediate frequency (yr^{-1})**	**Tolerable frequency (yr^{-1})**
Power outage (LESS/NO electric voltage)	1 (33)	0.1	$1 \cdot 10^{-1}$	$1 \cdot 10^{-4}$

The SIL required to decrease the frequency of the initiating event is SIL 3. Therefore a high-performance strategy is required.

Table 4.37: *Additional independent protection layers to manage a scenario of power outage.*

Initiating event	**Frequency (yr^{-1})**	**IPLs** **1** **SIL 3**	**IPLs** **2** **Hood (Passive IPL)**	**Intermediate frequency (yr^{-1})**	**Tolerable frequency (yr^{-1})**
Power outage (LESS/NO electric voltage)	1	0.001	0.1	$1 \cdot 10^{-4}$	$1 \cdot 10^{-4}$

Possible protective layers can include the following:

---

[33] From personal communication with the operators of the pilot plant. Such a scenario has been experienced statistically one time per year.

- Backup utility supplies;
- AutoStart of standby equipment.

These are discussed in Section §3.4.9.

Table 4.38: *Required independent protection layers to manage a scenario of power outage.*

Initiating event	Frequency (yr^{-1})	IPLs			Intermediate frequency (yr^{-1})	Tolerable frequency (yr^{-1})
		1	2	3		
		Backup utility supplies	**AutoStart of standby equipment**	**Hood (Passive IPL)**		
Power outage (LESS/NO electric voltage)	1	0.1 (34)	0.1 (35)	0.1	$1\cdot10^{-3}$	$1\cdot10^{-4}$

The final frequency is higher than the tolerable one, but no additional protection layer can be added. So, the event of a power outage and associated consequences is a partially protected scenario. Further strategies are required, including a variation of the design of the experimental setup.

The final risk class of the scenario, once the proposed independent layers are added, is *low* (Figure 4.22).

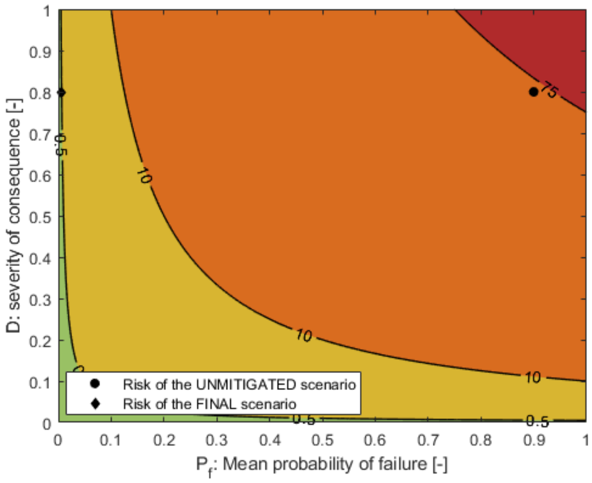


Figure 4.22: *Risk class when there is a power outage in Node 2 (D = 5). According to the LOPA analysis, in the current framework the scenario is still unprotected.*

---

[34] §4.6.12 of [48]

[35] §4.6.4 of [48]

4.5.4.9 Deviations related to catalyst poisoning in R-01

According to the design intent, the reactants fed to the process are pure, so no catalyst poisoning exists. A variation in the feed quality can modify the experimental run by introducing poisonous compounds, including:

- Sulphur: formation of stable sulfuric compounds;
- Phosphorus: formation of stable compounds;
- Halogens: inhibition of active sites (increased danger: iodine, bromine, chlorine, fluorine);
- Heavy hydrocarbons: formation of carbon residues.

Table 4.39 illustrates the classification of the consequences. According to Table 4.39, unacceptable consequences are not expected, and the primary concern is due to the increase of the internal pressure in the experimental equipment. The main effects of introducing poisons in the catalytic reactive system are related to a loss of the experimental test because of an altered composition of the products.

Table 4.39: *Classification of the consequences in the case of catalyst poisoning.*

Classification of consequences	Detail of consequences
Acceptable	AS WELL AS final composition, i.e., altered product mixture. MORE flow rate of gaseous components. Loss of an experimental test.
Undesired	MORE pressure (see §4.5.1)
Unacceptable	-

For the scenario concerning the poisoning of the catalyst, the LOPA analysis is not carried out since the presence of toxic compounds cannot be prevented or managed unless a prior control of the composition of the reactants is carried out (composition of T-01, T-02, T-03, T-04).

4.5.5 Deviations in Node 3: the separation section

Node 3 purpose is to separate the heavy phase from the light phase. The stream from E-01 is made of a gaseous phase where different substances are present: C_2-C_6, water, C_7-C_{30} and incondensable gases (CO, CO_2, H_2 and N_2). Table 4.40 shows which are the usual composition of stream 8 (R-01 outlet stream).

Table 4.40: *Composition of stream 8 according to the design intent. Total flowrate: 40-50 ml/min.*

Component	mol. %	Component	mol. % dry basis
Methane	5	Methane	2
Carbon dioxide	15	Carbon dioxide	41
Water	50	C_2-C_6	17
Hydrocarbons (C_2-C_{30})	30	C_7-C_{30}	40

The light phase is composed of C_2-C_6 and incondensable gases fed to Node 4. The heavy phase condenses inside D-01, consisting of water and C_7-C_{30}.

4.5.5.1 Deviations related to PRC-09

PRC-09 is already analyzed in §4.5.4.3 but is connected to valve 15 of Node 3. If the pressure set point exceeds the intended operating condition, pressure and flow may increase.
The additional independent protection layer designed to manage the outcoming scenario is reported in Table 4.26. An additional protection layer is valve 12, a flanged valve (pressure relief device, §3.4.5) managing the increase in pressure in D-01.

4.5.5.2 Deviations related to PI-02

The comments are similar to those reported in §4.5.4.1.

Table 4.41: *Consequences related to the event of pressure increases due to PI-02 not working properly.*

Deviation	Primary safeguard	Comments
MORE pressure in D-01	Basic process control system (BPCS) of pressure	If PI-02 is not working properly, the actual pressure can be higher than the design intent. A direct consequence is the poor performance of the separation. A redundant pressure indicator is a suggested IPL for managing this deviation.
AS WELL AS product composition (altered outlet composition due to poor separation)	-	A deviation of MORE pressure in D-02 reduces the performance of the separation of stream 12.
Loss of the experimental test	-	-
Leakages or rupture	Sensors for leakages Sensors for pressure Hood	Flammable or toxic materials can be released. If the unprotected frequency is higher than tolerable, additional IPLs are required.
Loss of containment and additional final events		

Considering the deviation of MORE pressure, the existing protection layers are Valve 10, 12 and the hood, respectively. The corresponding mitigation performance on the initiating event frequency is reported in Table 4.42.

Table 4.42: *Independent protection layers required to manage a PI-02 failure.*

Initiating event	**Frequency (yr^{-1})**	**IPLs**			**Intermediate frequency (yr^{-1})**	**Tolerable frequency (yr^{-1})**
		1	**2**	**3**		
		Valve 10 (Rupture disk)	**Valve 12**	**Hood (Passive IPLs)**		
PI-02 fails (MORE pressure)	≈ 1 (36)	0.01	0.01 (37)	0.1	$1 \cdot 10^{-5}$	$1 \cdot 10^{-4}$

As indicated, the actual protection layers are sufficient to manage the event, provided the resulting frequency is lower than the tolerable threshold assigned to the expected consequences class.

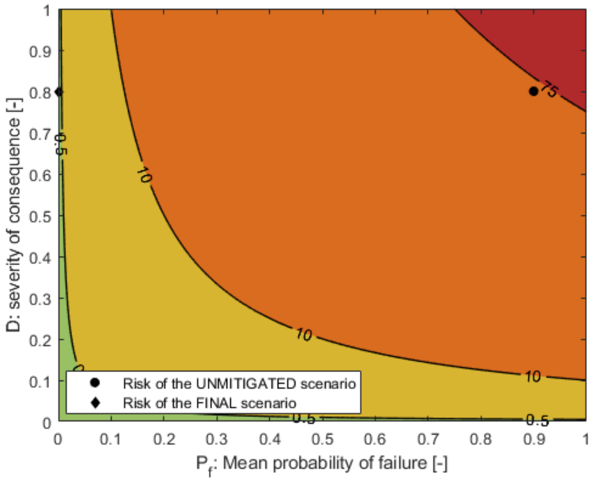


Figure 4.23: *Risk class in the case of an event related to a failure of PI-02 in Node 3 (D = 5).*

The resulting risk class is *low* (Figure 4.23).

4.5.5.3 Deviations related to an electrical power outage

The consequences of a power outage for Node 3 are reported in Table 4.35.

---

(36) Table 11-1 of [65]

(37) Table G.7 of [34]

Table 4.43: *Existing independent protection layers to manage a power outage in Node 3.*

Initiating event	Frequency (yr^{-1})	IPLs 1 Pressure relief device (valve 12)	IPLs 2 Hood (Passive IPLs)	Intermediate frequency (yr^{-1})	Tolerable frequency (yr^{-1})
Power outage (LESS/NO electric voltage)	1	0.01	0.1	$1\cdot10^{-3}$	$1\cdot10^{-4}$

From Table 4.43, the resulting RRF equals 10, so a SIL 1 is required, provided that the existing layers of protection are insufficient to provide the required safety level. Among the possible protective layers, the following are considered (as in §4.5.4.8):

- Backup utility supplies;
- AutoStart of standby equipment.

Table 4.44: *Additional independent protection layers required to manage a power outage in Node 3.*

Initiating event	Frequency (yr^{-1})	IPLs 1 SIL 1	IPLs 2 Valve 12	IPLs 3 Hood (Passive IPLs)	Intermediate frequency (yr^{-1})	Tolerable frequency (yr^{-1})
Power outage (LESS/NO electric voltage)	1	0.1	0.01	0.1	$1\cdot10^{-4}$	$1\cdot10^{-4}$

Table 4.45: *Independent protection layers required to manage a power outage in Node 3*

Initiating event	Frequency (yr^{-1})	IPLs 1 Backup utility supplies	IPLs 2 AutoStart of standby equipment	IPLs 3 Valve 12	IPLs 4 Hood (Passive IPLs)	Intermediate frequency (yr^{-1})	Tolerable frequency (yr^{-1})
Power outage (LESS/NO electric voltage)	1	0.1 (38)	0.1 (39)	0.01	0.1	$1\cdot10^{-5}$	$1\cdot10^{-4}$

---

[38] For further details refer to §4.6.12 of [48].

[39] For further details refer to §4.6.4 of [48].

The final frequency is lower than the tolerable one. The risk class of the mitigated scenario is *low*.

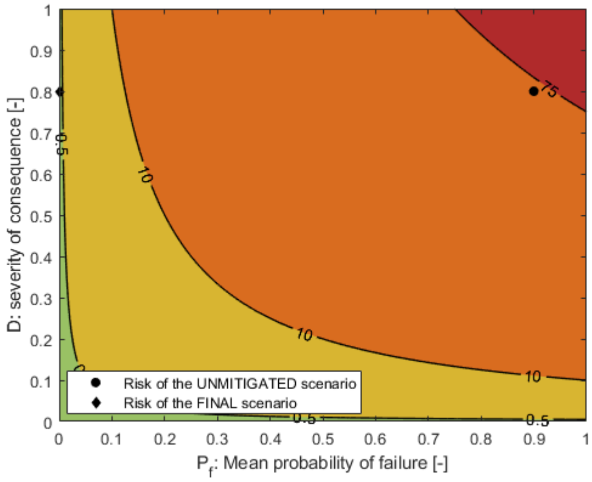


Figure 4.24: *Risk class when there is a power dip (Node 3) (D rank= 5)*

4.5.6 Deviations in Node 4: the analysis of the gaseous phase.

Node 4 purpose is to define the composition of the light phase from the cold trap. The equipment used is a Micro CG, which works under isothermal conditions (60°C), and the time required for the analysis cycle is around 3 minutes.

This node is not related to initial events with a risk classification of A, B or C. Therefore, no LOPA is required, and the scenarios associated with Node 4 are minor.

4.6 Final comments on the protection layers

According to the HAZOP analysis, the experimental setup for Fischer-Tropsch synthesis has been divided into four nodes.

A set of deviations and credible consequences and recommendations have been identified. Moreover, the HAZOP has shown that a specific set of deviations is characterized by a moderate-to-severe risk, requiring proper layers of protection. In the case of risk classes A-C, a subsequent LOPA has been established to quantify the risk reduction target.

Figure 4.25 provides the improvements proposed by the combined HAZOP-LOPA, in which specific sets of IPLs are provided to manage unprotected or insufficiently protected events.

The primary concern is related to a prominent set of manual operations, in which misoperations or errors can lead to relevant deviations in the process parameters. Moreover, releasing material from the apparatus is always an undesired event, even if proper protection layers are already in place.

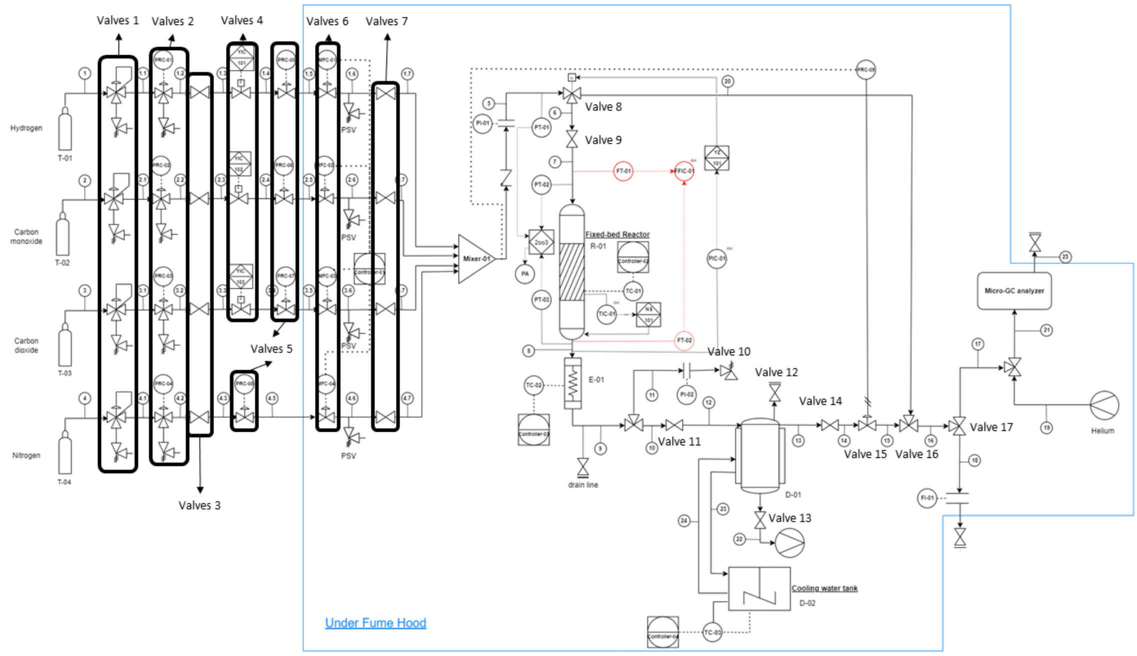


Figure 4.25: *Improved process diagram of the experimental setup following the recommendations emerged from the combination HAZOP-LOPA.*

Table 4.46: *Additional equipment, systems and layers of protection required for the experimental setup.*

Additional components	**Notes**
Pressure safety valves (PSVs) between valves 6 and 7	The scenario managed concerns the pressure increase after valves 5.
2oo3 redundant scheme of PI-01/02	This accommodates a SIL 3 requirement for managing failures of the pressure indicators. The strategy is also helpful in avoiding manual misoperations induced by a hardware error in indicating the pressure to the operator.
TIC-01 interlocked	This architecture shuts down the furnace if the temperature in R-01 is above the safe threshold (400°C).
PIC-01 automatic pressure control	This automatic control loop acts when the pressure in stream 8 is above the threshold (> 20% of the operating pressure). Valve 8 changes direction from stream 6 to stream 20 (bypass line)
FFIC-01 ratio control	This control cannot be considered as an IPL. It compares the two signals from FT-01 and FT-02, which measures the mass flowrate respectively before and after R-01. When the ratio between the two signals is above 1.2, the alarm starts.
Drain line	The drain line is essential to remove liquid residues in stream 9.
NRV in stream 5	The non-return valve avoids reverse flow downstream of the mixing of reactants.

The main modifications on the experimental setup, driven by the structured quantitative risk assessment, are listed in Table 4.46.

As there are multiple connections and valves in the system, an additional consideration can be made for leaks. When leaks occur, a difference in mass flow rates can be observed. This difference in flow rates cannot be considered across reactor R-01 since volumetric data can change due to chemical reactions. Figure 4.26 shows an option for arranging the flow indicators (FI) in Node 2. If the coupled flow rates measured in 1-2 or 3-4 are significantly different, a leakage can be expected in the monitored section. Periodic soapy testing along the piping and periodic inspection of seals, gaskets, and joints should be performed to avoid potential sources of leakage.

