Management of cyber-physical risks in the process industry

Tamara Oueidat

THÈSE

Pour obtenir le grade de

DOCTEUR DE L'UNIVERSITÉ GRENOBLE ALPES

Spécialité : AUTOMATIQUE - PRODUCTIQUE

Arrêté ministériel : 25 mai 2016

Présentée par

Tamara OUEIDAT

Thèse dirigée par **Jean-Marie FLAUS** ,Professeur
et co-encadrée par **François MASSE**

préparée au sein du **Laboratoire des Sciences pour la Conception, l'Optimisation et la Production de Grenoble**
dans **l'École Doctorale Electronique, Electrotechnique, Automatique, Traitement du Signal (EEATS)**

Maitrise des risques cyber-physiques dans l'industrie du procédé

Management of cyber-physical risks in the process industry

Thèse soutenue publiquement le **12 juillet 2022**,
devant le jury composé de :

Monsieur Jean-Marie FLAUS
PROFESSEUR, Université Grenoble Alpes , Directeur de thèse
Monsieur Frédéric KRATZ
PROFESSEUR, INSA Centre Val de Loire, Rapporteur
Monsieur Gilles DUSSERRE
PROFESSEUR, IMT Mines Alès, Rapporteur
Madame Maria DI MASCOLO
DIRECTEUR DE RECHERCHE, CNRS, Présidente
Monsieur Laurent CIARLETTA
MAITRE DE CONFERENCE, Université de Lorraine, Examinateur
Monsieur Emmanuel SIMEU
MAITRE DE CONFERENCE, Université Grenoble Alpes, Examinateur
Monsieur François MASSE
INGENIEUR, INERIS , Co-directeur de thèse

"For last year's words belong to last year's language
And next year's words await another voice.
And to make an end is to make a beginning..."

T.S. ELIOT

Remerciements

En préambule à cette thèse, je souhaite adresser mes remerciements les plus sincères à tous ceux qui m'ont apporté leur aide et qui ont contribué de près ou de loin à l'élaboration de ce travail.

Je tiens tout d'abord à exprimer ma vive reconnaissance envers Jean-Marie FLAUS, mon directeur de thèse, qui s'est toujours montré à l'écoute tout au long de la réalisation de cette thèse. Je le remercie pour son excellent encadrement, l'aide et le temps qu'il a bien voulu me consacrer, et pour la confiance qu'il a pu m'accorder. Son intérêt et ses précieux conseils m'ont été d'un grand profit. Ce fut un réel plaisir d'avoir été son étudiante.

Je remercie sincèrement François MASSE, mon encadrant de thèse, pour avoir consacré une partie de son temps au suivi de cette thèse. Son écoute et ses conseils avisés ont été précieux et un profit pour l'aboutissement de ces travaux.

Mes remerciements s'adressent également à Fréderic KRATZ et Gilles DUSSERRE, pour avoir accepté d'être les rapporteurs de ma thèse. J'exprime également ma profonde gratitude à tous les membres du jury qui me font l'honneur de participer à ce travail d'évaluation.

J'aime également remercier les membres du laboratoire G-SCOP, service administratif, permanents, doctorants et amis, qui ont rendu mes passages au labo, tellement agréables et conviviaux. Merci pour leur soutien et les bons moments avec eux.

Je tiens à exprimer toute ma gratitude à mes parents, ma sœur et mon frère, qui m'ont toujours soutenu, avec leurs encouragements et leur amour, pour aller jusqu'au bout de mes rêves. Je leur dédie cette thèse, car c'est grâce à eux que j'en suis là aujourd'hui. Je dédie la thèse aussi à mon neveu, mon petit prince qui est arrivé à la fin de thèse…

J'adresse mes profonds remerciements finalement à une personne spéciale,
Farid, qui m'encouragé à faire cette thèse et qui a participé à son aboutissement.
Merci d'être toujours présent à mes côtés pour me soutenir, m'encourager, me conseiller, et m'aimer…

Résumé

La réglementation française définit les installations classées (IC) comme des exploitations industrielles susceptibles de créer des risques ou de provoquer des pollutions ou nuisances, notamment pour la sécurité et la santé des riverains. Différents régimes sont définis pour les installations classées, en fonction de l'importance des risques. Les installations présentant les risques les plus importants – identifiés sur la base de la nomenclature des installations classées qui fixe des seuils en fonction des quantités de substances dangereuses employées ou stockées sur le site et du type d'activité – sont soumises au régime de l'autorisation.

Pour démontrer l'acceptabilité des risques, l'exploitant d'une IC soumise à autorisation réalise une Étude de Danger (EDD). L'analyse des risques est au cœur du processus de l'EDD. L'objectif est de recenser l'ensemble des phénomènes dangereux et accidents majeurs liés à l'installation et pouvant avoir des effets à l'extérieur du site, d'identifier les séquences d'événements qui mènent à ces phénomènes (scénarios d'accident) et d'évaluer leur intensité et gravité (distance d'effet et nombre de personnes potentiellement exposées) et leur probabilité d'occurrence.

L'évaluation de la probabilité dans les EDD a été instaurée dans le code de l'environnement par la loi du 30 Juillet 2003. Les probabilités et les gravités sont estimées selon des échelles définies dans l'annexe 1 de l'arrêté ministériel du 29 Décembre 2005. Le couple gravité/probabilité permet de situer les différents accidents identifiés dans une matrice d'acceptabilité et ainsi d'apprécier l'acceptabilité des risques d'accidents majeurs.

L'INERIS réalise différents types d'études pour les sites à risque de l'industrie du procédé qui couvrent l'ensemble du processus de maitrise des risques accidentels liées aux installations classées. Ces études comprennent par exemple les analyses de risques ou les évaluations des mesures de maitrise des risques réalisées dans le cadre d'études de danger.

La cyber sécurité n'est pas intégrée aux scénarios d'accidents déterminés dans le cadre des EDD. Or, elle apparait de plus en plus comme un sujet critique pour les sites industriels : ceux-ci deviennent en effet de plus en plus vulnérables aux

cyberattaques du fait leur numérisation et connectivité croissantes et de l'utilisation des technologies issues de l'IT dans les systèmes de contrôle industriel (OT). Les attaques visant ces systèmes peuvent notamment avoir des conséquences sur la maitrise des risques physiques pour les populations et l'environnement. L'INERIS souhaite donc intégrer les problématiques de la cyber sécurité dans les différentes étapes de la maitrise des risques que font peser les installations classées sur les personnes et l'environnement.