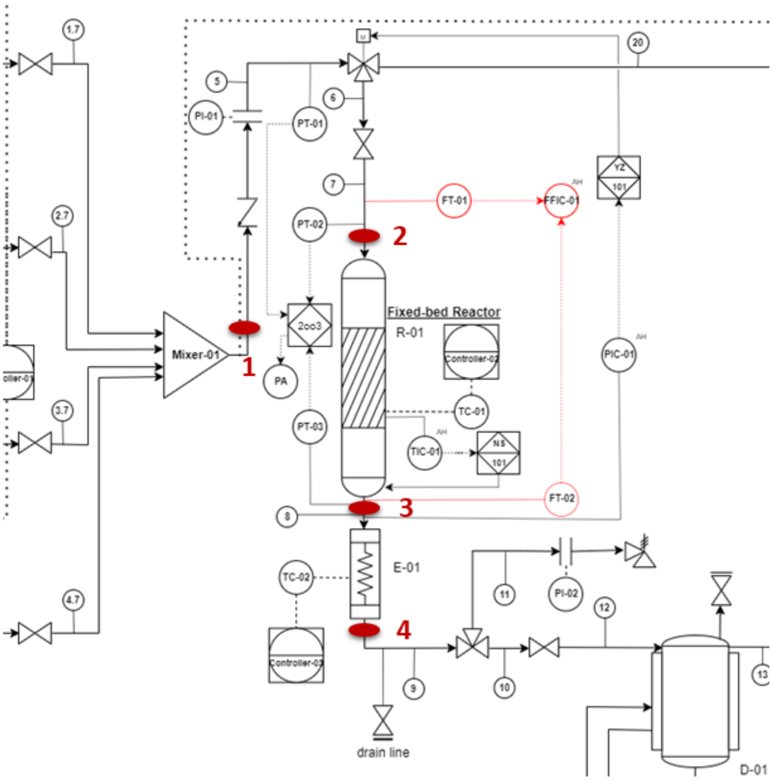


Figure 4.26: *Arrangement of mass flow indicators (FIs) to detect eventual leakage occurring in node 2. A relevant variation of data provided by the sensors is representative of leakages affecting the monitored sections of the experimental setup.*

Finally, the numbering of the valves and, more generally, of the equipment should be updated to avoid mistakes due to the non-unique labeling of process equipment.

Conclusions

This work discussed safety engineering and management in an academic environment, specifically in relation to the risk assessment of an experimental setup used for Fischer-Tropsch synthesis. Due to the unique nature of experimental setups and academic settings, a combined Hazard and Operability Analysis (HAZOP) and Layers of Protection Analysis (LOPA) were implemented. This allowed for the inclusion of specific features that characterize these frameworks, such as the impact of manual procedures and transient operations.

The first section of the work focused on the analysis of the frameworks while discussing accident statistics and the leading factors that contribute to hazards and risks in pilot plants and academic settings.

The experimental setup used for Fischer-Tropsch synthesis was then analyzed in terms of operability issues through a structured HAZOP analysis. High-risk deviations and related scenarios were identified, some of which were not sufficiently protected against the associated consequences. The Fischer-Tropsch reactor and the feeding section were identified as the most critical nodes, in relation to which different manual procedures were expected.

A subsequent LOPA analysis was conducted, which allowed for the identification of proper preventive and mitigative strategies while assessing the features of protection layers, both automatic and human-action-based. Recommended measures included the automation of the experimental setup, embedding safety interlocks and devices, automatic control loops, and redundant schemes. Special attention was given to the impact of manual operations and settings on the establishment of hazardous or risk scenarios and specific hazardous frameworks that may be present in experimental apparatus like that analyzed. Unlike usual risk assessment approaches, the presence of laboratory infrastructures and equipment (e.g. hood, ventilation, and procedures) was included when assessing the functionality of specific risk reduction measures.

Appendix

A.1 Instrumented diagram of the experimental setup

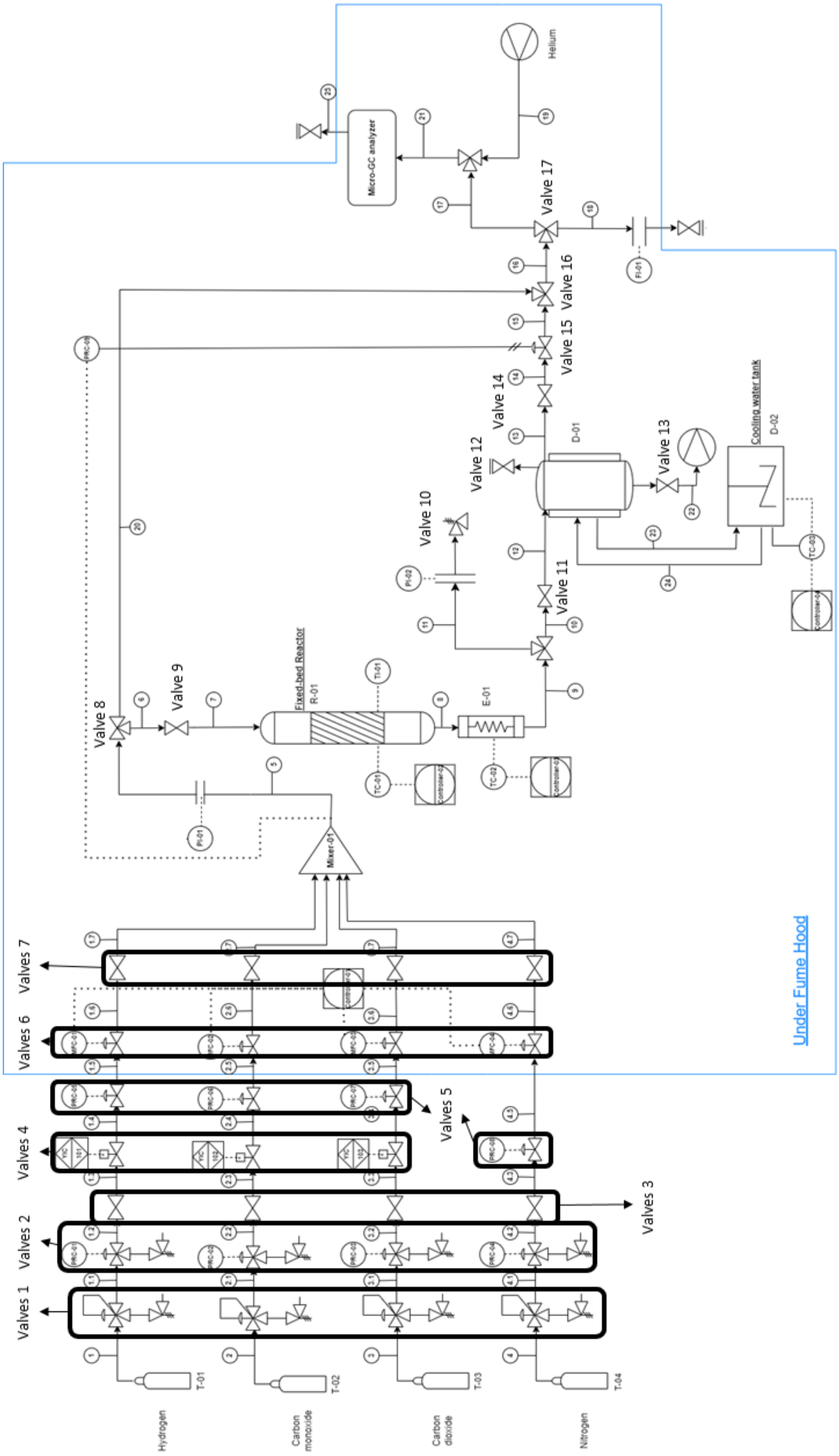


Figure A.1.1: *Instrumented diagram of FT pilot plant with details on the valve systems.*

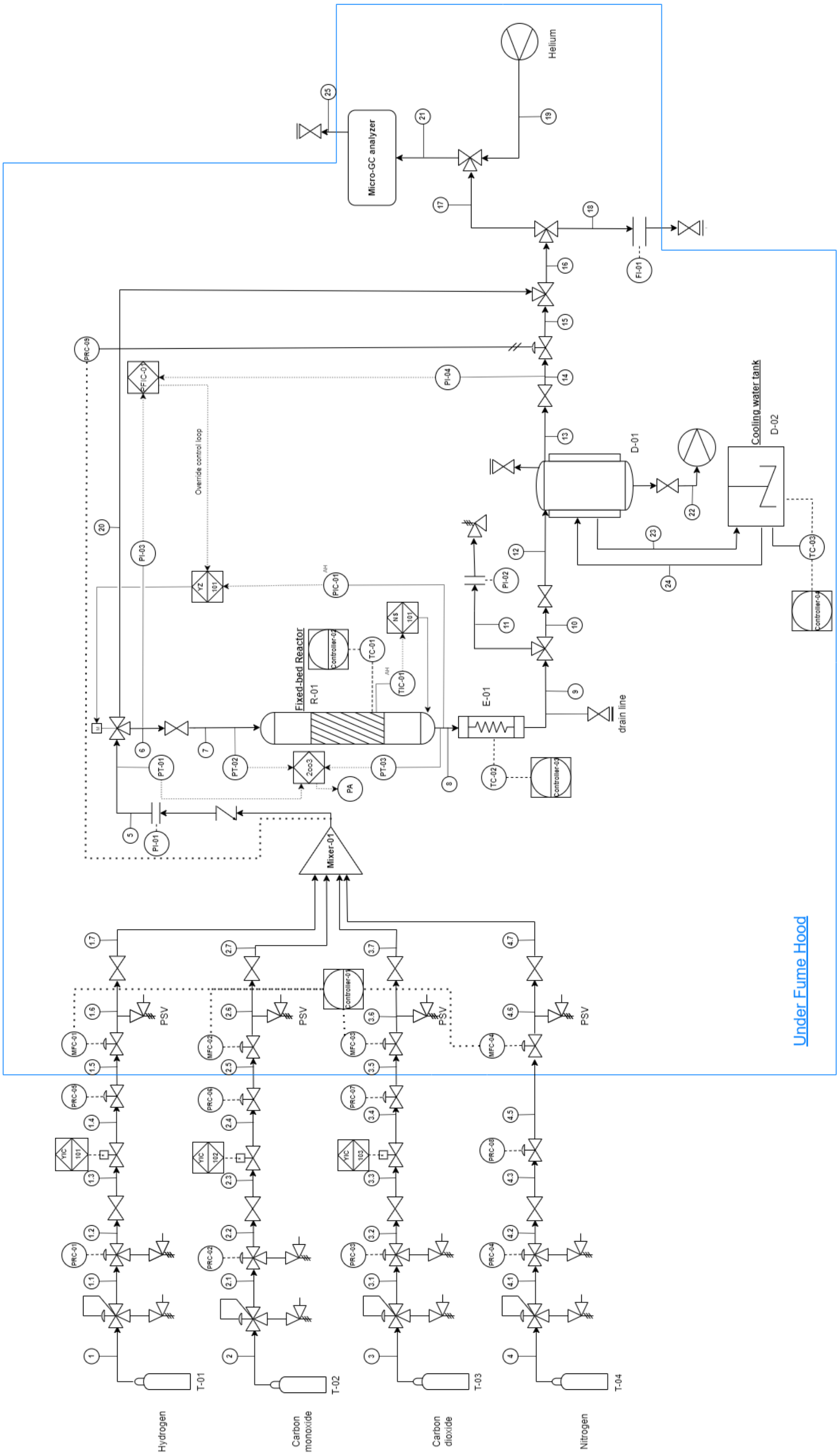


Figure A.1.2: *Instrumented diagram of FT pilot plant*

A.2 Specifications of the valves used in the experimental setup

Table A.2.1: *List and specifications of the valves.*

Valve	Description	Fail open (FO) or Fail close (FC)	Number of times the valve is touched (month^{-1})
01	Self-regulating valve and pressure safety valve with the function of avoiding the MAWP. Safety valve size: 6 x 3 cm (length x width)	FC	0
02	Control valve (PRC and three-way) and pressure safety valve with the function of decreasing the pressure from 180 to 40 bar and avoiding the MAWP. Safety valve size: 7 x 3 cm (length x width)	FC	0
03	Ball-valve (open manual isolation valve) with the function of isolation	FC	0
04	Solenoid valve (with a gas detection system) with the function of shutting off the plant in the case of a leakage	FC	0
05	Pressure regulator (control valve with PRC), i.e. pressure reduction from 40 to 5-10 bar	FC	1
06	Mass flow meter (control valve with MFC), with the function of realizing the correct composition in Mixer-01	FC	5
07	Open-close valve with the function of isolation	FC	5
08	Three-way valve (open manual isolation valve) with the function of isolation	FC	1
09	Open manual isolation valve with the function of isolation	FC	10
After E-01 (three-way valve)	It is a tee junction serving the safety valve 10	-	0
10	Pressure relief valve working at 51.7 bar Size: 2.5 x 2 cm (length x width)	Rupture disk valve	0
11	Open manual isolation valve with the function of isolation	FC	10
12	Nupro gas shut-off valves with the function of relief	FC	0
13	Nupro gas shut-off valves with the function of sampling	FC	5
14	Open manual isolation valve with the function of isolation	FC	10
15	Back pressure regulator valve with the function of pressure regulation	FC	0
16-17	Three-way valve and open manual isolation valve, i.e. a tee junction and a valve driving to the analyzer section	FC	10
After the rotameter	Flanged valve with the function of relief (out of the hood)	FC	0
Before GC	Three-way valve with the function of isolating the analyzer section	FC	20
After GC	Flanged valve with the function of relief (out of the hood)	FC	0

A.3 Main equipment of the experimental setup

Table A.3.1: *Main equipment of the experimental setup.*

Equipment	Description
Pipes	Material: SS316 MAWP [40]: 80 bar
H_2 Detector	Valve-04 communicates with the gas detector Detection range: 0-100% LFL Alarm: 10% max detection value
CO Detector	Valve-04 communicates with the gas detector Detection range: 0-500 ppm Alarm: 10% max detection value
CO_2 Detector	Valve-04 communicates with the gas detector. Detection range: 0-500 ppm Alarm: 10% max detection value
CH_4 Detector	Valve-04 communicates with the gas detector. Detection range: 0-100%LFL Alarm: 10% max detection value
H_2 Mass flow meter	Product: Mass flow meter SLA5860 Manufacturer: Brooks instruments Flow range: 0.003-50 slpm P max: 1500 psi/103 bar Accuracy: ± 0.6% of SP T limits: 0-65°C Seal material: elastomeric Wetted parts: SS with Viton
CO Mass flow meter	Product: Mass flow meter SLA5860 Manufacturer: Brooks instruments Flow range: 0.003-50 slpm P max: 1500 psi/103 bar Accuracy: ± 0.6% of SP T limits: 0-65°C Seal material: elastomeric Wetted parts: SS with Viton
CO_2 Mass flow meter	Product: Mass flow meter SLA5860 Manufacturer: Brooks instruments Flow range: 0.003-50 slpm P max: 1500 psi/103 bar Accuracy: ± 0.6% of SP T limits: 0-65°C Seal material: elastomeric Wetted parts: SS with Viton

---

[40] Maximum allowable working pressure.

N_2 Mass flow meter	Product: Mass flow meter SLA5860 Manufacturer: Brooks instruments Flow range: 0.003-50 slpm P max: 1500 psi/103 bar Accuracy: ± 0.6% of SP T limits: 0-65°C Seal material: elastomeric Wetted parts: SS with Viton
Flow input controller (Controller-01A): CO_2	Gas and liquid mass flow secondary electronics Controller 0254 Manufacturer: Brooks instruments Power input: Voltage: 12-24 Vdc required, -15 Vdc permitted Current: 400 mA max current per channel Instrument power draw: 0.8 Watts Power Output: +15V/2.0 A, -15 V/1.0 A or 12-24 Vdc/2.0 A Signal Input/Output: 0(1)-5 V, 0(2)-10 V, 0(4)-20 mA Operating T: 0-50°C, 0-95% non-condensing
Flow input controller (Controller-01B): H_2, CO, N_2	Gas and liquid mass flow secondary electronics Controller 0154 Manufacturer: Brooks instruments Power Input: 0-260 Vac, 50/60 Hz 70 W Power Output: +15V/2.9 A, -15 V /1.4 A max or 24 Vdc/2.5 A max Signal Input/Output: 0(1)-5 V, 0(4)-20 mA Operating T: 0-50°C
Mixer (Mixer-01)	Mixing chamber up to 4 gaseous Material: SS 316
Pressure indicator (PI-01)	Differential Bourdon manometer Manufacturer: Tagliabue manometri Material: 304 SS T max: 100°C Degree of protection: IP65 Operating pressure: max 90% of full-scale value
Reactor furnace (R-01)	Tubular wired heating furnace Manufacturer: Fornomab Srl T max: 900°C Power: 900 Watt Electric potential: 230 V
Temperature indicator and temperature controller of reactor furnace (respectively: TI-01 and TC-01)	P108- Temperature/ Process Controllers, Temperature indicator Manufacturer: Eurotherm ltd Operating temperature: 0 to 55°C 24 V ac/dc supply voltage Sample rate: 4 Hz (250 ms) Protection class: IP66, IP65 Coupled with two K-type thermocouples

Electric heater (E-01)	Wired electric heater Manufacturer: Colaver srl Material: fiberglass
Temperature controller of electric heater (TC-02)	-
Pressure indicator (PI-02)	Pressure gauge ind PGI-63B Manufacturer: Swagelok Material: SS316 T max: 60°C P min: 0 bar P max: 60 bar T min: -40°C Lens gasket: Buna N
Cold trap (D-01)	Flanged cooling jacket reservoir Manufacturer: Sofferia Sestese Material: SS316 V: 192 ml Equipped with valve 12 and 13 and flanged via 4 screws
Water tank (D-02)	CRIOTERM 190 ISCO Manufacturer: ISCO Material: Aluminium
Temperature controller (TC-03)	ISCO GTR 90 Manufacturer: ISCO T range: -9.9°C to +104.9°C Heating power: 1.05 kW to 230 V Pump capacity: 1.7 m Pump flow: 8 l/min Temperature stability: 0.05°C
Bubble flow-meter: rotameter (F-01)	Material: glass Capacity: 120 ml Tightness: O-ring Junction with the plant through a plastic tube clamped on the joints
Micro-GC	Micro-GC 3000 A Manufacturer: Agilent

A.4 Operative conditions of the experimental setup

Table A.4.1: *Operative conditions of the experimental setup according to the design intent.*

Part of the plant	Operative conditions
T-01, T-02, T-03, T-04	Gas cylinders: respectively H_2, CO, CO_2, N_2 P =180 bar Sizes (each, G2 classified cylinder tank): 10.2 m^3 T = ambient
Gas detectors	Respectively: H_2, CO, CO_2, CH_4 Detection range H_2: 0-LEL ppm (LEL: 4%) Detection range CO: 0-500 ppm (LEL: 12%) Detection range CO_2: 0-500 ppm (IDLH: 40000 ppm) Detection range CH_4: 0-LEL ppm (LEL: 5%) Alert sound (for all the detectors): 10% of the maximum detection range value
PRC-01, PRC-02, PRC-03, PRC-04	Pressure control from 180 bar to 40 bar
PRC-05, PRC-06, PRC-07, PRC-08	Pressure control from 40 bar to 5-10 bar
MFC-01, MFC-02, MFC-03, MFC-04	The MFCs are connected to controller-01, which has a panel control where the operator sets the fluxes of each substance. The total flux is equal to 50 ml. 1. $H_2/CO/N_2$: 30/15/5 ml/min ($H_2/CO=2$) 2. $H_2/CO_2/N_2$: 30/10/5 ml/min ($H_2/CO_2=3$)
Mixer	All the streams are mixed
PI-01, PRC-09	The line works under P =20 bar
Reactor	The reactor is made of (external) stainless steel, (internal) unknown (probably ceramic fiber) Temperatures: 1. With CO: 200-300°C @ 20 bar 2. With CO_2: 250-350°C @ 20 bar A ramp is applied starting from the lowest temperature reported (respectively 200 and 250°C) for day one. On the following days, 25°C/day are added to obtain the final temperature during the 5th day (Figures A.4.1-2) The furnace of the reactor is electrical.
TC-01, TI-01, Controller-02	TI-01 is a thermocouple, and the signal received by Controller-02 coupled with TC-01 that governs the reactor temperature The reactor SP temperature is manually set on a daily basis
E-01	Wired electric heater made of fiberglass T=60÷80°C The main purpose is to maintain the products in the gas phase
TC-02, Controller-03	The temperature is indirectly set by an operator, acting on the power of E-01 through Controller-03 The controller sends a signal to TC-02 in order to obtain a temperature within 60-80°C
PI-02	Pressure gauge. P = 20 bar.
D-01: Cold trap	Flanged cooling jacket reservoir. T = 5°C.
D-02: Cooling water tank (cryostat)	The water used in D-01 is cooled down with CFC

TC-03, Controller-04	The temperature is set manually to 5°C, and the controller sends a signal to TC-03
FI-01	The bubble flowmeter is made of glass and the junction with the plant is through a plastic tube To obtain an adequate flow to the GC
Micro-GC	Carrier: Helium T is set equal to 60°C P is equal to 20 psi Analysis time is 2-3 minutes The analysis is automatic

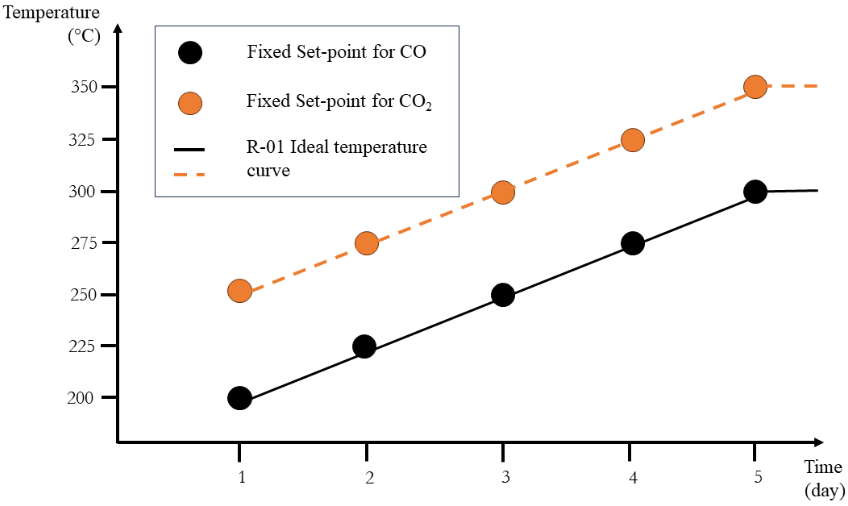


Figure A.4.1: *Temperature ramp in R-01 when CO or CO$_2$ are used as feed.*

Table A.4.2: *Procedures for start-up and shut-down*

Shut-down basic procedure	Start-up basic procedure
Decrease the temperature inside the reactor (Controller-02) in order to obtain an ambient temperature (20°C) (this step requires almost 2 hours). Close input valves (valves 07) of the reactants (this step can be done when the temperature inside the reactor is 20°C). Set to 0 the volume flow rate of Controller-01. Decrease the pressure (in PRC-09) in order to guarantee atmospheric conditions in the experimental setup.	Open input valves (valves 07). Set volume flow rates at Controller-01. Set the operative pressure at PRC-09. Increase the temperature of the reactor (Controller-02) according to three different steps (as a ramp): 20-150°C; 150-200°C; 200°C- operative temperature.

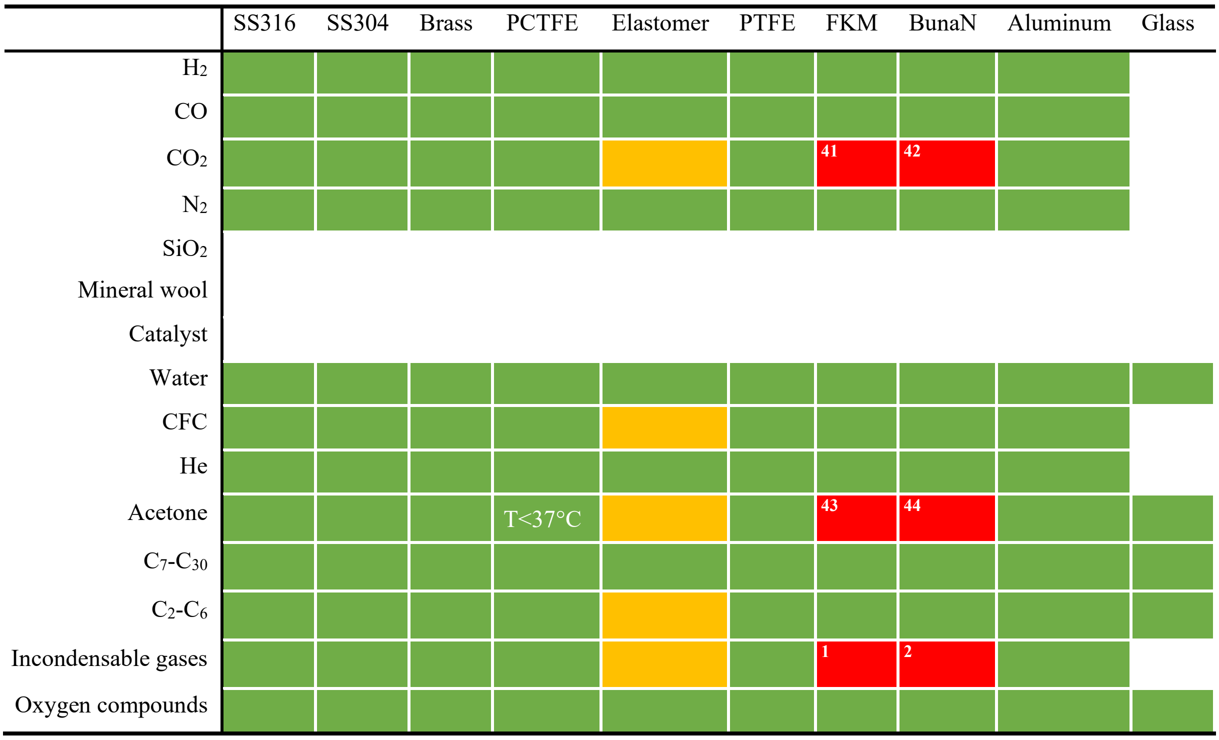
A.5 Chemicals used or produced while operating the process

Table A.5.1: *Chemicals used or involved while operating the process.*

Classification	**Substance**	**Section involved**
Reactants	Hydrogen Carbon monoxide Carbon dioxide	Feeding Mixer R-01 E-01 D-01 Micro-GC
Inert	Nitrogen	Feeding Mixer R-01 E-01 D-01 Micro-GC
	SiO_2 Mineral wool	R-01
Catalyst	Iron-based Mg-Cu-**Fe**-K, Mg-Cu-Co-**Fe**-K, Zn-Cu-**Fe**	R-01
Utilities	Water	D-01 D-02
	Electricity	Feeding Mixer R-01 E-01 D-01 D-02 Micro-GC
	CFC (with F)	D-01 D-02
	Helium	Micro-GC
	Acetone	R-01 D-01
Contaminants	-	-
Products	Heavy phase: C_7-C_{30} Light gaseous phase: C_2-C_6 Oxygen compounds: long-chain alcohols	R-01 E-01 D-01
	Incondensable gases: CO, H_2, CO_2, CH_4	R-01 E-01 D-01 Micro-GC

A.6 Interaction matrix: chemicals and materials

Table A.6.1: *Interaction matrix between chemicals and materials.*



	SS316	SS304	Brass	PCTFE	Elastomer	PTFE	FKM	BunaN	Aluminum	Glass
H_2	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	
CO	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	
CO_2	🟩	🟩	🟩	🟩	🟨	🟩	🟥[41]	🟥[42]	🟩	
N_2	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	
SiO_2										
Mineral wool										
Catalyst										
Water	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
CFC	🟩	🟩	🟩	🟩	🟨	🟩	🟩	🟩	🟩	
He	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	
Acetone	🟩	🟩	🟩	🟩 T<37°C	🟨	🟩	🟥[43]	🟥[44]	🟩	🟩
C_7-C_{30}	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
C_2-C_6	🟩	🟩	🟩	🟩	🟨	🟩	🟩	🟩	🟩	🟩
Incondensable gases	🟩	🟩	🟩	🟩	🟨	🟩	🟥 1	🟥 2	🟩	
Oxygen compounds	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩

Legend:

🟩 Compatible
🟨 Can be compatible, depending on the elastomeric material used
Unknown/no data
🟥 Not compatible

---

[41] Not compatible: N (not compatible for use under normal service conditions), S (swelling), M (change of mechanical properties) .

[42] Not compatible: N (not compatible for use under normal service conditions), S (swelling), M (change of mechanical properties).

[43] Probably incompatible.

[44] Not compatible.

A.7 Interaction matrix: chemicals

Table A.7.1: *Interaction matrix among chemicals.*

	H_2	CO	CO_2	N_2	SiO_2	Mineral wool	Catalyst	Water	CFC	He	Acetone	C_2-C_6	C_7-C_{30}	O_2 compounds	Incondensable gases	High T	High P	Environment
Catalyst	⬛	⬛	⬛	⬛	⬛	⬛	🟩 *	🟥 [45][45]	🟥 [69][46]	🟨 [45][47]	🟨 [45][48]	🟩 [70]	🟩 [70]	🟨 *	🟩 *	🟩	🟨 [49]	🟩
Mineral wool	⬛	⬛	⬛	⬛	⬛	🟩 *	🟩 *	🟩 *	🟩 *	🟩 *	🟩 *	🟩 *	🟩 *	🟩 *	🟩 *	🟩	🟩 *	🟩
SiO_2	⬛	⬛	⬛	⬛	🟩 *	🟩 *	🟨 [71]	🟨 [72][50]	🟩 [73]	🟩 *	🟩	🟩 *	🟩 *	🟩 *	🟩 *	🟩	🟩	🟥 [51]
N_2	⬛	⬛	⬛	🟩 *	🟩 *	🟩 *	🟨 [45][47]	🟩 *	🟩	🟩 *	🟩	🟩	🟩 *	🟩 *	🟩 *	🟩	🟩	🟥 [52]
CO_2	⬛	⬛	🟩 *	🟩 *	🟩 [74]	🟩 *	🟨 [45][47]	🟥 [75][53]	🟩 *	🟩 *	🟩	🟩 *	🟩 *	🟩 *	🟩 *	🟩	🟩	🟥 [54]
CO	⬛	🟩 *	🟩 *	🟩 *	🟩 *	🟩 *	🟥 [45][55]	🟥 [76][77][56]	🟩 *	🟩 *	🟩	🟩 *	🟩 *[57]	🟩 *	🟩 *	🟨	🟩	🟥 [58]
H_2	🟩 *	🟩 [78]	🟩 [78]	🟨 [79][59]	🟩 [80]	🟩 *	🟥 [45][55]	🟥 [77][60]	🟨 [73][61]	🟩 *	🟩	🟩 *	🟩 *[62]	🟩 *	🟩 *	🟥 [81][63]	🟥 [64]	🟥 [65]

---

[45] Reaction products may be flammable. The reaction generates gaseous products and may cause pressurization. Exothermic reaction and the products may be toxic.

[46] Possible CFC degradation. Reaction products may be corrosive. The reaction generates gaseous products (which could be toxic) and may cause pressurization. Exothermic reaction at ambient temperature. The reaction may be particularly intense, violent or explosive.

[47] Reaction products may be flammable. Exothermic reaction at ambient temperatures (releases heat)

[48] Reaction products may be flammable. Reaction liberates gaseous products and may cause pressurization. Exothermic reaction at ambient temperatures (releases heat)

[49] Pyrophoric material.

[50] H_2SiO_3 formation.

[51] If silica is present as powder.

[52] Possible problem related to asphyxiation.

[53] H_2CO_3 formation.

[54] Toxic material.

[55] Reaction products may be flammable. Exothermic reaction at ambient temperatures (releases heat). Reaction products may be unstable above ambient temperatures. Reaction may be particularly intense, violent, or explosive.

[56] CO is highly flammable in contact with water and air, Water Gas Shift reactions.

[57] Possible CO addition in order with Fischer Tropsch synthesis.

[58] Flammable and toxic material.

[59] NH_3 formation: if the pressure increases (above 100 bar).

[60] H_2 is highly flammable in contact with water and air.

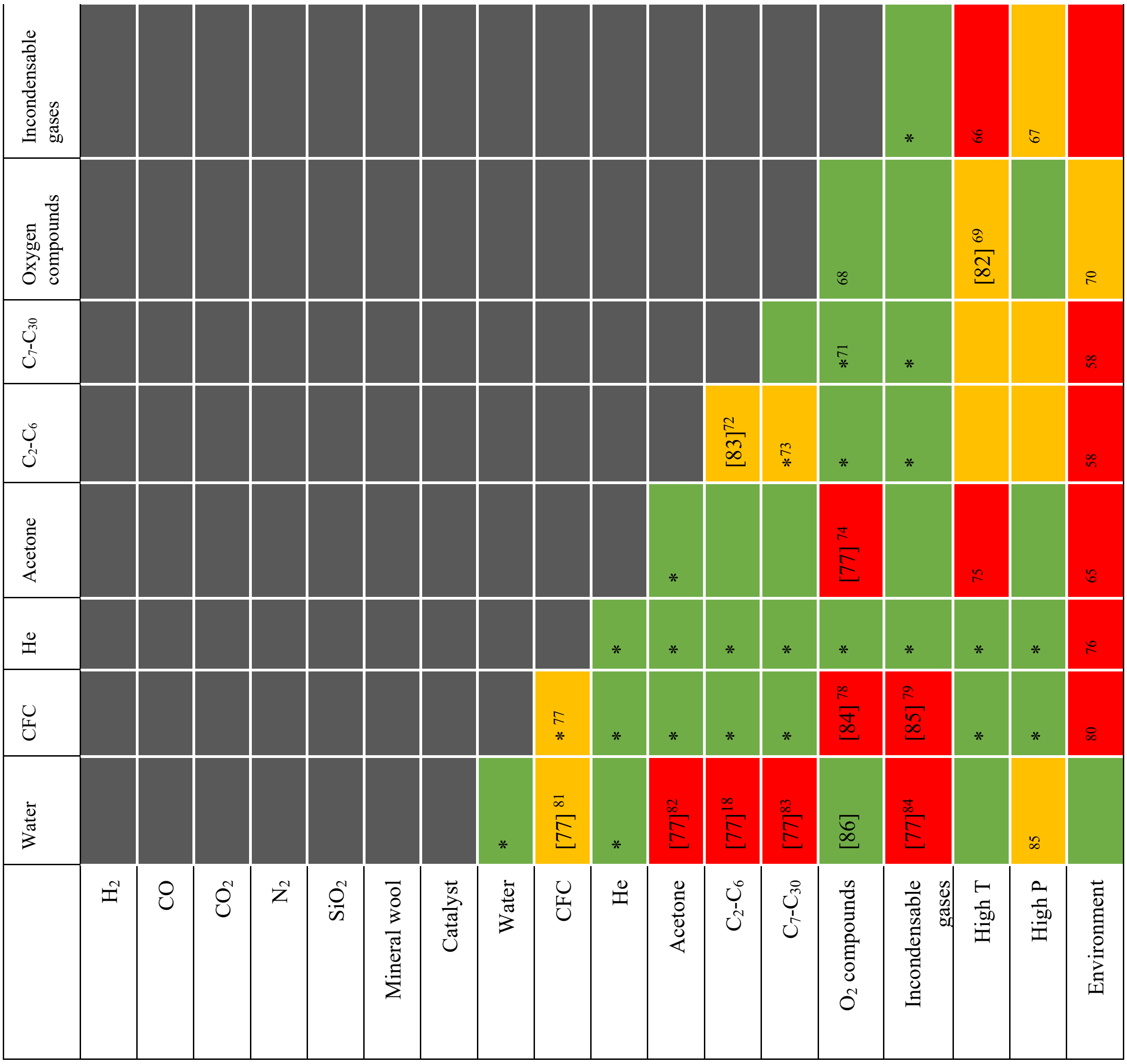
[61] Possible hydrochlorination and dimerization (operative condition unknown).

[62] Saturation of the double bond (if there is any double bond).

[63] HTHA (high-temperature hydrogen attack).

[64] Embrittlement.

[65] Flammable material.