Les méthodes d'analyse des risques et les moyens de prévention des risques accidentels ne sont pas adaptés à traiter et analyser les risques liés à la cyber sécurité, et ces derniers sont rarement évalués et lorsqu'ils le sont, sont évalués dans des processus et des études dissociées des analyses des risques accidentels. L'objectif de cette thèse était donc de développer une nouvelle méthode d'analyse des risques intégrant les risques liés à la cyber sécurité avec les risques accidentels. La méthode d'analyse doit prendre en compte la spécificité des installations de l'industrie du procédé et être applicable en maitrisant la complexité et le nombre des scénarios potentiels. Pour cela, la mise en œuvre de cette méthode doit être facilitée par des données propres aux systèmes industriels telles que des guides sur les vulnérabilités génériques, ou des méta-modèles pour représenter les différents scénarios d'attaques. Cela permet de générer et de chercher automatiquement les scenarios d'attaques à partir des données collectées sur l'installation industrielle combinés avec les scénarios accidentels extraits d'une étude de danger et des méta-modèles. Ces données sont combinées dans un même nœud papillon appelé cyber nœud papillon.

En outre, l'évaluation du risque pour des scénarios combinant la sûreté et la sécurité en termes du niveau de gravité et de vraisemblance représente une étape importante pour déterminer le niveau de criticité du scenario de risque et mettre en place des mesures et des barrières de sécurité pour diminuer ou éliminer les risques non acceptables. Pour cela, dans la méthode d'analyse des risques développée, les étapes de l'évaluation et du traitement des risques combinés sont prises en considération. Les vraisemblances des risques combinées sont évaluées selon un vecteur à deux dimensions représentant la vraisemblance des événements de cyber sécurité et les événements de sûreté puisqu'il existe différents concepts pour définir la vraisemblance liée à la sûreté et à la cyber sécurité. La combinaison des risques cyber sécurité et sûreté dans un même nœud papillon et l'évaluation des niveaux des différents types de scénarios des risques fournissent une représentation exhaustive des scénarios des risques en termes de sûreté et de sécurité.

Abstract

French regulations define classified installations (IC) as industrial operations likely to create risks or cause pollution or nuisances, particularly for the safety and health of local residents. Different schemes are defined for classified facilities, depending on the importance of the risks. Facilities presenting the highest risks – identified on the basis of the nomenclature of classified facilities, which sets thresholds according to the quantities of hazardous substances used or stored on the site and the type of the activity – are subject to the authorization scheme.

To demonstrate the acceptability of the risks, the operator of an IC subject to the authorization produces a Safety report (EDD). The risk analysis is at the heart of the EDD. The objective is to identify all the hazardous phenomena and major accidents associated with the facility that could have effects outside the industrial site, to identify the sequences of events that lead to these phenomena (accident scenarios) and to assess their intensity and severity (distance of effect and number of people potentially exposed) and their probability of occurrence.

The assessment of the probability in the EDD was introduced in the French environmental code by the law of July 30, 2003. The probability and severity are estimated according to the scales defined in Annex 1 of the ministerial order of 29 September 2005. The severity/probability pairing enables the identified various accidents to be placed in an acceptability matrix and thus to assess the acceptability of the risks of major accidents.

INERIS carries out various types of studies for hazardous sites in the process industry that cover the entire process of accidental risk management related to the classified installations. These studies include, for example, risk analysis or assessment of risk control measures carried out as part of EDD.

Cybersecurity is not included in the accident scenarios determined in the framework of the EDD. However, it appears more and more as a critical issue for industrial sites: they are indeed becoming more and more vulnerable to cyberattacks due to their increasing of the digitization, the connectivity and the use of IT technologies in industrial control systems (ICS). Attacks on these systems can have consequences on the management of physical risks for people

and the environment. Therefore, INERIS wishes to integrate cybersecurity issues into the various stages of the management of the risks on industrial installations that can have harm on people and the environment.

Risk analysis approaches and accidental risk prevention means are not adapted to deal with and analyze the risks related to cybersecurity, and the latter are rarely evaluated and when they are, they are evaluated in processes and studies dissociated from the accidental risk analysis. The objective of this thesis was therefore to develop a new risk analysis approach integrating the cybersecurity risks with the accidental risks. The analysis approach must consider the specificity of the process industry installations and be applicable by controlling the complexity and the number of potential scenarios. For this, the implementation of this approach must be facilitated by specific data to the industrial system such as the generic vulnerability guides and meta-models to represent the different attack scenarios. This allows to automatically generate and search the attack scenarios, from data collected on the industrial installation combined with the accidental scenarios extracted from a hazard study and meta-models. These data are combined in a single Bow-Tie called Cyber Bow-Tie.

In addition, the risk assessment for combined safety and cybersecurity scenarios in terms of the severity and likelihood levels represents an important step to determine the criticality level of the risk scenario and to implement safety measures and barriers to reduce or eliminate the unacceptable risks. For this purpose, in the developed risk analysis approach, the steps of the evaluation and treatment of the combined risks are taken into consideration. The combined risks likelihoods are evaluated according to a two-dimensional vector representing respectively the likelihood of cybersecurity events and safety events since there are different concepts to define the likelihood related to safety and cybersecurity. Combining safety and cybersecurity risks in a single Bow-Tie and evaluating the levels of different types of risk scenarios provides a comprehensive representation of safety and cybersecurity risk scenarios.

Contents

List of tables

List of figures

Abbreviations

AADL	*Architecture Analysis and Design Language*
ANSSI	*Agence Nationale de la Sécurité des Systèmes d'information*
ATBT	*Attack Tre, Bow-Tie*
BDMP	*Boolean Logic Driven Markov Process*
CDA	*Control Digital Asset*
CFT	*Component Failure Tree*
CHASSIS	*Combined Harm Assessment of Safety and Security for Information system*
CIM	*Computer-Integrated Manufacturing*
CORAS	*Credibility of Risk Assessment*
CPS	*Cyber-Physical System*
CR	*Control Risk*
CVE	*Common Vulnerabilities and Exposures*
DFD	*Data Flow Diagram*
EBIOS RM	*Expression des Besoins et Identification des Objectifs de Sécurité – Risk Manager*
EFT	*Extended Fault Tree*
FACT	*Failure-Attack CounTermeasures*
FMEA	*Failure Mode and Effects Analysis*
FMVEA	*Failure Mode, Vulnerabilities and Effects Analysis*
FTA	*Fault Tree Analysis*
HARA	*Hazard Analysis and Risk Assessment*
HAZOP	*HAZard and OPerability*
HMI	*Human Machine Interface*
ICS	*Industrial Control System*
IEC	*International Electrotechnical Committee*
IIoT	*Industrial Internet of Things*

INERIS	*Institut National de l'Environnement industriel et des Risques*
ISO	*International Organisation for Standardisation*
IT	*Information Technology*
KB	*Knowledge Base*
NIST	*National Institute of Standards and Technology*
OT	*Operational Technology*
PHA	*Preliminary Hazard Analysis*
PLC	*Programmable Logic Controller*
SCADA	*Supervisory Control and Data Acquisition*
SECFT	*Security Enhanced Component Fault Tree*
SecL	*Security Level*
SGM	*Security Guide-word Method*
SIL	*Safety Integrity Level*
SL	*Security level*
SQL	*Structured Query Language*
STAMP	*System-Theoretic Accident Model and Processes*
STPA	*Systemic Theoretic Process Analysis*
STRIDE	*Spoofing, Tampering, Repudiation, Information Disclosure, Denial of service, and Elevation of Privilege*
TVRA	*Threat and Vulnerability Risk Assessment*
UCA	*Unsafe Control Action*
UML	*Unified Modeling Language*
VSM	*Viable System Model*

Introduction

Context and motivations

Critical industrial systems around the world, such as energy production, chemical production, and automotive manufacture, etc., are vulnerable to disastrous industrial accidents that have serious consequences on the environment and people. For a long time, the risks associated with these industrial sites have been monitored and managed in order to prevent the occurrence of the hazardous accidents and protect the installations, by applying the appropriate safety measures. For this reason, a large number of hazard study methodology have been developed over the years for industrial systems.

Until recently, industrial systems were based on mechanical and electrotechnical devices, closed systems, and human resources. With the development of the world in the industrial context, these systems have grown unable to keep up with and follow the innovation. Therefore, industrial systems around the world are increasingly integrated by automated systems and modern control systems with communicating and digital technologies: the use of connected objects, the technological convergence and the interconnexion between IT and OT, the connection of control systems to the internet, the remote access to control systems, and so on. This shift from analog towards digital equipment has simplified the industrial process and saved expenses for industrial operators. Despite the advantages of this digitization, it has challenges. The digitalization increases the degree of complexity and communication among systems, making the whole industrial infrastructure vulnerable to internal and external malicious accidents, and exposing them to new cybersecurity risks. In addition, various cybersecurity incidents affecting the industrial systems have been reported such as Stuxnet, NotPeya, Triton, and so on.

Therefore, two terms should be distinguished and treated differently in industrial systems: Safety and Cybersecurity. Safety is concerned with the hazardous and accidental risks, while cybersecurity is concerned with the

malicious risks caused by cybersecurity attacks. In the next section, the objective of our work related to safety and cybersecurity for industrial systems is explained.

Objectives

For long time, industries have concentrated on safety subjects without necessarily taking into consideration that a cyberattack might also compromise the safety system. Because of to the integration of automated and digital systems in industrial control systems, the cybersecurity has become a key issue for the critical industries that must be addressed. Thus, the industries should be more conscious, and raise awareness about the risks related to cybersecurity.

There is a strong interest in the development of risk analysis approaches combining safety and cybersecurity, particularly in the industrial process, which is a major potential hazard for local populations and the environment. There have been numerous risk analysis approaches proposed. The majority of them evaluate separately the risks related to safety and cybersecurity, despite their interdependencies and the common consequences between them. Since the relevance of merging safety and cybersecurity has grown, a transformation has been seen by proposing approaches that integrating them in risk assessment, to improve a complete risk analysis.

To address these issues, the objective of this thesis is to propose a new risk analysis approach that combines the safety and cybersecurity by providing a process by gathering and identifying the data needed for the analysis, as well as and a process for combining the two types of risks and presenting their potential relationships. These goals aid to provide a complete and exhaustive industrial safety and cybersecurity risk analysis approach.

Contributions

A study of twenty existing risk analysis approaches that integrate the safety and cybersecurity risks was conducted, and these approaches were classified using a comparative analysis. This study helps us in proposing a new risk analysis approach and identifying our contributions. In this thesis, we offer a new model-based risk analysis for process industry that considers both safety and cybersecurity. The normal procedure for safety and cybersecurity risk analysis is

to identify the attack scenarios that could result in the occurrence of physical undesirable events and integrate them with safety risks in the same analysis.

The proposed approach allows for the creation of a model that describes the industrial installation, which represents a valuable source of data for the rest of the approach. It aims to make the process of identifying the cyberattack scenarios easier by defining a guide to define simply the vulnerabilities that are an important source for the execution of a cyberattack, constructing new meta-models to define the generic cyberattacks scenarios, and developing an algorithm in order to generate these attacks scenarios automatically. In addition to these main contributions, the proposed approach is applied to a real case study.

Thesis outline

The first chapter discusses the various relationships between the terms of safety and cybersecurity, including their differences, similarities, and interdependencies. The structure of industrial control systems (the various levels and components) is then explained, along with the new cybersecurity challenges that these systems face: why the cybersecurity has become an important subject that should be considered in risk analysis in addition to the safety risks. Some cyberattacks incidents that have occurred around the world are illustrated to improve the inclusion of cybersecurity in the risk analysis process. Finally, we highlight the problem and objective of our work, which is the proposition of a new model-based risk analysis approach that combines safety and cybersecurity.

Chapter 2 presents the state-of-the-art overview of roughly twenty existing risk analysis approaches that have already been developed to integrate safety and cybersecurity risks. The process of each approach is depicted, and these approaches are classified into categories according to their integration and analysis processes. At the end, we finish by comparing and classifying the risk analysis approaches based on a set of criteria in order to determinate their benefits and limits.

Chapter 3 addresses the contribution and the different steps of the proposed risk analysis approach: the different steps to collect the data needed to perform the analysis process, as well as the steps to generate the cyberattacks that should be integrated with safety risks in the same analysis. These steps are modeled in UML, and an algorithm is developed to generate automatically the attack

scenarios using some of the collected data. At the end, the steps in this chapter are discussed.