	Water	CFC	He	Acetone	C_2-C_6	C_7-C_{30}	Oxygen compounds	Incondensable gases
H_2	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛
CO	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛
CO_2	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛
N_2	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛
SiO_2	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛
Mineral wool	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛
Catalyst	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛
Water	🟩 *	⬛	⬛	⬛	⬛	⬛	⬛	⬛
CFC	🟨 [77] [81]	🟨 * [77]	⬛	⬛	⬛	⬛	⬛	⬛
He	🟩 *	🟩 *	🟩 *	⬛	⬛	⬛	⬛	⬛
Acetone	🟥 [77][82]	🟩 *	🟩 *	🟩 *	⬛	⬛	⬛	⬛
C_2-C_6	🟥 [77][18]	🟩 *	🟩 *	🟩	🟨 [83][72]	⬛	⬛	⬛
C_7-C_{30}	🟥 [77][83]	🟩 *	🟩 *	🟩	🟨 *[73]	🟩	⬛	⬛
O_2 compounds	🟩 [86]	🟥 [84] [78]	🟩 *	🟥 [77] [74]	🟩 *	🟩 *[71]	🟩 [68]	⬛
Incondensable gases	🟥 [77][84]	🟥 [85] [79]	🟩 *	🟩	🟩 *	🟩 *	🟩	🟩 *
High T	🟩	🟩 *	🟩 *	🟥 [75]	🟨	🟨	🟨 [82] [69]	🟥 [66]
High P	🟨 [85]	🟩 *	🟩 *	🟩	🟨	🟨	🟩	🟨 [67]
Environment	🟩	🟥 [80]	🟥 [76]	🟥 [65]	🟥 [58]	🟥 [58]	🟨 [70]	🟥

---

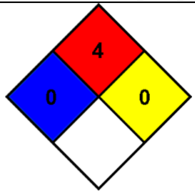
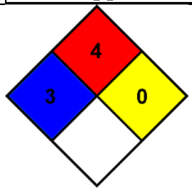
[66] Flammable gases.
[67] Possible material stresses.
[68] Aldehydes, alkenes, -COOH formation.
[69] Possible thermal composition.
[70] Possible health problems related to alcohol dispersion.
[71] Ether formation.
[72] Possible polymerization.
[73] Possible polymerization.
[74] Acetone with Ethanol can burn with an invisible flame.
[75] Acetone decomposition.
[76] Problems related to asphyxiation.
[77] Possible F_2 formation.
[78] HF formation.
[79] HCl formation.
[80] Health problems related to CFC dispersion.
[81] It could be flammable (type of CFC is unknown)
[82] Highly flammable.
[83] Highly flammable.
[84] Highly flammable mixture. Steam reforming reactions can occur.
[85] Possible material stresses.

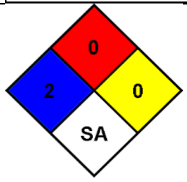
Legend of Table A.7.1:

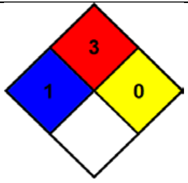
🟩	Compatible
🟩 *	Probably compatible (no data available)
🟨	Probably not compatible
🟨 *	Probably not compatible (no data available)
🟥	Not compatible

A.8 Properties of hazardous chemicals ([77][87])

TableA.8.1: *Hazardous properties of materials.*

<table>
<tr><th>Chemical</th><th>Hazardous properties</th></tr>
<tr><td>*Hydrogen* [87]</td><td>
Flammable Gas
LEL: 4.1
UEL: 74.2%
Autoignition T: 400°C
Melting point: -259.18°C
Boiling point: -252.8°C
IDLH: -
AEGLs (Acute Exposure Guideline Levels): -
PACs (Protective Action Criteria): Hydrogen (1333-74-0)[12]
<table>
<tr><th>PAC-1</th><th>PAC-2</th><th>PAC-3</th><th>LEL</th></tr>
<tr><td>65000 ppm</td><td>230000 ppm</td><td>400000 ppm</td><td>40000 ppm</td></tr>
</table></td></tr>
<tr><td>*Carbon monoxide* [77][87]</td><td>
Flammable Gas; Poison Gas
LEL: 12.5%
UEL: 74.2%
Autoignition T: 608.9°C
Melting point: -213°C
Boiling point: -190°C
Water Solubility: 2%
Vapor pressure: >35 atm
IDLH: 1200 ppm
LCLo (ihl-man): 4000 ppm/ 30M
LC50 (ihl-rat): 1807 ppm/4H
AEGLs (Acute Exposure Guideline Levels):
<table>
<tr><th>Exposure period</th><th>AEGL-1</th><th>AEGL-2</th><th>AEGL-3</th></tr>
<tr><td>10 min</td><td>NR</td><td>420 ppm</td><td>1700 ppm</td></tr>
<tr><td>30 min</td><td>NR</td><td>150 ppm</td><td>600 ppm</td></tr>
<tr><td>60 min</td><td>NR</td><td>83 ppm</td><td>330 ppm</td></tr>
<tr><td>4 hours</td><td>NR</td><td>33 ppm</td><td>150 ppm</td></tr>
<tr><td>8 hours</td><td>NR</td><td>27 ppm</td><td>130 ppm</td></tr>
</table>
NR= not recommended

PACs (Protective Action Criteria): Carbon monoxide (630-08-0)
<table>
<tr><th>PAC-1</th><th>PAC-2</th><th>PAC-3</th><th>LEL</th></tr>
<tr><td>75 ppm</td><td>83 ppm</td><td>330 ppm</td><td>125000 ppm</td></tr>
</table></td></tr>
<tr><td>*Carbon dioxide* [77][87]</td><td>
Non-Flammable Gas
Melting point: 57°C (sublimes @-78.5°C)
Boiling point: -
Water Solubility: 0.2% (21.1°C)
Vapor pressure: 56.5 atm
IDLH: 40000 ppm
LCLo (ihl-human): 9 pph/ 5M
LC50: -</td></tr>
</table>

<table>
<tr><td></td><td>AEGLs (Acute Exposure Guideline Levels): -
PACs (Protective Action Criteria): -</td></tr>
<tr><td><i>Nitrogen</i> [77]</td><td>Non-Flammable Gas
Melting point: -214.4°C
Boiling point: -195.6°C
IDLH: -
AEGLs (Acute Exposure Guideline Levels): -
PACs (Protective Action Criteria): -</td></tr>
<tr><td><i>Catalyst (Fe)</i> [77][87]</td><td>Flammable solid; Strong Reducing Agent; Known Catalytic Activity; Water-Reactive; Pyrophoric.
Melting point: 1535°C
Boiling point: 27°C (@3000 mm)
IDHL: -
AEGLs (Acute Exposure Guideline Levels): -
PACs (Protective Action Criteria): Iron (7439-89-6)
<table>
<tr><td>PAC-1</td><td>PAC-2</td><td>PAC-3</td></tr>
<tr><td>3.2 mg/m^3</td><td>35 mg/m^3</td><td>150 mg/m^3</td></tr>
</table></td></tr>
<tr><td><i>Water</i> [77]</td><td>Boiling point: 100°C (60 mmHg)
Melting point: 0°C
IDLH: -
AEGLs (Acute Exposure Guideline Levels): -
PACs (Protective Action Criteria): -</td></tr>
<tr><td>SiO_2 [77][87]</td><td>Boiling point: 2230°C (60 mmHg)
Melting point: 1716-1736°C
Water solubility: Insoluble (soluble in HF)
Vapor pressure: 0 mmHg
IDLH: 3000 mg/m^3
AEGLs (Acute Exposure Guideline Levels): -
PACs (Protective Action Criteria):
Silica amorphous hydrated (7631-86-9)
<table>
<tr><td>PAC-1</td><td>PAC-2</td><td>PAC-3</td></tr>
<tr><td>18 mg/m^3</td><td>740 mg/m^3</td><td>4500 mg/m^3</td></tr>
</table></td></tr>
<tr><td><i>Alcohol with a long chain (e.g.; 2-heptanol)</i> [87]</td><td>Poison
Boiling point: 160.4°C
Melting point: -
Flash point: 71.1°C
IDLH: -
LD50 (orl-rat): 2580 mg/kg
LD50 (skn-rbt): 1780 mg/kg
AEGLs (Acute Exposure Guideline Levels): -
PACs (Protective Action Criteria): -</td></tr>
<tr><td><i>C7-C30 (e.g.n-heptane)</i> [77][87]</td><td>

Flammable liquid
LEL: 1.05%
UEL: 6.7%
Autoignition T: 223°C
Flash point: -3.9°C
Melting point: -91.61°C
Boiling point: 98.52°C</td></tr>
</table>

Water Solubility: 0.0003%
Vapor pressure: 40 mmHg (22.3°C)
IDLH: 750 ppm
TCLo (ihl-human): 1000 ppm/ 6M:CNS
LC50 (ihl-rat): 103 g/m^3 /4H
AEGLs (Acute Exposure Guideline Levels): -
PACs (Protective Action Criteria): Heptane (142-82-5)

PAC-1	PAC-2	PAC-3	LEL
500 ppm	830 ppm	5000 ppm	10500 ppm

C$_2$-C$_6$ (e.g.; propane)
[77][87]

Flammable Gas
LEL: 2.3%
UEL: 9.5%
Autoignition T: 450°C
Flash point: -104.4°C
Melting point: -187.7°C
Boiling point: -44.5°C
Water Solubility: 0.01%
Vapor pressure: 9823 mmHg
IDLH: 2100 ppm (Based on 10% of the lower explosive limit)
AEGLs (Acute Exposure Guideline Levels):

Exposure period	AEGL-1	AEGL-2	AEGL-3
10 min	10000 ppm	17000 ppm	33000 ppm
30 min	6900 ppm	17000 ppm	33000 ppm
60 min	5500 ppm	17000 ppm	33000 ppm
4 hours	5500 ppm	17000 ppm	33000 ppm
8 hours	5500 ppm	17000 ppm	33000 ppm

PACs (Protective Action Criteria): Propane (74-98-6)

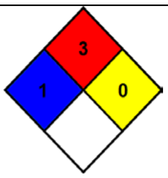
PAC-1	PAC-2	PAC-3	LEL
5500 ppm	17000 ppm	33000 ppm	23000 ppm

Methane (inside incondensable gases)
[77][87]

Flammable Gas; Strong Reducing Agent.
LEL: 5.3%
UEL: 15%
Autoignition T: 650°C
Flash point: -183.2°C
Melting point: -182.6°C
Boiling point: -161.5°C (760 mmHg)
Water Solubility: 3.5 mL/100 mL (17.2°C)
Vapor pressure: 258574 mmHg (37.8°C); 760 mmHg (-161.5°C)
IDLH: -
AEGLs (Acute Exposure Guideline Levels): -
PACs (Protective Action Criteria): Methane (74-82-8)

PAC-1	PAC-2	PAC-3	LEL
65000 ppm	230000 ppm	400000 ppm	50000 ppm

Acetone [77][87]



Flammable Liquid
LEL: 2.6%
UEL: 12.8%
Autoignition T: 465°C
Flash point: -17.8°C
Melting point: -94.6°C
Boiling point: 56.2°C
Water Solubility: greater than or equal to 100 mg/mL (22.2°C)
Vapor pressure: 180 mmHg (20°C); 270 mmHg (30°C)
IDLH: 2500 ppm; based on 10% of the lower explosive limit
AEGLs (Acute Exposure Guideline Levels):

Exposure period	AEGL-1	AEGL-2	AEGL-3
10 min	200 ppm	9300 ppm	16000 ppm
30 min	200 ppm	4900 ppm	8600 ppm
60 min	200 ppm	3200 ppm	5700 ppm
4 hours	200 ppm	1400 ppm	2500 ppm
8 hours	200 ppm	950 ppm	1700 ppm

PACs (Protective Action Criteria): Acetone (67-64-1)

PAC-1	PAC-2	PAC-3	LEL
200 ppm	3200 ppm	5700 ppm	26000 ppm

Helium [77][87]

Boiling point: -268.9°C
Melting point: -272.2°C
Water solubility: -
Vapor pressure: -
IDLH: -
AEGLs (Acute Exposure Guideline Levels): -
PACs (Protective Action Criteria): Helium (7440-59-7)

PAC-1	PAC-2	PAC-3
65000 ppm	230000 ppm	400000 ppm

CFC
(e.g.;
Chlorodifluoromethane)
[77][87]

Gas
Autoignition T: 632.2°C
Flash point: -160°C
Boiling point: -40.8°C
Melting point: -146°C
Water solubility: 0.3% (25°C)
Vapor pressure: 10991.42 mmHg
IDLH: -
LCLo (ihl-dog): 70 pph
LC50 (ihl-rat): 35pph/ 15M
AEGLs (Acute Exposure Guideline Levels): -
PACs (Protective Action Criteria):
Chlorodifluoromethane (75-45-6)

PAC-1	PAC-2	PAC-3
1250 ppm	2400 ppm	14000 ppm

A.9 HAZOP analysis

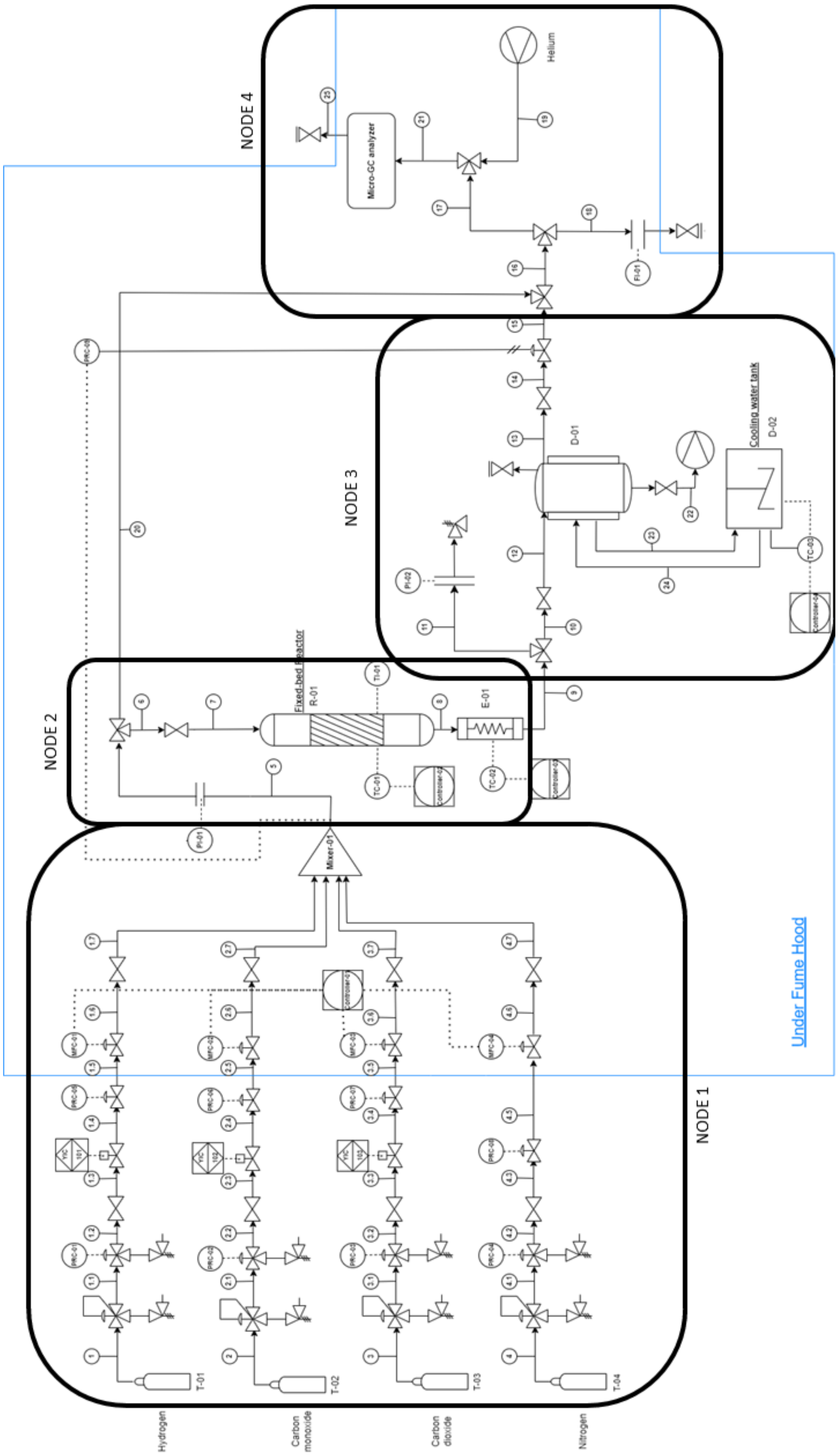


Figure A.9.1: *HAZOP analysis: nodes based on the experimental setup for Fischer-Tropsch synthesis.*

Table A.9.1: *Deviations considered in the HAZOP analysis.*

NODE	GUIDE WORD	PARAMETER
Node 1	MORE	Flow
		Pressure
		Temperature
		Voltage
	LESS	Pressure
		Temperature
	NO/LESS	Flow
		Voltage
	AS WELL AS	Material
Node 2	MORE	Flow
		Pressure
		Temperature
		Voltage
		Reaction rate
	LESS	Pressure
		Temperature
		Voltage
		Reaction rate
	NO/LESS	Flow
		Reaction rate
		Electrical insulation
	AS WELL AS	Material
	TOO EARLY	Open reactor
	TOO LATE	Close reactor
	Operation	
Node 3	MORE	Flow
		Pressure
		Temperature
		Voltage
	LESS	Pressure
		Temperature
		Separation
	NO/LESS	Flow
		Voltage
Node 4	MORE	Flow
		Pressure
		Temperature
		Voltage
		Concentration
	LESS	Pressure
		Temperature
		Concentration
	NO/LESS	Flow
		Voltage
		Concentration

Table A.9.2: *Deviations considered in the HAZOP analysis for transient states.*

Node	Deviation
Node 1	Close input valves before the reactor's temperature is equal to 20°C
Node 2	Close input valves before the reactor's temperature is equal to 20°C NO/LESS conversion TOO EARLY reactor opening before the feed is closed TOO LATE reactor closure after the feed is opened

For each deviation, the following points are analysed: causes, consequences, safeguards, recommendations, severity (S), likelihood (L), and risk class (RC).