Chapter 4 presents the remaining steps of the proposed approach: Combining the cyberattacks with the safety risks in the same graph (cyber Bow-Tie), evaluating the cybersecurity and safety events separately, and then evaluating the likelihood of the combined risk scenario and how to treat them by proposing safety and cybersecurity measures. At the end, the steps in this chapter are discussed.

Chapter 5 demonstrates the steps of the proposed approach using a case study of a polymerization system from INERIS, that runs a chemical reaction and can have serious consequences in case of a cyberattack or a hazardous situation. The different functions and components of this case study are described first. The approach is then applied step by step, with the results being listed and discussed. The end of this thesis shows a global conclusion and some perspectives for future work research.

Chapter 1: Safety and cybersecurity in industrial systems

The chapter presents, in the first section, the two terms of safety and cybersecurity and the corresponding terminologies in risk analysis, as well as similarities, differences, interdependencies between each one. The second section covers the various levels of an ICS process as well as the issues and challenges of cybersecurity on industrial systems. The third section describes some critical cyberattacks that have happened on different industrial systems worldwide. Finally, the problematic and the objective of our work are concluded with a conclusion.

1.1. Introduction

Safety and cybersecurity in industrial systems are two different terms and they are related to different types of risks. As such, they differ in terms of risk analysis, but they also have similarities and different types of interdependencies between them. In this chapter, Section 1.2 clarifies the definitions of safety and cybersecurity, how they relate, and the differences between them in risk analysis.

Until the 2010's industrial systems were based on electro-mechanical devices, closed automation systems to assist operators (Industry 3.0), and human resources, they took into consideration only safety issues when analyzing risk. In the past years, the industries increasingly integrate digital and communication technologies into their automated control systems such as internet connections and the remote access to the control systems [1]. The digitization of these industries makes them more vulnerable to attacks, which can adversely affect their safety. Cybersecurity has become a critical issue in ICS and must be considered as part of risk assessment. In this chapter, Section 1.3 illustrates the structure and levels of an industrial system, together with the new issues and challenges of cybersecurity besides the safety issues related to ICS. Section 1.4 provides some examples of some happening attacks that have had negative impacts on industrial installations and the environment. Following these cybersecurity issues, Section 1.5 describes the problem and the objective of our work. Finally, Section 1.6 draws some conclusions and summarizes this chapter.

1.2. Safety and Cybersecurity

The purpose of this section is to explain the relationship between safety and cybersecurity in the risk analysis process, as well as the definitions of both terms. Section 1.2.1 explains the terminologies of safety and cybersecurity. Section 1.2.2 illustrates the differences between safety and cybersecurity. Section 1.2.3 shows the similarities and the different types of interdependencies between safety and cybersecurity.

1.2.1. Terminologies of safety and cybersecurity in risk analysis

There are different definitions of safety and cybersecurity terms around the world in different contexts and technical communities [2] [3]. For example, electrical engineers understand safety and cybersecurity differently than those in

the nuclear community. In the following, we will define exactly what safety and cybersecurity mean in our thesis to clarify its objective and scope.

Both safety and cybersecurity address risk, the two terms can be the source of risk to industrial systems, and each term has its definition in risk analysis. In general, the source of risk on an industrial system can be accidental or deliberate. The operators of classified industrial facilities according to the French code of environment, such as the chemical industry, for example, must analyze and control the major and potential risks that their facilities may pose to people and the environment. The causes of these risks are random and accidental, and these risks are identified by the risks related to safety in our thesis work. The safety risk analysis should improve the operational safety (in French "Sûreté de Fonctionnement") and the functional safety of an industrial system. There are some standards, such as IEC 61508, IEC 61511, that can be applied to improve the industrial safety and the reliability of the industrial system.

The deliberate threats can be internal or external and caused by attacks that can be done physically or by cyber means. Protecting against malicious and deliberate acts that could have critical consequences for the industrial facility or its environment, is security. Security events may have an impact on safety. For the malicious actions on computer systems, the terms "cybersecurity" and "cyberattack" are used in this thesis. To analyze the cybersecurity risks for industrial systems and to improve the industrial security, the standard IEC 62443 can be applied.

Until the 2010's, the cybersecurity for these industries was absent because their control systems were considered as isolated and protected from the outside world. Therefore, the industrial safety, including the operational and operational safety, corresponds to analyze the safety risks only. During years, the cybersecurity in industrial control systems have been appeared and their risks can affect the industrial safety with the safety risks. Figure 1.1 depicts the interactions between the safety and cybersecurity. Therefore, it is essential to understand the similarities and the differences that unite and differentiate these two disciplines.

There is a high level of interest in developing risk analysis approaches to improve the industrial safety. For every source of risk, safety or cybersecurity, numerous risk analysis approaches are developed. Examples of safety risk analysis approaches are the following: FMEA [4], PHA [5], Bow-Tie [6], HAZOP [7]. The last three approaches are used particularly within the French regulatory

context. Examples of cybersecurity risk analysis approaches are the following: EBIOS RM [1], CORAS [8], Attack Tree [9]. In the next section, the differences between safety and cybersecurity in the context of risk analysis are discussed.

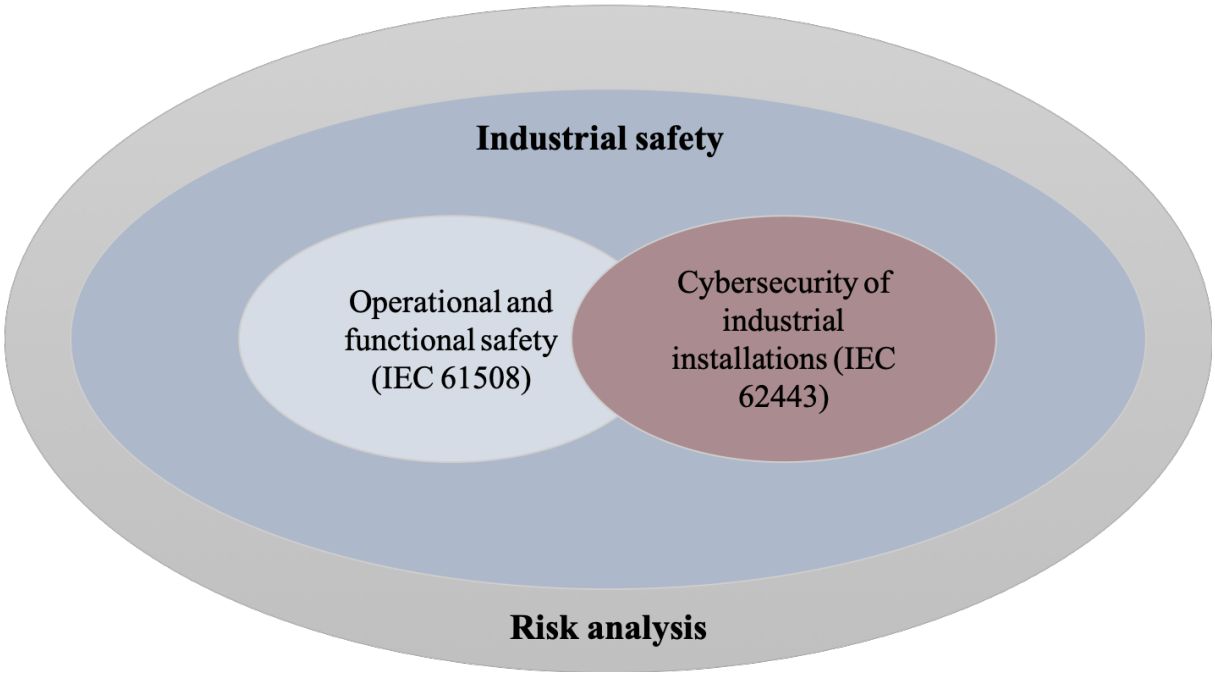

Figure 1.1 - The interactions between safety and cybersecurity

1.2.2. Differences between safety and cybersecurity

There are many differences between safety and cybersecurity in risk analysis: such as the source of risk for each term, the tools and standards and the way to assess them, the evaluation of the likelihood of occurrence of each type of risk. These differences are detailed as follows:

- Safety and cybersecurity are two different terms with common objectives, but there are often problems caused by the lack of common language and reference. Even when the same word is used by the two disciplines, it can be defined or interpreted differently, resulting in confusion. In this research, Safety and cybersecurity are defined separately with their different origins of risk. The safety discipline is associated with internal accidents caused by

a system failure or some combination of accidental conditions, external accidents, or any non-deliberate source of hazard that can harm the environment. While security discipline refers to cybersecurity and not to physical security. It is related to internal or external deliberate threats caused by malicious attacks which can be accomplished physically or by cyber means and can impact the assets of the system and its operation due to the vulnerabilities on the assets.

- In risk analysis, the risk assessment tools, standards, and the ways to assess the risks related to these two areas are different. Cybersecurity threats risk analysis differs from safety risk analysis. The sources of the cybersecurity threats are not well-known, it can exist an extremely range of attack scenarios with many different attacker behaviors and objectives and a rapid change to threats and vulnerabilities. While hazardous situations are more known and accessible, the scenarios that must be taken into consideration in risk analysis can be reduced to the critical ones only.

- The likelihood of a successful cyberattack is more dynamic than that considered in a usual safety analysis. For cybersecurity events, a sequence of events is required to successfully perform an attack with many factors such as the attacker profile, its skills, and motivation. Depending on these factors, the cybersecurity attributes are less predictable and it is difficult to assess and quantify the cybersecurity scenarios risks. While the evaluation of likelihoods of risks related to safety is more applicable quantitatively than for the cybersecurity risks. The data needed to quantify safety hazards are available and stable over time based on feedback from the analysts. Therefore, the use of likelihoods in the quantitative approach is widely adopted in the safety field. In the following section, the similarities and interdependencies between safety and cybersecurity are presented.

1.2.3. Similarities and interdependencies between safety and cybersecurity

Safety and cybersecurity have long been independently and separately reviewed despite their similarities. The system's assets can be impacted by either safety accidents or cybersecurity threats which can have the same nature of consequences, both safety and cybersecurity risks can have impacts on the system

itself and the environment. In addition, safety and cybersecurity risk analysis approaches have general steps in common (Standard ISO 31000): risk identification, risk evaluation, and risk treatment. However, with the increasing integration of new technologies in the context of the industrial control system, cybersecurity threats can affect the system's safety, and a pure safety risk analysis approach or a pure security risk analysis approach alone cannot mitigate the risks of the physical infrastructure of the system. Unfortunately, maintaining separate analyses for safety and cybersecurity can lead to redundant work and missed safety or security problems [10]. Therefore, safety and cybersecurity are complementary and must be assessed jointly as part of risk management and they should not be treated separately from each other throughout the system's lifecycle [11].

In addition to that safety and cybersecurity events can lead to the same undesirable event in risk assessment, they are interdependent and it is important that these interdependencies have to be considered during the risk assessment and the system's lifecycle. There are many types of interdependencies between safety and cybersecurity [12]: Conditional dependencies, cybersecurity is a condition for safety and vice versa; Mutual reinforcement where safety and cybersecurity measures can reinforce each other; Antagonism where safety and cybersecurity measures can weaken each other; Independence, safety, and cybersecurity do not have any interaction between them. The first three types of interdependency are presented with examples below.

- Conditional dependencies: This type of interdependence is defined in particular in the sense of cybersecurity conditional on safety. For example, a malicious attack to modify the configuration of a PLC can actually affect the system's safety and avoid protecting the industrial installation from accidents. It can exist on all types of automated industrial systems presenting critical safety risks. Otherwise, the safety conditional on cybersecurity is more rarely presented, but in some situations, safety can condition a level of cybersecurity. For example, catastrophic conditions associated with a safety incident can weaken the security level of a system and lead to malicious threats, in case if the safety incident is not properly managed.

- Mutual reinforcement: This type of interdependence allows safety and cybersecurity measures to be mutually reinforcing. An applicable

cybersecurity measure may improve the system safety and vice versa. This kind of interdependence can lead to value for money and avoid some redundant data and overlaps. For example, in the nuclear context, some arrangements for safety, such as the physical separations and physical diversification of particular operations, can also protect the physical system against sabotage. The use of identical treatment for safety and cybersecurity, in particular, can be modified for the tolerance of accidental faults but it does not prove an effective defense against an attacker who can exploit a vulnerability replicated to the same.

- Antagonism: Despite the fact that safety and cybersecurity measures are mutually reinforcing, they can undermine each other and it is possible to have conflicts between them. In some cases, a cybersecurity measure can decrease the system's safety and vice versa. For example, a door with limited access for a production process in an industrial installation [13]: for cybersecurity reasons, the door must be locked and accessible with keys and badges to prevent unauthorized access, while for safety reasons, the door must be always unlocked to respond in case of a fire resulting for a hazardous situation.