A.9.1 HAZOP analysis: Node 1, feeding section

Table A.9.3: *MORE pressure (Node 1)*

Deviation name: MORE (increasing) pressure **Node description (design intent): reactants' feeding and mixing in the right composition (which could change from one experimental test to another)**						
Cause	**Consequence**	**Safeguards**	**Recommendations**	**S**	**L**	**R**
1. The pressure-drop in valve 02 is not enough	The down-stream sections are not with the correct pressure, the valve can break, possible leakages, failures, ruptures, explosions and death.	Hood, sensor for leakages, Sensors for pressure, alarmed high-pressure sensor (PIAH)	Correct valve sizing, maintenance of the pipes and the valve.	E3	W3	D
2. The pressure-drop in valve 05 is not enough	As above	As above	As above	E3	W3	D
3. The control pressure fails (PRC-01 to PRC-08)	The pressure can reach the MAWP of the pipes (or P_{max} of the operation units). Possible ruptures, leakages and loss of containment of toxics or flammables.	Hood, sensor for leakages, sensors for pressure, alarmed high-pressure sensor (PIAH)	Maintenance of the pipes, the valves and the mixer.	E3	W3	D
4. The control pressure set point is wrong (for PRC-01 to PRC-04)	As above	As above	Checklist	E3	W3	D

5. The control pressure set point is wrong (for PRC-05 to PRC-08)	As above	As above	Checklist	E3	W3	D
6. Valve-03 closes	As above	As above	Maintenance of the pipes and the valves.	E3	W3	D
7. Valve-07 closes	As above	As above	Maintenance of the pipes and the valves.	E3	W3/W2	E/D
8. Relief valves fail (the ones connected to valve-01 and 02)	As above	As above	As above	E3	W2	E
9. Wrong set point at least one of MFC-01, 02, 03 and 04	As above	As above	As above	E3	W4	C
10.Controller-01 fails	As above	As above	As above	E3	W3	D
11.At least one of the MFCs fail	As above	As above	As above	E3	W3	D

Table A.9.4: *LESS pressure (Node 1)*

Deviation name: LESS (decreasing) pressure
Node description (design intent): reactants' feeding and mixing in the right composition (which could change from one experimental test to another)

Cause	Consequence	Safeguards	Recommendations	S	L	RC
12.Higher pressure-drop in valve-02	Less pressure in the reactor and the outlet composition will change. Loss of the experimental test. Possible problems related to low temperature in CO_2 line.	Sensor for pressure	Correct sizing	E2	W3	E
13.Higher pressure-drop in valve-05	As above	As above	As above	E2	W3	E
14.Wrong set point for pressure controllers	As above	As above	Periodic check of the SP	E2	W4	D
15.Wrong set point on the mass flow controller	As above	As above	Periodic check of the SP	E2	W4	D
16.Leakages (gaskets' rupture)	Less pressure in the reactor and the outlet composition will change. Loss of the test. Dispersion of dangerous chemicals (toxic and flammable).	Hood, Sensor for leakages, Sensor for pressure	Periodic maintenance.	E3	W3	D

17. Controller-01 fails	Less pressure in the reactor and the outlet composition will change. Loss of the test.	Sensor for pressure	Periodic maintenance.	E2	W3	E
18. At least one of the MFCs fail	As above	As above	As above	E2	W3	E

Table A.9.5: *MORE flow (Node 1)*

Deviation name: MORE (increasing) flow
Node description (design intent): reactants' feeding and mixture them with the right composition (which could change from one experimental test to another)

Cause	**Consequence**	**Safeguards**	**Recommendations**	**S**	**L**	**RC**
19. Wrong set point in the mass flow controller	Possible increase in pressure (refer to MORE - increasing pressure) and changes in the final composition with loss of the experimental test.	Hood, sensor for leakages, sensors for pressure, alarmed high-pressure sensor (PIAH)	Periodic check of the SP	E2/E3	W4	D/C
20. At least one of the Mass flow controllers (MFC-01 to MFC-04) fails	As above	As above	Periodic maintenance	E2/E3	W4	D/C
21. At least one of the pressure controllers fails (PRC-01 to PRC-08)	As above	As above	Periodic maintenance	E2/E3	W3	E/D

Table A.9.6: *LESS/NO flow (Node 1)*

Deviation name: LESS/NO Flow
Node description (design intent): reactants' feeding and mixture them with the right composition (which could change from one experimental test to another)

Cause	**Consequence**	**Safeguards**	**Recommendations**	**S**	**L**	**RC**
22. Electricity shut-down	The safety valve closes, No flow in the reactor, No reaction, Exposure to reactants.	Hood, Sensor for leakages.		E2	W3	E
23. One or more tanks are empty	No reaction, different composition and loss of the test.	Sensor for pressure	Periodic check	E2	W4	D
24. Valves close (at least one)	Increasing pressure, leakages, explosion, death.	Hood, Sensor for leakages, Sensor for pressure.	Periodic maintenance	E3	W3	D

25. Failure of pressure controller	As above	As above	Periodic maintenance	E3	W3	D
26. Failure of mass flow controller	As above	As above	Periodic maintenance	E3	W3	D
27. Leakages	Loss of reactants, which are toxic and flammable. Subsequent fire or explosion.	Hood, Sensor for leakages	Periodic maintenance	E3	W3	D
28. Plug in the pipes	Increase in pressure, loss of containment of material.	As above	Periodic maintenance	E3	W2/W3	E/D
29. Set flowrates equal to zero before closing input valves (Shutdown)	Decreasing in pressure, less conversion inside the reactor, loss of the experimental test.	-	Checklist, procedures.	E2	W4	D

Table A.9.7: *MORE temperature (Node 1)*

Deviation name: MORE Temperature
Node description (design intent): reactants' feeding and mixture them with the right composition (which could change from one experimental test to another)

Cause	**Consequence**	**Safeguards**	**Recommendations**	**S**	**L**	**RC**
30. High external environmental temperature	Moles of the substances decrease, and the final composition can change.	-	Work in a temperature-controlled environment	E2	W4	D

Table A.9.8: *LESS temperature (Node 1)*

Deviation name: LESS Temperature
Node description (design intent): reactants' feeding and mixture them with the right composition (which could change from one experimental test to another)

Cause	**Consequence**	**Safeguards**	**Recommendations**	**S**	**L**	**RC**
31. Low external environmental temperature	Increasing moles of the substances and change in the final composition	-	Work in a temperature-controlled environment	E2	W4	D

Table A.9.9: *OTHER THAN MATERIAL (Node 1)*

Deviation name: OTHER THAN material/substance
Node description (design intent): reactants' feeding and mixture them with the right composition (which could change from one experimental test to another)

Cause	**Consequence**	**Safeguards**	**Recommendations**	**S**	**L**	**RC**
32. Wrong opening of valves/stream (e.g., use of CO instead of CO_2 or vice versa)	Wrong composition and loss of the experimental test.	Detection system	Checklist, Labelling	E2	W3/W4	E/D
33. At least one pressure or mass flow controller with a wrong set point	Wrong composition and loss of the experimental test.	-	Checklist	E2	W4	D

Table A.9.10: *MORE voltage (Node 1)*

<table>
<tr><td colspan="7">Deviation name: MORE voltage
Node description (design intent): reactants’ feeding and mixture them with the right composition (which could change from one experimental test to another)</td></tr>
<tr><th>Cause</th><th>Consequence</th><th>Safeguards</th><th>Recommendations</th><th>S</th><th>L</th><th>RC</th></tr>
<tr><td>34.Electrical current overload</td><td>Electrical short circuit.
Fire.
Damage to equipment.</td><td>Compliance of the electrical system with regulations.
Fire protection systems.</td><td>Maintenance.</td><td>E4</td><td>W2</td><td>D</td></tr>
<tr><td>35.Defective grounding of equipment</td><td>Circulating currents.
Uncontrolled ignition sources.</td><td>-</td><td>Inspection and regular check of grounding.</td><td>E4</td><td>W2</td><td>D</td></tr>
</table>

Table A.9.11: *LESS/NO voltage (Node 1)*

<table>
<tr><td colspan="7">Deviation name: LESS/NO voltage
Node description (design intent): reactants’ feeding and mixture them with the right composition (which could change from one experimental test to another)</td></tr>
<tr><th>Cause</th><th>Consequence</th><th>Safeguards</th><th>Recommendations</th><th>S</th><th>L</th><th>RC</th></tr>
<tr><td>36.Shut-down electricity</td><td>Wrong composition to the reactor, wrong/no flowrate to the reactor (valves are FC), decreasing pressure, increasing pressure before valve 4.</td><td>Safety valve</td><td>-</td><td>E2</td><td>W3</td><td>E</td></tr>
<tr><td>37.Power outage</td><td>As above</td><td>Compliance of the electrical system with regulations.
Hood, sensors for leakages.</td><td>Maintenance.</td><td>E3</td><td>W4</td><td>C</td></tr>
</table>

Table A.9.12: *Close input valves BEFORE required - TOO EARLY (Node 1)*

<table>
<tr><td colspan="7">Deviation name: Close input valves <u>before</u> the reactor’s temperature is equal to 20°C (TOO EARLY closure)
Node description (design intent): reactants’ feeding and mixture them with the right composition (which could change from one experimental test to another)</td></tr>
<tr><th>Cause</th><th>Consequence</th><th>Safeguards</th><th>Recommendations</th><th>S</th><th>L</th><th>RC</th></tr>
<tr><td>38.TI-01 fails</td><td>Possible damage to the catalyst, different final composition, loss of the experimental test.</td><td>Hood, sensors for pressure.</td><td>Checklist, procedure.</td><td>E2</td><td>W4</td><td>D</td></tr>
<tr><td>39.Wrong reading of TI-01</td><td>As above</td><td>As above</td><td>As above</td><td>E2</td><td>W4</td><td>D</td></tr>
</table>

A.9.2 HAZOP analysis: Node 2, reaction section

Table A.9.13: *MORE pressure (Node 2)*

Deviation name: MORE Pressure

Node description (design intent): Establish the intended conversion inside the reactor and maintain the product stream in a gas phase after exchanging heat.

Cause	**Consequence**	**Safeguards**	**Recommendations**	**S**	**L**	**RC**
40.Pressure controller fails (PRC-09)	Higher conversion of CO. Different final composition. Loss of the experimental test. Leakages (from reactor or pipes). Rupture of the reactor.	Hood, sensor for leakages, sensors for pressure, alarmed high-pressure sensor (PIAH)	Maintenance	E3	W3	D
41.Wrong SP of PRC-09	As above	As above	Maintenance. Checklist, double check (> 2 people)	E3	W4	C
42.PI-01 fails (The displayed pressure is incorrect, and there is no perception from the operator of the error)	As above	As above	Periodic maintenance. Checklist.	E3	W4	C
43.Valve 08 closes	No reaction, uncontrolled leakages from the pipes.	As above	As above	E3	W3	D
44.Valve 09 closes	As above	As above	As above	E3	W3	D
45.Higher P in the previous section	Higher conversion of CO. Different final composition. Loss of the experimental test. Leakages (from reactor or pipes). Rupture of the reactor.	As above	Maintenance.	E3	W3	D
46.Overpacked reactor	As above	As above	As above	E3	W4	C

Table A.9.14: *LESS pressure (Node 2)*

Deviation name: LESS Pressure

Node description (design intent): Establish the intended conversion inside the reactor and maintain the product stream in a gas phase after exchanging heat.

Cause	**Consequence**	**Safeguards**	**Recommendations**	**S**	**L**	**RC**
47.Wrong SP in PRC-09	Less conversion of CO. Different final composition. Loss of experimental test.	Pressure sensor	Periodic check.	E2	W4	D
48.Wrong SP in the previous valves	As above	Pressure sensor		E2	W3	E
49.Leakages	Release of flammable or toxic materials. Uncontrolled ignition with final events of fire/explosion.	Hood, Sensors for leakages, Sensors.	Periodic maintenance.	E4	W3	C
50.Not adequately packed reactor	Less conversion, different final composition, loss of the test	As above	As above	E2	W3	E
51.More pressure drops at least in valve 08 or 09	Less conversion, Different final composition, loss of test. Leakages, death.	As above	As above	E2	W3	E

Table A.9.15: *MORE temperature (Node 2)*

Deviation name: MORE Temperature

Node description (design intent): Establish the intended conversion inside the reactor and maintain the product stream in a gas phase after exchanging heat.

Cause	**Consequence**	**Safeguards**	**Recommendations**	**S**	**L**	**RC**
52.Wrong SP in TC-01	More energy and higher temperature than required. Different final composition. Loss of the experimental test. Increasing pressure, possible leakages or ruptures. Damage to the catalyst.	Hood, Sensors for leakages, Sensors.	Periodic check.	E3	W4	C
53.TI-01 fails	As above	As above	As above	E3	W3	D
54.Controller-02 fails	As above	As above	As above	E3	W3	D
55.Set the wrong temperature in the temperature ramp for the start-up	Damage to the catalyst. Increasing pressure. Altered final composition. Loss of the experimental test.	Hood, sensor for leakages, sensors for pressure, alarmed high-pressure sensor (PIAH)	Checklist, procedure (double check)	E3	W4	C

56.Set the volume flowrates after starting the temperature ramp	Possible damage to the catalyst. Different final composition. Loss of the experimental test.	-	As above	E2	W4	D

Table A.9.16: *LESS temperature (Node 2)*

Deviation name: LESS Temperature
Node description (design intent): Establish the intended conversion inside the reactor and maintain the product stream in a gas phase after exchanging heat.

Cause	**Consequence**	**Safeguards**	**Recommendations**	**S**	**L**	**RC**
57.Wrong SP in TC-01	Less energy and lower temperature than required. Different final composition (less reaction). Possible issues in the heat exchanger with partial evaporation of the products.	Temperature sensor	Periodic check.	E2	W4	D
58.TC-01 fails	Different final composition. Loss of the experimental test. Possible plugs of the pipes by heavy hydrocarbons. Increasing pressure. Leakages, loss of containment.	Hood, Sensors for leakages, Sensors.	Maintenance.	E3	W3	D
59.Electricity shut-down	No energy, no reaction. Loss of the experimental test. Possible plugs of the pipes. Increasing pressure. Leakages, loss of containment.	As above	Maintenance.	E3	W3	D
60.TC-02 fails	Plugs in the lines by heavy hydrocarbons. Increasing pressure. Leakages, loss of containment.	As above	Maintenance.	E3	W3	D

Table A.9.17: *MORE flow (Node 2)*

Deviation name: MORE Flow
Node description (design intent): Establish the intended conversion inside the reactor and maintain the product stream in a gas phase after exchanging heat.

Cause	**Consequence**	**Safeguards**	**Recommendations**	**S**	**L**	**RC**
61.PI-01 fails	Higher pressure in the reactor with possible failures. Leakages and loss of containment. Different final composition.	Hood, sensor for leakages, sensors for pressure, alarmed high-pressure sensor (PIAH)	Periodic maintenance.	E3	W3	D

	Loss of the experimental test. Issues when exchanging heat to achieve the final temperature in E-01 and R-01.					
62.PRC-09 fails	As above	As above	As above	E3	W3	D
63.Wrong SP of PRC-09	As above	As above	Maintenance, checklist, double check (> 2 people)	E3	W4	C
64.Deviations in Node 1	As above	As above	As above	E3	W3	D
65.Less pressure drops at least in valve-08 and/or in valve-09	As above	As above	Periodic maintenance, proper sizing of equipment.	E3	W3	D

Table A.9.18: *LESS/NO flow (Node 2)*

Deviation name: LESS/NO Flow

Node description (design intent): Establish the intended conversion inside the reactor and maintain the product stream in a gas phase after exchanging heat.

Cause	Consequence	Safeguards	Recommendations	S	L	RC
66.Deviations in Node 1	Less pressure in the reactor. Less conversion. Loss of the experimental test. Leakages and loss of containment.	Hood, Sensors for leakages, Sensors.	Periodic maintenance.	E2	W3	E
67.PI-01 fails	Increasing pressure in the pipes. Leakages and loss of containment. Less pressure in the reactor. Less conversion. Loss of the experimental test.	As above	As above	E2	W3	D
68.Closure of valves 08 or 09	Increasing in pressure. Leakages and loss of containment. No reaction. Loss of the experimental test.	As above	As above	E2	W3	D
69.PRC-09 fails	Less pressure in the reactor. Less conversion. Loss of the experimental test.	As above	As above	E2	W3	E
70.Wrong SP of PRC-09	As above	As above	As above	E2	W3	E
71.Use of the by-pass	No reaction. Loss of the experimental test. Increasing pressure in the by-pass line.	As above	As above	E3	W3	D

	Leakages and loss of containment.					
72.Leakage/defect connection	No or reduced circulating flow. No reaction. Leakages and loss of containment.	No safeguards.	Environmental sensor system.	E4	W2/W3	D/C

Table A.9.19: *MORE voltage (Node 2)*

<table>
<tr><td colspan="7">Deviation name: MORE voltage
Node description (design intent): Establish the intended conversion inside the reactor and maintain the product stream in a gas phase after exchanging heat.</td></tr>
<tr><td>Cause</td><td>Consequence</td><td>Safeguards</td><td>Recommendations</td><td>S</td><td>L</td><td>RC</td></tr>
<tr><td>73.Electrical current overload</td><td>Electrical short circuit, fire.
Damage to equipment.</td><td>Electrical system compliant with regulations, fire protection systems.</td><td>Maintenance.</td><td>E4</td><td>W2</td><td>D</td></tr>
<tr><td>74.Defective grounding of equipment</td><td>Circulating currents.
Uncontrolled ignition sources.</td><td></td><td>Inspection and regular check of grounding.</td><td>E4</td><td>W2</td><td>D</td></tr>
</table>

Table A.9.20: *LESS/NO voltage (Node 2)*

<table>
<tr><td colspan="7">Deviation name: LESS/NO voltage
Node description (design intent): Establish the intended conversion inside the reactor and maintain the product stream in a gas phase after exchanging heat.</td></tr>
<tr><td>Cause</td><td>Consequence</td><td>Safeguards</td><td>Recommendations</td><td>S</td><td>L</td><td>RC</td></tr>
<tr><td>75.Shut-down electricity</td><td>No reaction.
No vaporization in E-01.</td><td>Safety valve, i.e. if there is no electricity, the reactor will have a mixture of unreacted material and products (valves: FC). The reaction inside the reactor will continue, but the operative conditions are not controlled.</td><td>Checklist for the following start-up</td><td>E2</td><td>W3</td><td>E</td></tr>
<tr><td>76.Power outage</td><td>Less or no reaction, problems related to the vaporization in E-01.</td><td>Electrical system compliant with regulations,
hood, sensors for leakages.</td><td>Maintenance.</td><td>E3</td><td>W4</td><td>C</td></tr>
</table>

	Plugs in pipelines due to heavy hydrocarbons. Leakages and loss of containment.					