The differences and interdependencies between safety and cybersecurity given in this section, demonstrate the importance of combining safety and cybersecurity in the risk analysis process, by considering their interdependencies and conflicts. After presenting the cybersecurity problems on the industrial system in the following part, this combination will be more assured in risk analysis for ICS.

1.3. ICS process and cybersecurity challenges

This section gives an overview of the Industrial Control System, as well as the issues it faces in terms of safety and cybersecurity challenges. Section 1.3.1 depicts and specifies the ICS, including its architecture and the related connected levels. The cybersecurity challenges with industrial control systems are discussed in Section 1.3.2.

1.3.1. Overview of ICS: Definition and architecture

An Industrial control system ICS is one of the most widely used control systems in the planet. It is a combination of software and hardware, that act

together to achieve an industrial objective, by monitoring and controlling vital industrial infrastructure, industrial processes, machine physical operations, networking, and any other equipment in the industrial environment. The use of ICS in the industrial process aids productivity, quality, and flexibility in the manufacturing process [14].

ICS includes Supervisory Control Data Acquisition systems (SCADA), that are used to control scattered assets through centralized data acquisition and supervisory control. It also comprises small control system configurations such as Programmable Logic Controllers (PLC) that are commonly used to regulate the manufacturing process and physical components, often found in the industrial sectors and critical installations, such as sensors, valves, pumps, and other key installation.

Vital systems and services of modern society are controlled by ICS processes including, electric production and grids, power plants, water distribution and treatment, oil and natural gas refining, chemical processing and production, transportation domain, discrete manufacturing [15]. In addition, ICS can also control hospital systems and commonly utilized high-tech medical equipment.

The architecture and various levels of an ICS are depicted in the CIM pyramid, as shown in Figure 1.2. This pyramid represents the basic architecture and the hierarchy of an ICS, which is made up of five different levels presented as follows:

- Level 0 – Field level: The lowest level of an ICS which contains physical components like sensors, valves, pumps, actuators, and so on. These components are directly connected to the physical world of the industrial process which can contain reactors, pipes, mechanical equipment, or critical substances. They gather and generate data that will be utilized at higher levels to supervise and regulate the industrial process.

- Level 1 – Control level: This level uses the PLC components with automates, and it is linked to the field and supervision levels via a communication network in order to control the manufacturing process by receiving data from the other levels and sending control signals to the physical components. In addition, at this level, there are configuration and programming stations for PLCs.

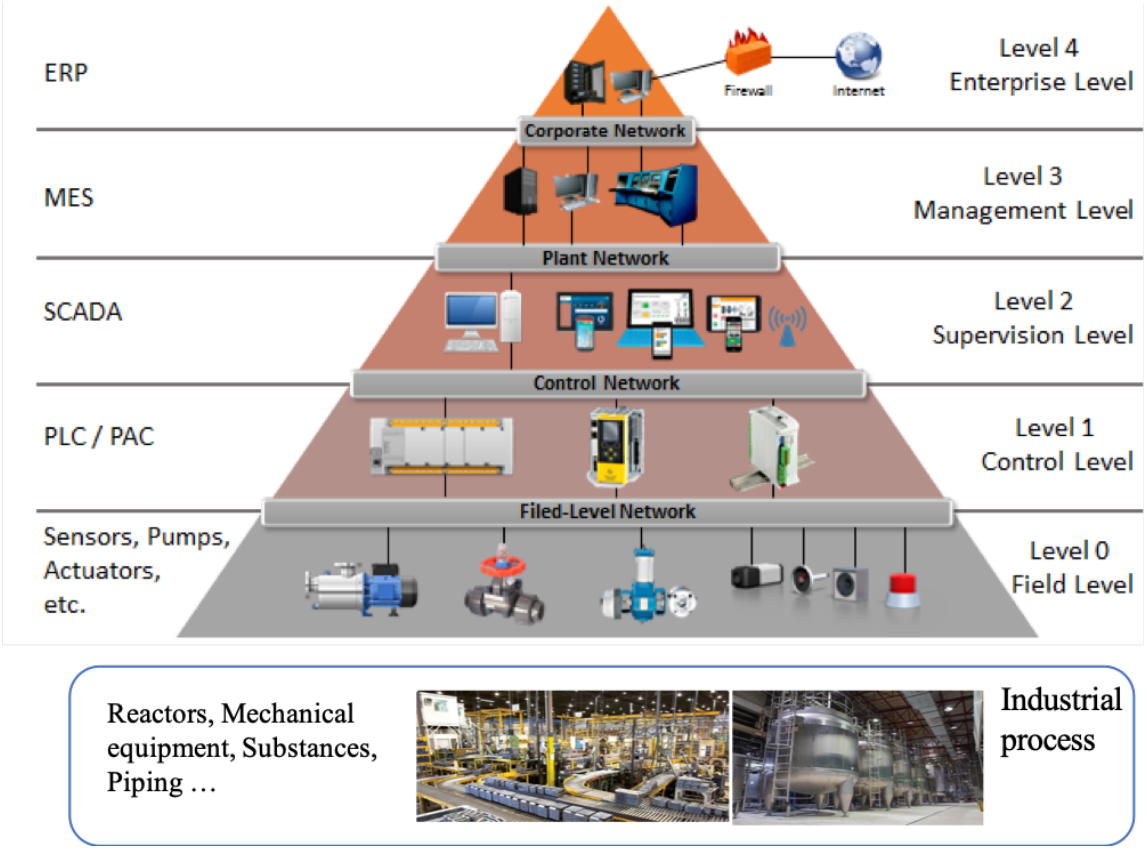

Figure 1.2 - The architecture and the hierarchy of an ICS

- Level 2 – Supervision level: This level contains SCADA systems with supervision stations such as HMIs, servers, computer stations, and databases in order to monitor and maintain industrial processes and physical components.

- Level 3 – Management level: This level is in charge for process scheduling, material handling, maintenance, inventory, etc.

- Level 4 – Enterprise level: The highest level of an ICS, which oversees the whole industrial control system and all levels. It has to do with commercial tasks like production planning, customer and market analysis, order and sales, and so on.

A typical ICS is made up of control loops of sensors, valves, pumps, and actuators that interact with the physical world, as well as HMI, remote diagnostics, and maintenance utilities. To accomplish a controlled process, each

control loop consists of hardware such as sensors, actuators, and controllers (PLC). The sensors on the field level detect changes or other quantities in the physical world, and thereby provide outputs in form of signals as a result. These outputs are then delivered as controlled variables from the control level to the PLC, which interprets them and generates corresponding manipulated variables based on the functionality of the automate implemented on the PLC. These generated variables are then transmitted as command inputs to the actuators, pumps, or valves, causing them to act and manipulate the regulated process (close the valve, stop the process of the actuator, etc.). At the control level, the configuration and programming stations are used to monitor, configure, and operate the PLCs' algorithm, as well as alter the parameters in the controllers.

At the supervision level, the operators and engineers employ HMI (supervision stations), which is a graphical user interface that allows the interaction between people and the controlled process hardware. It can also be used to show information and historical data acquired by devices in an ICS environment in real-time, in the form of graphs, diagrams, and the representative schema. Remote diagnostics and maintenance utilities are used to avoid, recover from and prevent abnormal activities or failures. Furthermore, there is a SCADA system at this level, which consists of servers with databases and historical databases. These databases are centralized databases for logging all process information inside an ICS environment. The data collected is then used for process analysis, statistical process control, and enterprise-level planning. In the following section, the revolution of industrial systems during the years as well as new cybersecurity challenges are discussed.

1.3.2. Cybersecurity issues on industrial control systems

The first industrial systems were built on electro-mechanical devices and closed systems, with human resources and equipment performing the production process and fabrication operations, as shown in Figure 1.3 for the first and second industrial revolutions. During the years, due to the development of digital technology related to instrumentation and industrial automation, computers and automation processes have increasingly penetrated industrial systems which become more and more automated (the third resolution in Figure 1.3).

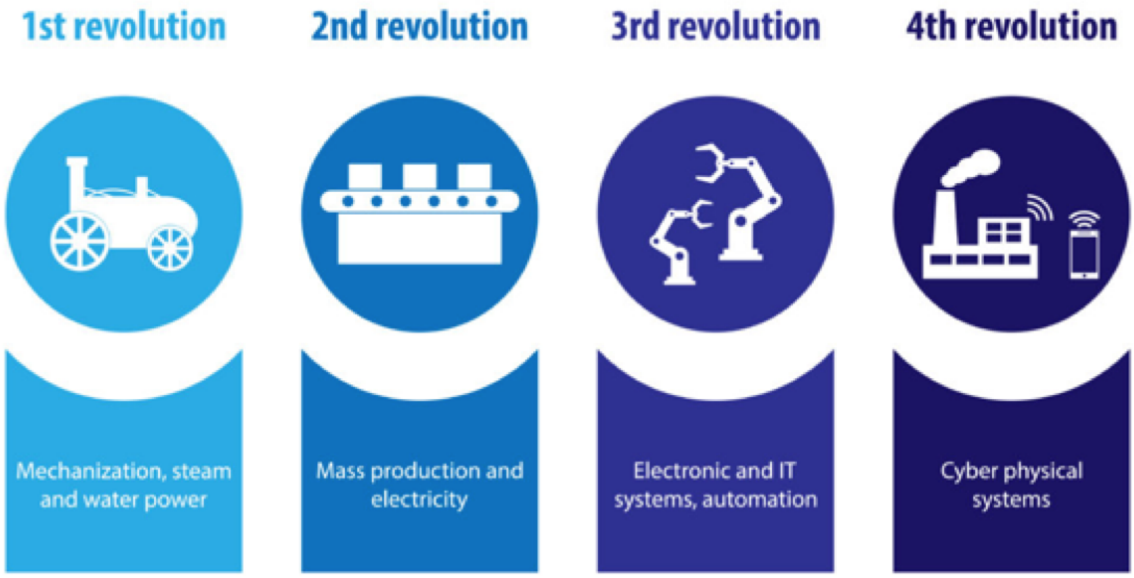

Figure 1.3 - The revolution of industrial systems

Nowadays, most industries around the world have advanced and automated control systems, and they are increasingly integrating digital and communicating technologies into their automated control systems such as the use of a large number of connected objects in the industrial process (IIoT), the technological convergence between the IT and the OT refers respectively to anything related to computer technology (software and material), and to the material and software used to monitor and control industrial processes. Other technologies integrated into the industrial control system include internet connectivity from the industrial system's equipment, remote access to control and manage systems [1], and digitization initiatives in the industrial process. Furthermore, cyber-physical systems are rapidly being developed and applied in industrial systems. The majority of industries are now automated and digitized, and they are classified as "Industry 4.0.". Despite the benefits of this digitization in industrial control systems, such as the increased production speed and the high quality and repeatability, this shift increases the industrial infrastructure's attack surface and makes it more vulnerable to cyberattacks, which can affect the safety of an industrial system as well as the hazardous situations. Furthermore, the complexity and heterogeneity of CPS used in industrial systems introduce difficulties to their security and privacy system. Therefore, the industrial system safety is no longer limited to problems linked to failure or human errors, or environmental disastrous but also is linked to the occurrence of cyberattacks related to cybersecurity risks.

A new version of the pyramid CIM, displayed in Figure 1.2, is depicted in Figure 1.3 as a result of the digitization of industrial control systems. It represents the different levels of an ICS, along with the relevant components and the integrated technologies: remote access to stations, wireless sensor connections, and internet connectivity. As previously indicated, all levels of an ICS process are linked and send data back and forth. As a result, a cyberattack on any level of the ICS might have a significant impact on the whole system. For example, an insider attacker can get illegal physical access to the PLC and disconnects it from the physical process. This PLC controls the functionality of a valve from the field level that is responsible for the introduction of a critical product, and due to this attack, the functionality of this valve changes and can lead to high consequences on the industrial system. The cybersecurity risks in the schema of Figure 1.4 can be encountered on the all ICS levels and can lead to dangerous phenomena. Therefore, cybersecurity has become a crucial and important issue in industrial control systems [16], such as those in the power generation and distribution industries or the chemical industries [17], and their risks should be integrated in the safety risk analysis which exist on the physical process with the field and control levels.