Table A.9.21: *MORE reaction rate (Node 2)*

Deviation name: MORE Reaction rate
Node description (design intent): Establish the intended conversion inside the reactor and maintain the product stream in a gas phase after exchanging heat.

Cause	**Consequence**	**Safeguards**	**Recommendations**	**S**	**L**	**RC**
77.Higher temperature (wrong SP in TC-01)	Increasing in temperature (see MORE Temperature). Different composition. Loss of the experimental test. More quantity of heavy-phase. Damage to catalyst.	Hood, sensor for leakages, Sensors for pressure, alarmed high-pressure sensor (PIAH)	Checklist, double check (> 2 people)	E3	W4	C

Table A.9.22: *LESS reaction rate (Node 2)*

Deviation name: Decreasing Reaction rate
Node description (design intent): Establish the intended conversion inside the reactor and maintain the product stream in a gas phase after exchanging heat.

Cause	**Consequence**	**Safeguards**	**Recommendations**	**S**	**L**	**RC**
78.Catalyst poisoning	Different composition. Loss of the experimental test. Increasing gaseous components. Increasing pressure (see MORE pressure)	Hood, sensor for leakages, Sensors for pressure, alarmed high-pressure sensor (PIAH)	Periodic change of the catalyst	E4	W3	C
79.Wrong SP of TC-01	Less conversion. Different final composition. Loss of the experimental test Increasing in pressure.	As above	As above	E2	W4	D

Table A.9.23: *LESS/NO reaction rate (Node 2)*

Deviation name: LESS/NO Reaction rate **Node description (design intent): Establish the intended conversion inside the reactor and maintain the product stream in a gas phase after exchanging heat.**						
Cause	**Consequence**	**Safeguards**	**Recommendations**	**S**	**L**	**RC**
80.Catalyst poisoning	Different composition. Loss of the experimental test. Increasing gaseous components. Increasing pressure (see MORE pressure)	Hood, sensor for leakages, Sensors for pressure, alarmed high-pressure sensor (PIAH)	Periodic change of the catalyst	E4	W3	C
81.Wrong SP of TC-01	Less conversion. Different final composition. Loss of the experimental test. Increasing pressure.	As above	As above	E2	W4	D

Table A.9.24: *OTHER THAN material (Node 2)*

Deviation name: OTHER THAN material **Node description (design intent): Establish the intended conversion inside the reactor and maintain the product stream in a gas phase after exchanging heat.**						
Cause	**Consequence**	**Safeguards**	**Recommendations**	**S**	**L**	**RC**
82.Opening of the wrong equipment (from Node 1) (CO instead of CO_2 or vice versa)	LESS/MORE reaction rate. Loss of the experimental test.		Checklist. Labelling. Double-check (> 2 operators)	E3	W3	D

Table A.9.25: *TOO EARLY reactor opening (Node 2)*

Deviation name: TOO EARLY reactor opening (before the feed is closed) **Node description (design intent): Establish the intended conversion inside the reactor and maintain the product stream in a gas phase after exchanging heat.**						
Cause	**Consequence**	**Safeguards**	**Recommendations**	**S**	**L**	**RC**
83.Open the reactor before the feeding stream is closed	Possible release of toxic and flammable gases. Uncontrolled ignition. Final events of fire/explosion.	Sensors, hood.	Procedure to open and close the reactor, no ignition sources.	E3	W4	C

Table A.9.26: *TOO LATE reactor closure (Node 2)*

Deviation name: TOO LATE reactor closure (after the feed is opened)
Node description (design intent): Establish the intended conversion inside the reactor and maintain the product stream in a gas phase after exchanging heat.

Cause	**Consequence**	**Safeguards**	**Recommendations**	**S**	**L**	**RC**
84.Close the reactor after opening the feeding stream (Start-up)	Possible release of toxic and flammable gases. Uncontrolled ignition. Final events of fire/explosion.	Sensors, hood.	Procedure to open and close the reactor, no ignition sources.	E3	W4	C

Table A.9.27: *LESS/NO electrical insulation (Node 2)*

Deviation name: LESS/NO electrical insulation
Node description (design intent): Establish the intended conversion inside the reactor and maintain the product stream in a gas phase after exchanging heat.

Cause	**Consequence**	**Safeguards**	**Recommendations**	**S**	**L**	**RC**
85.Damage to the electrical insulation of the reactor	Contact with electricity, possible electrocution, damage to the operator.	Grounding system, insulation.	Periodic maintenance	E3	W3	D
86.Damage to the electrical insulation of the heat exchanger	As above	Grounding system.	As above	E3	W3	D

Table A.9.28: *Deviation during cleaning operations (Node 2)*

Deviation name: Operation
Node description (design intent): Establish the intended conversion inside the reactor and maintain the product stream in a gas phase after exchanging heat.

Cause	**Consequence**	**Safeguards**	**Recommendations**	**S**	**L**	**RC**
87.Cleaning the reactor	Damage to the reactor.		Proper procedure to clean the reactor.	E1	W4	E

Table A.9.29: *Close input valves BEFORE required (Node 2)*

Deviation name: Close input valves before the temperature in the reactor is 20°C
Node description (design intent): Establish the intended conversion inside the reactor and maintain the product stream in a gas phase after exchanging heat.

Cause	**Consequence**	**Safeguards**	**Recommendations**	**S**	**L**	**RC**
88.TI-01 fails (Shutdown)	Possible damage to the catalyst. Different final composition. Loss of the experimental test.	Hood, sensors for pressure.	Checklist, procedure.	E2	W4	D
89.Wrong reading of TI-01 (Shutdown)	As above	As above	As above	E2	W4	D

Table A.9.30: *LESS/NO conversion (Node 2)*

Deviation name: LESS/NO conversion **Node description (design intent): Establish the intended conversion inside the reactor and maintain the product stream in a gas phase after exchanging heat.**						
Cause	**Consequence**	**Safeguards**	**Recommendations**	**S**	**L**	**RC**
90.Decreasing pressure inside the plant before setting the flowrate equal to zero. (Shutdown)	Pressure decrease inside the reactor. LESS/NO conversion. Loss of the experimental test.	-	Checklist and procedure (double check)	E2	W4	D
91.Decreasing pressure inside the plant before closing the input valves. (Shutdown)	As above	-	As above	E2	W4	D

A.9.3 HAZOP analysis: Node 3, separation section

Table A.9.31: *MORE pressure (Node 3)*

Deviation name: MORE Pressure **Node description (design intent): Condensation of the heavy phase (C_7-C_{30}) and the water to separate from condensable gases and the light phase (C_2-C_6).**						
Cause	**Consequence**	**Safeguards**	**Recommendations**	**S**	**L**	**RC**
92.PI-02 fails	Achieve the maximum pressure of the pipes/equipment. Less separation. Ruptures and leakages.	Hood, sensor for leakages, sensors for pressure, alarmed high-pressure sensor (PIAH)	Periodic maintenance.	E3	W4	C
93.Valve 10 fails	As above	As above	As above	E3	W2	E
94.Valve 11 closes (three-way valve)	As above	As above	As above	E3	W3	D
95.PRC-09 fails	As above	As above	As above	E3	W3	D
96.Wrong SP of PRC-09	As above	As above	Periodic maintenance, periodic check of SP.	E3	W4	C
97.Valve 14 closes	As above	As above	Periodic maintenance.	E3	W3	D
98.Valve 13 closes	As above	As above	As above	E3	W3	D
99.Valve 12 closes	As above	As above	As above	E3	W3	D
100.Higher pressure from the previous nodes	Less condensation. Less separation. Loss of the experimental test. Plugs in the external tubes.	Temperature indicator		E3	W3	D
101.Higher water temperature in the jacket of D-01	Less condensation. Less separation.	Temperature indicator. Hood.	Periodic maintenance. Checklist.	E3	W3	D

	Loss of the experimental test. Plugs in the external tubes. Rupture, leakages with loss of containment.	Sensors for leakages. Sensors.	Periodic check of TC-03.			

Table A.9.32: *LESS pressure (Node 3)*

Deviation name: LESS Pressure
Node description (design intent): Condensation of the heavy phase (C_7-C_{30}) and the water to separate from condensable gases and the light phase (C_2-C_6).

Cause	**Consequence**	**Safeguards**	**Recommendations**	**S**	**L**	**RC**
102.Lower temperature in the jacket	More condensed phase. Plugs in the pipes. Plug in D-01. Loss of containment of heavy and light phases.	Temperature indicator. Hood. Sensor for leakages. Sensors.	Maintenance, periodic check of the temperature controller set point	E2	W3	E
103.Wrong SP of PRC-09	More condensation. More separation. Loss of the experimental test.	Pressure sensor.	Periodic check.	E2	W4	D
104.Valve 12 completely open	Loss of the experimental test. Loss of the experimental test.	Hood, Sensors.	Periodic maintenance.	E2	W3	E
105.Valve 13 completely open	Partial condensation. Loss of containment of incondensable gases. Loss of the experimental test.	Hood, Sensors.	As above.	E2	W3	E

Table A.9.33 *MORE flow (Node 3)*

Deviation name: MORE Flow
Node description (design intent): Condensation of the heavy phase (C_7-C_{30}) and the water to separate from condensable gases and the light phase (C_2-C_6).

Cause	**Consequence**	**Safeguards**	**Recommendations**	**S**	**L**	**RC**
106.Higher flow from previous nodes	More quantity to condensate. Less separation. Loss of the experimental test. Increasing pressure. Leakages, loss of containment.	Hood, Sensors for leakages, Sensor of pressure, PIAH.	Periodic maintenance and periodic check of the operative conditions.	E3	W3	D

107.Less pressure drops in valves 11 or three-way before D-01	As above.	As above.	As above.	E3	W3	D
108.Wrong SP of PRC-09	Increasing pressure. Less separation. Leakages, loss of containment.	As above.	Periodic check, checklist.	E3	W4	C

Table A.9.34: *LESS/NO flow (Node 3)*

Deviation name: LESS/NO Flow
Node description (design intent): Condensation of the heavy phase (C_7-C_{30}) and the water to separate from condensable gases and the light phase (C_2-C_6).

Cause	**Consequence**	**Safeguards**	**Recommendations**	**S**	**L**	**RC**
109.Plug in the reactor	Increasing pressure. Ruptures, leakages and loss of containment.	Hood, Sensors for leakages, Sensors.	Periodic maintenance.	E3	W3	D
110.Decreased/no flow from previous nodes	Loss of the test.	-	-	E1	W3	F
111.Plugs in the pipes	Increasing pressure. Ruptures, leakages and loss of containment.	Hood, Sensors for leakages, Sensors.	Periodic maintenance.	E3	W3	D
112.Leakages	Release of toxic, flammable or condensable gases. Possible fire or explosion.	Hood, Sensors for leakages, Fire protection systems.	Work far from possible sources of fire.	E3	W3	D
113.Valve 11 closes	Increasing pressure. Plugs in the pipes. Ruptures, leakages and loss of containment.	Hood, Sensors for leakages, Sensors.	Periodic maintenance.	E3	W3	D
114.Valve 10 fails	Ruptures, leakages and loss of containment of flammables/toxics.	As above	As above	E3	W3	D
115.No Flow of CFC	Higher water temperature. No/less separation. Plugs in the pipes. Increasing pressure. Ruptures, leakages and loss of containment.	Temperature indicator, Hood, Sensors for leakages, Sensors.	Checklist.	E3	W3	D
116.No water	No/less separation. Plugs in the pipes. Increasing pressure. Ruptures, leakages and loss of containment.	As above	As above	E3	W3	D

Table A.9.35: *MORE temperature (Node 3)*

Deviation name: MORE Temperature **Node description (design intent): Condensation of the heavy phase (C_7-C_{30}) and the water to separate from condensable gases and the light phase (C_2-C_6).**						
Cause	**Consequence**	**Safeguards**	**Recommendations**	**S**	**L**	**RC**
117.TC-02 fails	More difference in temperature than required. Less separation. Increasing pressure. Ruptures, leakages and loss of containment.	Hood, sensor for leakages, sensors for pressure, alarmed high-pressure sensor (PIAH)	Periodic maintenance, periodic check.	E3	W3	D
118.TC-03 fails	Less separation. Increasing pressure. Ruptures, leakages and loss of containment.	As above.	As above.	E3	W3	D
119.Controller 4 fails	As above.	As above.	As above.	E3	W3	D
120.Fouling in the jacket	As above.	As above.	As above.	E3	W3	D

Table A.9.36: *LESS temperature (Node 3)*

Deviation name: LESS Temperature **Node description (design intent): Condensation of the heavy phase (C_7-C_{30}) and the water to separate from condensable gases and the light phase (C_2-C_6).**						
Cause	**Consequence**	**Safeguards**	**Recommendations**	**S**	**L**	**RC**
121.Lower temperature from E-01	Plug in the pipe. Increasing pressure. Ruptures, leakages and loss of containment.	Temperature indicator, Hood, Sensors for leakages, Sensors.	Periodic check and maintenance.	E3	W3	D
122.TC-03 has a wrong SP	More condensation. More separation. Plugs in the pipes. Loss of the experimental test.	Temperature indicator, Hood, Sensors for leakages, Sensors.	Periodic check and maintenance.	E2	W4	D
123.Controller 4 fails	As above.	As above.	As above.	E2	W3	E

Table A.9.37: *LESS separation (Node 3)*

Deviation name: LESS Separation
Node description (design intent): Condensation of the heavy phase (C_7-C_{30}) and the water to separate from condensable gases and the light phase (C_2-C_6).

Cause	Consequence	Safeguards	Recommendations	S	L	RC
124.Higher Temperature in D-01	Increasing pressure. Ruptures, leakages and loss of containment.	Temperature indicator, Hood, Sensors for leakages, Sensors.	Periodic maintenance, periodic check.	E3	W3	D
125.Higher flow in D-01	Ruptures, leakages and loss of containment. Loss of the experimental test.	Hood, Sensors for leakages, Sensors.	As above.	E3	W3	D

Table A.9.38: *MORE voltage (Node 3)*

Deviation name: MORE voltage
Node description (design intent): Condensation of the heavy phase (C_7-C_{30}) and the water to separate from condensable gases and the light phase (C_2-C_6).

Cause	Consequence	Safeguards	Recommendations	S	L	RC
126.Electrical current overload	Electrical short circuit. Possibility of fire. Damage to equipment.	Electrical system compliant with regulations. Fire protection systems.	Maintenance.	E4	W2	D
127.Defective grounding of equipment	Circulating currents. Uncontrolled ignition sources.		Inspection and regular check of grounding.	E4	W2	D

Table A.9.39: *LESS/NO voltage (Node 3)*

Deviation name: LESS/NO voltage
Node description (design intent): Condensation of the heavy phase (C_7-C_{30}) and the water to separate from condensable gases and the light phase (C_2-C_6).

Cause	Consequence	Safeguards	Recommendations	S	L	RC
128. Shut-down of electricity	Decreasing in separation at D-01.	Safety valve. Hood. Sensor for leakages.		E2	W3	E

	Increasing pressure. Loss of the experimental test.					
129. Power outage	As above.	Electrical system compliant with regulations, hood, sensors for leakages, sensors for pressure, PIAH, and safety valve.	Maintenance.	E3	W4	C

A.9.4 HAZOP analysis: Node 4, analysis of the gas phase

Table A.9.40: *MORE pressure (Node 4)*

Deviation name: MORE Pressure **Node description (design intent): Analysis of the light phase after the reaction section.**						
Cause	**Consequence**	**Safeguards**	**Recommendations**	**S**	**L**	**RC**
130.Valve 16 closes	Leakages and loss of containment. Possible fire or explosion.	Hood, sensor for leakages, sensors for pressure, alarmed high-pressure sensor (PIAH)	Maintenance	E3	W3	D
131.Valve 17 closes	As above	As above	As above	E3	W3	D
132.Flanged valves close	As above	As above	As above	E3	W3	D

Table A.9.41: *LESS pressure (Node 4)*

Deviation name: LESS Pressure **Node description (design intent): Analysis of the light phase after the reaction section.**						
Cause	**Consequence**	**Safeguards**	**Recommendations**	**S**	**L**	**RC**
133.Lower pressure from previous nodes	Less quantity. Different final composition. Loss of the experimental test.	Hood. Sensors for leakages. Sensors.	Maintenance	E3	W3	D
134.Leakages	Release of flammable or toxic material(s).	Hood. Sensors.	Maintenance	E3	W1	F

Table A.9.42: *MORE flow (Node 4)*

Deviation name: MORE Flow **Node description (design intent): Analysis of the light phase after the reaction section.**						
Cause	**Consequence**	**Safeguards**	**Recommendations**	**S**	**L**	**RC**
135.Higher flow from previous nodes	Different composition. Loss of the experimental test.	Hood, sensor for leakages,	Maintenance	E3	W3	D

	Leakages and loss of containment.	sensors for pressure, alarmed high-pressure sensor (PIAH)				
136.FI-01 fails	Erroneous quantity in the Micro-GC. Loss of the experimental test.	As above	Periodic check	E2	W4	D

Table A.9.43: *LESS/NO flow (Node 4)*

Deviation name: LESS/NO flow **Node description (design intent): Analysis of the light phase after the reaction section.**						
Cause	**Consequence**	**Safeguards**	**Recommendations**	**S**	**L**	**RC**
137.Lower flow from previous nodes	Changes in the composition. Loss of the experimental test.	Hood, Sensors for leakages, sensors	Maintenance	E2	W3	E
138.Valve 16 closes	Increasing pressure. Leakages and loss of containment. Loss of the experimental test.	Hood, Sensors for leakages, sensors	Maintenance	E3	W3	D
139.Valve 17 closes	Increasing pressure. Leakages and loss of containment. Loss of the experimental test.	As above.	Maintenance	E3	W3	D
140.FI-01 fails	Erroneous quantity to the Micro-GC. Loss of the experimental test.	As above.	Maintenance, periodic check.	E2	W3	E
141.Valve before Micro-GC closes (three-way valve)	No carrier into the Micro-GC. Loss of the experimental test.		Check list, periodic check	E1	W3	F

Table A.9.44: *MORE temperature (Node 4)*

Deviation name: MORE Temperature **Node description (design intent): Analysis of the light phase after the reaction section.**						
Cause	**Consequence**	**Safeguards**	**Recommendations**	**S**	**L**	**RC**
142.Wrong setting of the temperature ramp.	Loss of the experimental test.		Checklist, procedure.	E1	W3	F
143.Thermostat failure in the Micro-GC.	Loss of the experimental test. Leakage and loss of containment.	Hood. Sensors.	Maintenance.	E3	W3	D

Table A.9.45: *LESS temperature (Node 4)*

Deviation name: LESS Temperature
Node description (design intent): Analysis of the light phase after the reaction section.

Cause	Consequence	Safeguards	Recommendations	S	L	RC
144.Wrong setting of the temperature ramp.	Loss of the experimental test.	-	Checklist, procedure.	E1	W3	F
145.Thermostat fails in the Micro-GC.	Loss of the experimental test.	-	Periodic maintenance.	E1	W3	F

Table A.9.46: *LESS/NO voltage (Node 4)*

Deviation name: LESS/NO voltage
Node description (design intent): Analysis of the light phase after the reaction section.

Cause	Consequence	Safeguards	Recommendations	S	L	RC
146.Shut down of the electricity.	No analysis. Loss of the experimental test.	-	-	E1	W3	F
147.Micro-GC is not connected to electricity.	No analysis. Loss of the experimental test.	-	Periodic check	E1	W3	F
148. Power outage.	As above	-	-	E1	W3	F

Table A.9.47: *MORE concentration (Node 4)*

Deviation name: MORE Concentration
Node description (design intent): Analysis of the light phase after the reaction section.

Cause	Consequence	Safeguards	Recommendations	S	L	RC
149. Detector fails	Loss of the experimental test.	-	Periodic maintenance	E1	W4	E

Table A.9.48: *LESS concentration (Node 4)*

Deviation name: LESS Concentration
Node description (design intent): Analysis of the light phase after the reaction section.

Cause	Consequence	Safeguards	Recommendations	S	L	RC
150. Detector fails	Loss of the experimental test.	-	Periodic maintenance	E1	W4	E

Table A.9.49: *LESS/NO concentration (Node 4)*

Deviation name: LESS/NO Concentration
Node description (design intent): Analysis of the light phase after the reaction section.

Cause	Consequence	Safeguards	Recommendations	S	L	RC
151. Detector fails	Loss of the test		Periodic maintenance	E1	W4	E

Table A.9.50: *MORE voltage (Node 4)*

Deviation name: MORE voltage **Node description (design intent): Analysis of the light phase after the reaction section.**						
Cause	**Consequence**	**Safeguards**	**Recommendations**	**S**	**L**	**RC**
152.Electrical current overloading	Electrical short circuit. Possible fire scenario.	Electrical system compliant with regulations. Fire protection systems.	Maintenance.	E4	W2	D

A.10 Supplementary material for LOPA analysis

Table A.10.1: *Hazardous events emerged from the HAZOP analysis (L: likelihood; S: severity; RC: risk class).*

Node	Initiating event	Characteristics of the basic event	Deviation	L	S	RC
1	Set a wrong set point in at least one of MFC-01/02/03/04	Human error	MORE pressure or flow	E3	W4	C
	A power outage	System failure	NO/LESS electric voltage-current	E3	W4	C
2	Wrong value at PI-01	System failure	MORE pressure	E3	W4	C
	Reactor too packed	Human error	MORE pressure	E3	W4	C
	Wrong set point in PRC-09	Human error	MORE pressure or flow	E3	W4	C
	Wrong set point in TC-01	Human error	MORE temperature/reaction rate	E3	W4	C
	Wrong set point of temperature (start-up)	Human error	MORE temperature	E3	W4	C
	Leakage/defective connection	System failure	LESS pressure, LESS/NO flow	E4	W3	C
	Reactor opening before closing the feed line(s)	Human error	TOO EARLY opening of the reactor	E3	W4	C
	Reactor closing after opening the feed line(s)	Human error	TOO LATE closing of the reactor	E3	W4	C
	A power outage	System failure	LESS/NO electric current/voltage	E3	W4	C
	Catalyst poisoning (not required)	System failure/human error	LESS/NO reaction rate or catalytic activity	E4	W3	C
3	Wrong set point in PRC-09	Human error	MORE pressure or flow	E3	W4	C
	PI-02 failure	System failure	MORE pressure	E3	W4	C
	Power outage	System failure	LESS/NO electric voltage	E3	W4	C

Table A.10.2: *Streams and associated equipment involved in Node 1.*

Stream	Equipment
Hydrogen	T-01 Valve 1 Valve 2 connected to PRC-01 Valve 3 Valve 4 connected to gas detectors (CO, CH_4, H_2 and CO_2) Valve 5 connected to PRC-05 Valve 6 connected to MFC-01 Valve 7 Mixer-01
Carbon monoxide	T-02 Valve 1 Valve 2 connected to PRC-02 Valve 3 Valve 4 connected to gas detectors (CO, CH_4, H_2 and CO_2) Valve 5 connected to PRC-06 Valve 6 connected to MFC-02 Valve 7 Mixer-01
Carbon dioxide	T-03 Valve 1 Valve 2 connected to PRC-03 Valve 3 Valve 4 connected to gas detectors (CO, CH_4, H_2 and CO_2) Valve 5 connected to PRC-07 Valve 6 connected to MFC-03 Valve 7 Mixer-01
Nitrogen	T-04 Valve 1 Valve 2 connected to PRC-04 Valve 3 Valve 5 connected to PRC-08 Valve 6 connected to MFC-01 Valve 7 Mixer-01

Table A.10.3: *LOPA analysis. Initial failure probability P_f and severity of the different initiating events.*

Node	Initiating event	Initial P_f *[-]*	Initial Severity *[-]*	Final P_f *[-]*	Final Severity *[-]*
1	Set a wrong set point in at least one of MFC-01/02/03	0.9	0.8	$1.4 \cdot 10^{-7}$	0.8
	Set a wrong set point in MFC-04	0.9	0.4	$1.4 \cdot 10^{-5}$	0.4
	A power outage	0.9	0.8	$1.4 \cdot 10^{-6}$	0.8
2	Wrong value at PI-01	0.9	0.8	$1.8 \cdot 10^{-7}$	0.8
	Incorrect reactor packing	0.9	0.8	$5.0 \cdot 10^{-4}$	0.8
	Wrong set point in PRC-09	0.9	0.8	$5.0 \cdot 10^{-4}$	0.8
	Wrong set point in TC-01	0.9	0.8	$5.0 \cdot 10^{-4}$	0.8
	Wrong set point of temperature (start-up)	0.9	0.8	$5.0 \cdot 10^{-4}$	0.8
	Leakage/defective connection	0.9	0.8	$3.7 \cdot 10^{-1}$	0.8
	Reactor opening before closing the feed line(s)	0.9	0.8	$3.7 \cdot 10^{-1}$	0.8
	Reactor closing after opening the feed line(s)	0.9	0.8	$3.7 \cdot 10^{-1}$	0.8
	A power outage	0.9	0.8	$5.0 \cdot 10^{-3}$	0.8
3	Wrong set point in PRC-09	0.9	0.8	$5.0 \cdot 10^{-4}$	0.8
	PI-02 failure	0.9	0.8	$5.0 \cdot 10^{-5}$	0.8
	A power outage	0.9	0.8	$5.0 \cdot 10^{-5}$	0.8

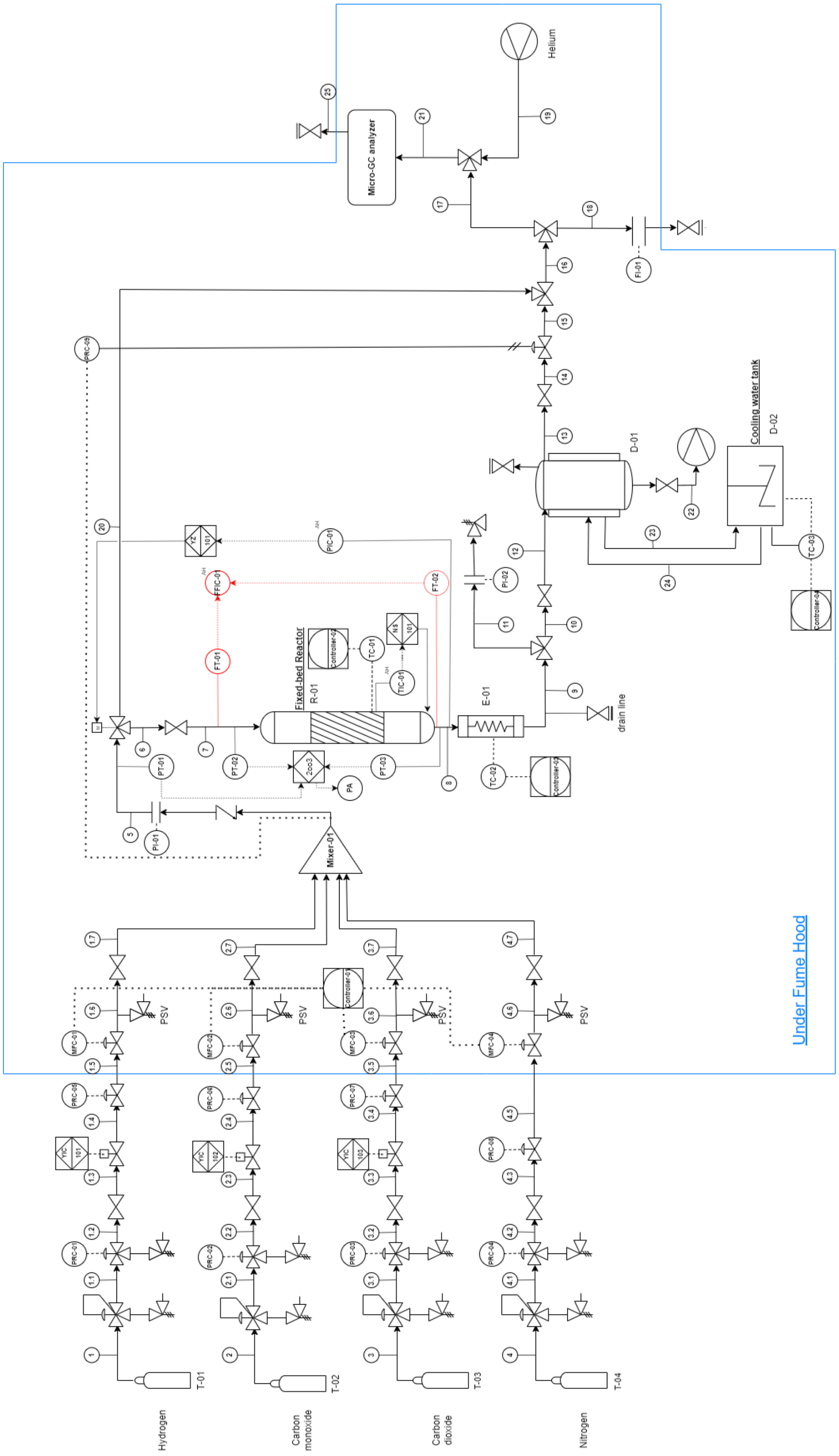


Figure A.10.1: *Improved P&ID of the pilot plant embedding modification from the combined HAZOP and LOPA analyses.*

Nomenclature

C = Cost of damage (€)
C_{max} = Maximum cost of damage (€)
D = Severity (-)
$\mathrm{E_{TNT}}$ = Explosive energy of TNT (4686 kJ/kg)
f = Frequency of the event ($\mathrm{yr^{-1}}$)
H_i = Heat of formation of species i (kJ/mol)
L = Likelihood (-)
m = Mass of the flammable substance (kg)
$\mathrm{m_{TNT}}$ = Equivalent mass of TNT (kg)
P_f = Mean probability of failure (-)
R = Risk (-)
RC = Risk Class (-)
S = Severity (-)
t = Time (years)

Greek letters

ΔH°_{298} = Standard enthalpy of reaction at 298 K (kJ/mol)
ΔH_R = Heat of reaction (kJ/mol)
ΔP = Difference between outlet and inlet pressures (bar)
η = Reactivity coefficient (-)
v_i = Stoichiometric coefficient (-)

Acronyms

ACS = American Chemical Society
ALARP = As Low As Reasonably Practicable
ATEX = Atmosphere Explosible
BPCS = Basic Process Control System
BST = Baker-Strehlow-Tang method
DDT = Deflagration to detonation transition
DSC = Differential Scanning Calorimeter
ETA = Event Tree Analysis
FC = Fail to close
FKM = Fluorine Kautschuk Material

FMEA = Failure Modes and Effects Analysis
FO = Fail to open
FT = Fischer Tropsch
FT = Flow Transmitter (equipment)
FTA = Fault Tree Analysis
FTIR = Fourier Transform Infrared
GC = Gas Chromatography
HAZOP = Hazard and Operability
H&RA = Hazard and Risk Assessment
IE = Initiating Event
IEF = Initiating Event Frequency
IPL = Independent Protection Layer
IRT = IPL Response Time
LEL = Lower Explosive Limit
LFL = Lower Flammable Limit
LOPA = Layer of Protection Analysis
MA FACE = Massachusetts Fatality Assessment and Control Evaluation
MAWP = Maximum Allowable Working Pressure
MFC = Mass-Flow Controller
MMC = Multiple Module Calorimeter
MOC = Management of Change
MooN = *M* out of *N* channel architecture
MSDS = Material Safety Data Sheet
MSP = Maximum Setpoint
MTTF = Mean time to failure
NFPA = The National Fire Protection Association
NGAP = Next Generation Advanced Procedures
OSHA = Occupational Safety and Health Administration
PA = Pressure Alarm
P&ID = Piping and Instrumentation Diagram
PCTFE = Polychlorotrifluoroethylene
PFD = Process Flow Diagram (Chapter 1 and 2)
PFD = Probability of Failure on Demand (Chapter 3 and 4)
PhD = Doctor of Philosophy
PI = Principal Investigator
PI = Pressure Indicator (equipment)
PIAH = High-Pressure Indicator and Alarm
PIC = Pressure Indicator Controller

PLT = Process Lag Time
PSV = Pressure Safety Valve
PRC = Pressure Recording Controller
PT = Pressure Transmitter
PTFE = Polytetrafluoroethylene
RAMP = Recognize hazards, Assess risk of hazard, Minimize risk of hazards, Prepare for emergencies
RC = Risk class
R&D = Research and Development
RRF = Risk Reduction Factor
SCAI = Safety controls, alarms and interlocks
SDSs = Safety Data Sheets
SIF = Safety Instrumented Function
SIL = Safety Integrity Level
SIS = Safety Instrumented System
SME = Subject Matter Expert
SOPs = Standard Operating Procedures
SP = Set-point
SS = Stainless Steel
TC = Temperature controller
TIC = Temperature Indicator Controller
TNO-MEM = TNO Multi Energy Method
TNT = Trinitro Toluene
UCD = User- Centered Design
UEF = Unmitigated event frequency
UEL = Upper Explosive Limit
UFL = Upper Flammable Limit

References

[1] S. Vidal, Safety First: A Recent Case of a Dichloromethane Injection Injury, ACS Cent. Sci. 6 (2020) 83–86. https://doi.org/10.1021/acscentsci.0c00100.

[2] The Laboratory Safety Institute, Memorial Wall-Killed in Lab Accident, (n.d.). https://www.labsafety.org/memorial-wall (accessed August 19, 2023).

[3] S. Ezenwa, A.D. Talpade, P. Ghanekar, R. Joshi, J. Devaraj, F.H. Ribeiro, R. Mentzer, Toward Improved Safety Culture in Academic and Industrial Chemical Laboratories: An Assessment and Recommendation of Best Practices, ACS Chem. Heal. Saf. 29 (2022) 202–213. https://doi.org/10.1021/acs.chas.1c00064.

[4] P. Reed, L.S. Marin, M. Zreiqat, Impact of Toolbox Training on Risk Perceptions in Hazardous Chemical Settings: A Case Study from a Bleach Processing Plant, ACS Chem. Heal. Saf. 30 (2023) 129–138. https://doi.org/10.1021/acs.chas.3c00041.

[5] CCPS (Center for Chemical Process Safety), Handbook for Process Safety in Laboratories and Pilot Plants: A Risk-based Approach, John Wiley & Sons, Inc., 2023.

[6] Sigma-Aldrich, Safety Data Sheet: Dichloromethane, (n.d.). https://www.sigmaaldrich.com/IT/en/sds/sial/270997 (accessed August 21, 2023).

[7] N. Langerman, Reactive chemistry incidents in laboratories, J. Chem. Heal. Saf. 16 (2009) 23–26. https://doi.org/10.1016/j.jchas.2008.04.003.

[8] N. Langerman, Management of Change for Laboratories and Pilot Plants, Org. Process Res. Dev. 12 (2008) 1305–1306. https://doi.org/10.1021/op8001855.

[9] D. Hendershot, A. Ness, Pilot Plant Reactive Chemistry Incidents: Case Studies and Prevention, AIChE Annu. Meet. Conf. Proc. (2005). https://www.researchgate.net/publication/228661125_Pilot_Plant_Reactive_Chemistry_Incidents_Case_Studies_and_Prevention.

[10] R.H.J. Hill, Recognizing and understanding hazards — The key first step to safety, J. Chem. Heal. Saf. 26 (2019) 5–10. https://doi.org/10.1016/j.jchas.2018.11.005.

[11] N. Langerman, Lab-scale process safety management, J. Chem. Heal. Saf. 16 (2009) 22–28. https://doi.org/10.1016/j.jchas.2008.09.013.

[12] CDC, Pilot Plant Operator Killed in Pressure Vessel Release at a Massachusetts Biotechnology Company, (1994) 1–7. https://www.cdc.gov/niosh/face/stateface/ma/94ma019.html#print (accessed August 17, 2023).

[13] CDC, Fatality Assessment and Control Evaluation(FACE) Program, (n.d.). https://www.cdc.gov/niosh/face/default.html (accessed August 24, 2023).

[14] M.P. Jones, K. Weiland, C. Mitterer, P. Verdross, R.T. Woodward, A. Bismarck, Insights from a laboratory fire, Nat. Chem. 15 (2023) 885–889. https://doi.org/10.1038/s41557-023-01254-6.

[15] A. Silver, Fatal lab explosion in China highlights wider safety fears, Nature. 601 (2022) 176–177. https://doi.org/10.1038/d41586-021-03589-x.

[16] Z. Lu, Analysis of China students' laboratory accidents in the past 39 years and the laboratory management reform in the future, Educ. Chem. Eng. 42 (2023) 54–60. https://doi.org/10.1016/j.ece.2022.12.001.

[17] S. Kong, P. Yang, X. Fang, Z. Yang, C. Tang, W. Wang, C. Ying, Analysis of Characteristics of Safety Accidents in University Laboratory and Research on the Causes of Accidents, E3S Web Conf. 257 (2021) 3–6. https://doi.org/10.1051/e3sconf/202125703050.

[18] M. Chen, Y. Wu, K. Wang, H. Guo, W. Ke, An explosion accident analysis of the laboratory in university, Process Saf. Prog. 39 (2020) e12150. https://doi.org/https://doi.org/10.1002/prs.12150.

[19] J.F. McCarthy, M.A. Fragala, B.J. Baker, Analyzing the Risk: Balancing Safety and Efficiency in Laboratory Ventilation, ACS Chem. Heal. \& Saf. 29 (2022) 434–440. https://doi.org/10.1021/acs.chas.1c00095.

[20] R. Palluzi, The Ten Most Common Laboratory Safety Issues, ACS Chem. Heal. Saf. 29 (2022) 19–26. https://doi.org/10.1021/acs.chas.1c00063.

[21] D. Wang, C. Pan, L. Wang, Design and Practice of an Organic Analysis Laboratory to Enhance Laboratory Safety, ACS Chem. Heal. \& Saf. 28 (2021) 238–243. https://doi.org/10.1021/acs.chas.1c00008.

[22] European Commission, Equipment for potentially explosive atmospheres (ATEX), (n.d.). https://single-market-economy.ec.europa.eu/sectors/mechanical-engineering/equipment-potentially-explosive-atmospheres-atex_en#:~:text=EU legislation and ATEX,placed on the EU market. (accessed October 18, 2023).

[23] H.A. Aziz, A.M. Shariff, R. Rusli, K.H. Yew, Managing process chemicals, technology and equipment information for pilot plant based on Process Safety Management standard, Process Saf. Environ. Prot. 92 (2014) 423–429. https://doi.org/10.1016/j.psep.2014.02.011.

[24] I.M. Nasrallah, A.K. El Kak, L.A. Ismaiil, R.R. Nasr, W.T. Bawab, Prevalence of Accident Occurrence Among Scientific Laboratory Workers of the Public University in Lebanon and the Impact of Safety Measures, Saf. Health Work. 13 (2022) 155–162. https://doi.org/10.1016/j.shaw.2022.02.001.

[25] H.E. Simmons, B. Matos, S.A. Simpson, Analysis of injury data to improve safety and training, J. Chem. Heal. Saf. 24 (2017) 21–28. https://doi.org/10.1016/j.jchas.2016.03.004.

[26] R. Palluzi, Code Considerations for the Design of Laboratories Which Will Also House Pilot Plants, ACS Chem. Heal. \& Saf. 27 (2020) 267–271. https://doi.org/10.1021/acs.chas.0c00053.

[27] A S Hornby, Oxford Advanced Learner's Dictionary, 8th Editio, Oxford University Press, Oxford, 2010.

[28] Billings Clinic, The Scientific Method vs. Engineering Design Process, (n.d.). https://www.billingsclinic.com/scienceexpo/scientific-method/ (accessed September 23, 2023).

[29] C.Ö. Çaparlar, A. Dönmez, What is Scientific Research and How Can it be Done?, Turkish J. Anaesthesiol. Reanim. 44 (2016) 212–218. https://doi.org/10.5152/TJAR.2016.34711.

[30] Indeed Editorial Team, The 7 Steps of the Engineering Design Process, (2023). https://www.indeed.com/career-advice/career-development/design-process (accessed

September 23, 2023).

[31] S.C. Peres, Human Factors Guidance for Writing Effective Laboratory Standard Operating Procedures, ACS Chem. Heal. \& Saf. 29 (2022) 476–484. https://doi.org/10.1021/acs.chas.2c00056.

[32] H.A. Aziz, M.R. Othman, A.M. Shariff, L.S. Tan, Application of analytical hierarchy process (AHP) in prioritizing HAZOP analysis for pilot plant, Chem. Eng. Res. Bull. 19 (2017) 87. https://doi.org/10.3329/cerb.v19i0.33801.

[33] European Commision, Chemicals legislation, (n.d.). https://single-market-economy.ec.europa.eu/sectors/chemicals/chemicals-legislation_en (accessed September 23, 2023).

[34] The British Standards Institution, BS EN 61511-3:2017, “Functional safety — Safety instrumented systems for the process industry sector- Part 3 : Guidance for the determination of the required safety integrity levels,” 2017. https://bsol.bsigroup.com/.

[35] R. Zhao, T.R. Furman, M. Roth, MSD’s Process Safety Scale-Up Methodology for Pilot Plant Scale and Beyond, Org. Process Res. Dev. 25 (2021) 2566–2577. https://doi.org/10.1021/acs.oprd.1c00360.

[36] T.A. Kletz, P. Amyotte, Process Plants: A Handbook for Inherently Safer Design, Second Edition, 2nd ed., CRC Press/Taylor & Francis Group, 2010.

[37] T. Adamopoulou, M.I. Papadaki, M. Kounalakis, V. Carreto, A. Pineda, M.S. Mannan, Use of isoperibolic calorimetry for the study of the effect of water concentration, temperature and reactor venting on the rate of hydroxylamine thermal decomposition, J. Loss Prev. Process Ind. 25 (2012) 803–808. https://doi.org/10.1016/j.jlp.2012.03.002.

[38] G. Pio, P. Mocellin, C. Vianello, E. Salzano, A detailed kinetic model for the thermal decomposition of hydroxylamine, J. Hazard. Mater. 416 (2021) 125641. https://doi.org/10.1016/j.jhazmat.2021.125641.

[39] D.A. Crowl, J.F. Louvar, Chemical process safety : Fundamentals with applications, 2. ed, Prentice Hall, Upper Saddle River, n.d.

[40] Consequence Analysis, in: Guidel. Chem. Process Quant. Risk Anal., John Wiley & Sons, Ltd, 2010: pp. 57–296. https://doi.org/https://doi.org/10.1002/9780470935422.ch2.

[41] G. De Smedt, F. De Corte, R. Notelé, J. Berghmans, Comparison of two standard test methods for determining explosion limits of gases at atmospheric conditions, J. Hazard. Mater. 70 (1999) 105–113. https://doi.org/10.1016/S0304-3894(99)00163-6.

[42] R. Stuart, E. Sweet, M. Labosky, M. Box, M.B. Mulcahy, Safe Lab Design: A Call for Papers, ACS Chem. Heal. \& Saf. 28 (2021) 144–147. https://doi.org/10.1021/acs.chas.1c00034.

[43] T.C. Smith, How Many Air Changes Are Required For Safety? A Risk-Based Approach for Establishing Ventilation Specifications in Laboratories and Critical Workspaces, ACS Chem. Heal. \& Saf. 29 (2022) 335–343. https://doi.org/10.1021/acs.chas.2c00007.

[44] CCPS (Center for Chemical Process Safety), Guidelines for hazard evaluation procedures, 3rd ed., John Wiley & Sons, Inc., 2008.

[45] AIChE, Chemical Reactivity Worksheet, (n.d.). https://www.aiche.org/ccps/resources/chemical-reactivity-worksheet (accessed May 24, 2023).

[46] F. Crawley, B. Tyler, HAZOP: Guide to Best Practice, 3rd ed., Elsevier, 2015. https://doi.org/https://doi.org/10.1016/C2014-0-04859-9.

[47] The British Standards Institution, BS EN 61882:2016, "Hazard and operability studies (HAZOP studies) — Application guide," 2016. https://bsol.bsigroup.com/.

[48] P. Clarke, Functional Safety from Scratch, Elsevier, 2023. https://doi.org/10.1016/C2022-0-01455-0.

[49] The British Standards Institution, BS EN 61511-1:2017+A1:2017, "Functional safety-Safety instrumented systems for the process industry sector- Part 1: Framework, definitions, system, hardware and application programming requirements," 2017. https://bsol.bsigroup.com/.

[50] The British Standards Institution, BS EN 61511-2:2017, "Functional safety - Safety instrumented systems for the process industry sector- Part 2: Guidelines for the application of IEC 61511-1 (IEC 61511-2:2016)," 2017. https://bsol.bsigroup.com/.

[51] CCPS (Center for Chemical Process Safety), Guidelines for initiating events and independent protection layers in layer of protection analysis, John Wiley & Sons, Inc., Hoboken, New Jersey, 2015.

[52] W.M. Goble, H. Cheddie, Safety Instrumented Systems Verification: Practical Probabilistic Calculations, ISA - The Instrumentation, Systems and Automation Society, 2005.

[53] exida, SILSafeData, (2023). https://silsafedata.com/ (accessed October 13, 2023).

[54] American Petroleum Institute, API Standard 520, "Sizing, Selection, and Installation of Pressure-relieving Devices. Part I: Sizing and Selection," 2014. https://www.api.org/.

[55] American Petroleum Institute, API STD 520 Part 1: Sizing, Selection, and Installation of Pressure-Relieving Devices in Refineries, (2023). https://www.apiwebstore.org/standards/520__Part_1 (accessed October 30, 2023).

[56] G. Evans, C. Smith, Biomass to liquids technology, Elsevier Ltd., 2012. https://doi.org/10.1016/B978-0-08-087872-0.00515-1.

[57] J.A. Moulijn, M. Makkee, A.E.: van Diepen, J.A. Moulijn, Chemical process technology, (2013).

[58] The British Standards Institution, BS EN ISO 11114-1:2020, "Gas cylinders. Compatibility of cylinder and valve materials with gas contents - Part 1: Metallic materials," 2020. https://bsol.bsigroup.com/.

[59] The British Standards Institution, BS EN ISO 11114-2:2021,"Transportable gas cylinders — Compatibility of cylinder and valve materials with gas contents — Part 2: Non-metallic materials", 2021. https://bsol.bsigroup.com/.

[60] R.K. Sinnott, G.P. Towler, Chemical engineering design, 6th ed., Butterworth-Heinemann, Oxford, 2020.

[61] R.K. Sinnott, G.P. Towler, Corrosion Chart, Chem. Eng. Des. (2020) e1–e19. https://doi.org/10.1016/b978-0-08-102599-4.09991-4.

[62] Work Metal S.p.A., Compatibility table, (n.d.). https://www.metalwork.it/media/Stumenti_manuali/Tab_compatibilita_19_02_2019.pdf (accessed April 26, 2023).

[63] The British Standards Institution, BS EN IEC 60079-10-1:2021, "Explosive atmospheres Part

10-1: Classification of areas - Explosive gas atmospheres,” 2021. https://bsol.bsigroup.com/.

[64] The British Standards Institution, PD IEC/TS 60079-46:2017, “Explosive atmospheres Part 46: Equipment assemblies,” 2017. https://bsol.bsigroup.com/.

[65] D.A. Crowl, J.F. Louvar, Chemical process safety : Fundamentals with applications, 2. ed, Prentice Hall PTR, Upper Saddle River, 2002.

[66] M. Sharifian, F. Galli, B. Timbers, N. Hudon, G.S. Patience, Safety analysis and risk assessment of a Micro-GtL Plant, J. Loss Prev. Process Ind. 83 (2023) 105071. https://doi.org/10.1016/j.jlp.2023.105071.

[67] The British Standards Institution, BS EN 764-7:2002, “Pressure equipment — Part 7: Safety systems for unfired pressure vessels,” 2002. https://bsol.bsigroup.com/.

[68] ABB, Manuale tecnico di riferimento Parametri di sistema, 20th Sept. 2023. (2023). https://search.abb.com/library/Download.aspx?DocumentID=3HAC050948-007&LanguageCode=it&DocumentPartId=&Action=Launch (accessed October 13, 2023).

[69] S.-W. Jeen, S. Lazar, L. Gui, R.W. Gillham, Degradation of chlorofluorocarbons using granular iron and bimetallic irons., J. Contam. Hydrol. 158 (2014) 55–64. https://doi.org/10.1016/j.jconhyd.2014.01.002.

[70] M.D. Greenhalgh, A.S. Jones, S.P. Thomas, Iron-catalysed hydrofunctionalisation of alkenes and alkynes, 2015. https://doi.org/10.1002/cctc.201402693.

[71] Q. sheng ZHOU, C. LI, X. bin LI, Z. hong PENG, G. hua LIU, T. gui QI, Reaction behavior of ferric oxide in system Fe2O3–SiO2–Al2O3 during reductive sintering process, Trans. Nonferrous Met. Soc. China (English Ed. 26 (2016) 842–848. https://doi.org/10.1016/S1003-6326(16)64175-4.

[72] M. Zhou, L. Zhang, H. Lu, L. Shao, M. Chen, Reaction of silicon dioxide with water: A matrix isolation infrared and density functional theoretical study, J. Mol. Struct. 605 (2002) 249–254. https://doi.org/10.1016/S0022-2860(01)00767-0.

[73] T. Mori, W. Ueda, Y. Morikawa, Hydrodechlorinative dimerization of 1,1,1-trifluorohaloethanes over Ru/SiO2 catalyst, Catal. Letters. 38 (1996) 73–76. https://doi.org/10.1007/BF00806902.

[74] X. Yong, J.S. Tse, J. Chen, Mechanism of Chemical Reactions between SiO2 and CO2 under Mantle Conditions, ACS Earth Sp. Chem. 2 (2018) 548–555. https://doi.org/10.1021/acsearthspacechem.7b00144.

[75] M.J. Mitchell, O.E. Jensen, K.A. Cliffe, M.M. Maroto-Valer, A model of carbon dioxide dissolution and mineral carbonation kinetics, Proc. R. Soc. A Math. Phys. Eng. Sci. 466 (2010) 1265–1290. https://doi.org/10.1098/rspa.2009.0349.

[76] H. Idriss, M. Scott, V. Subramani, 1 - Introduction to hydrogen and its properties, in: V. Subramani, A. Basile, T.N.B.T.-C. of H.E. Veziroğlu (Eds.), Woodhead Publ. Ser. Energy, Woodhead Publishing, Oxford, 2015: pp. 3–19. https://doi.org/https://doi.org/10.1016/B978-1-78242-361-4.00001-7.

[77] NOAA, CAMEO Chemicals, (n.d.). https://cameochemicals.noaa.gov/ (accessed April 26, 2023).

[78] H.H.B.T.-S. in S.S. and C. Kung, ed., Chapter 13 Catalytic Reaction Between Hydrogen and Carbon Oxides, in: Transit. Met. Oxides, Elsevier, 1989: pp. 227–251. https://doi.org/https://doi.org/10.1016/S0167-2991(08)60936-2.

[79] V. Pattabathula, J. Richardson, Introduction to ammonia production, Chem. Eng. Prog. 112 (2016) 69–75. https://www.aiche.org/resources/publications/cep/2016/september/introduction-ammonia-production.

[80] R.A. Gardner, The kinetics of silica reduction in hydrogen, J. Solid State Chem. 9 (1974) 336–344. https://doi.org/https://doi.org/10.1016/0022-4596(74)90092-9.

[81] S. Pillot, L. Coudreuse, 2 - Hydrogen-induced disbonding and embrittlement of steels used in petrochemical refining, in: R.P. Gangloff, B.P.B.T.-G.H.E. of M. in E.T. Somerday (Eds.), Woodhead Publ. Ser. Met. Surf. Eng., Woodhead Publishing, 2012: pp. 51–93. https://doi.org/https://doi.org/10.1533/9780857093899.1.51.

[82] R. Sivaramakrishnan, M.-C. Su, J. V Michael, S.J. Klippenstein, L.B. Harding, B. Ruscic, Rate Constants for the Thermal Decomposition of Ethanol and Its Bimolecular Reactions with OH and D: Reflected Shock Tube and Theoretical Studies, J. Phys. Chem. A. 114 (2010) 9425–9439. https://doi.org/10.1021/jp104759d.

[83] P.W. Musch, B. Engels, The Importance of the Ene Reaction for the C2−C6 Cyclization of Enyne−Allenes, J. Am. Chem. Soc. 123 (2001) 5557–5562. https://doi.org/10.1021/ja010346p.

[84] W.M.T.M. Reimerink, The use of activated carbon as catalyst and catalyst carrier in industrial applications, in: A.B.T.-S. in S.S. and C. Dąbrowski (Ed.), Adsorpt. Its Appl. Ind. Environ. Prot., Elsevier, 1999: pp. 751–769. https://doi.org/https://doi.org/10.1016/S0167-2991(99)80571-0.

[85] M.A. Uddin, E.M. Kennedy, B.Z. Dlugogorski, Gas-phase reaction of CCl2F2 (CFC-12) with methane, Chemosphere. 53 (2003) 1189–1191. https://doi.org/10.1016/S0045-6535(03)00658-1.

[86] H. Takahashi, S. Hisaoka, T. Nitta, Ethanol oxidation reactions catalyzed by water molecules:, Chem. Phys. Lett. 363 (2002) 80–86. http://linkinghub.elsevier.com/retrieve/pii/S0009261402011429.

[87] R.J. Lewis, Sax's dangerous properties of industrial materials, Choice Rev. Online. 30 (1993) 30-2435-30–2435. https://doi.org/10.5860/choice.30-2435.