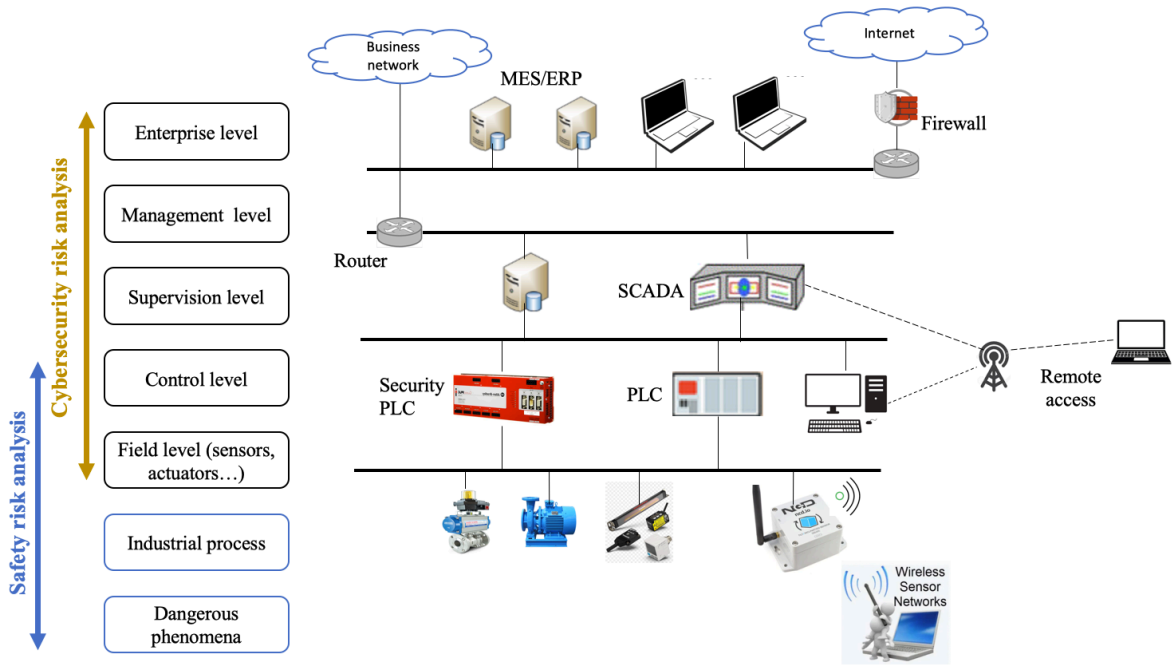

Figure 1.4 - The new version of the pyramid CIM

Critical automated industrial systems must consider cybersecurity, and they should raise awareness about the risks related to cybersecurity in risk analysis, in order to meet the following security criteria [18] [19]:

- Availability: The industrial control system and process data must be available at all times, in order to guarantee the good execution of the industrial process.

- Integrity: For a better execution of the industrial process, the data of the control and process system should be authentic and unchangeable.

- Confidentiality: Unlike the challenges of integrity and availability, data confidentiality is not as crucial for the execution of the industrial process. In some situation, an attack on this security need can harm the image of the industrial site.

- Fault-tolerance: During the presence of defects or component failures, the industrial process must continue.

- Time-criticality: The data acquired throughout the industrial process, as well as the controls are in real-time. This security need is only relevant in the case of an industrial system that requires frequent data updates.

These security requirements are met when cybersecurity risks are correctly examined as part of the risk analysis process, this cybersecurity risk analysis will be factored into the objective of our work. Before we get into our work objective and problematic, let us take a look in the following section at some of the most significant cyberattacks that have occurred in recent years around the world.

1.4. History of happening cyberattacks

The attacks performed on ICS, like other types of cyber threats, have grown in scope and sophistication in recent years. This increase is due to the increasing connectivity of industrial systems and their digitization. In this section, we will go over a list of the most well-known cyberattacks on ICS that have occurred around the world, with varying degrees of severity [20] [1]. The history of these cyberattacks, as well as their consequences, are presented in Table 1.1.

Year of occurrence	Cyberattack	Description	Consequences
2021	Colonial pipeline [21]	A hacker gang perform ransomware (Annex B) attack on the firm billing system and the internal business network in USA.	Financial losses, Stop of the gasoline supplies
2020	Water supply [22]	Attack on a PLC in the process of water supply, changing the command sent to a pump, exploiting the vulnerability that the PLC configuration station is accessible without authentication data.	Stop of water supplies
2017	Triton [23]	Attack on a security PLC (Triconex) by exploited the vulnerability in computers running the Microsoft Windows as operating system.	Stop of the industrial process, Potential industrial disaster
2017	Wannacry [24]	Attack on computers used in the industrial process implemented by Microsoft Windows (vulnerability) to	Financial losses (ransom), Stop of industrial process

		encrypt data and request ransom.	
2017	NotPetya [25]	Attack targeted an accounting software in Ukraine to encrypt data and request ransom.	Financial losses
2015 - 2016	BlackEnergy [26]	Two attacks on a power grid in Ukraine by executing a Trojan (Annex B) through phishing email on the computer used in the industrial process.	Electrical power cut
2016	Kemuri water company [20]	Attack on PLCs to manipulate the control applications in this industrial process, by gaining unauthorized access to these PLCs.	Alteration of water treatment chemicals
2014	DragonFly [27]	Attack on an energy industrial sector to compromise the ICS equipment through remote access trojan to component or through phishing emails.	Sabotage

2010	Stuxnet [28]	Attack on Siemens PLC used in the industrial process of the nuclear program in Iran, by exploiting the use of Microsoft windows	Degradation of a huge number of centrifuges

Table 1.1 - Cyberattacks incidents on industrial systems

In conclusion, because of the interdependencies and the similarities between safety and cybersecurity in risk analysis, as well as the digitization of industrial systems and the rise in cyberattacks on industrial systems, all these reasons make cybersecurity an important subject that should be addressed during the risk analysis process. In the next section, the challenge and the objective of our work, as well as the necessity of analyzing the risks related to cybersecurity on ICS, and merging them with the safety risks, are discussed.

1.5. Problematic and objective

As shown in the sections above, industrial systems are becoming more automated and digitized. This move increases the industrial infrastructure's attack surface, making it more vulnerable to cyberattacks, which might compromise the system safety. In section 1.4, the security incidents that occurred over the years are outlined. Therefore, cybersecurity has become a major concern for vital industries and their risk analysis. Most industries place a premium on safety subjects without necessarily taking into consideration that a cyberattack may compromise the safety of a system. Thus, critical automated industries should improve knowledge about the risks and dangers related to cybersecurity. Because each type of risk has its own analysis approach as shown above, other industries manage the safety and cybersecurity risks separately, despite their interdependencies and shared implications on an industrial system.

For all these reasons, the combination of safety and cybersecurity in risk analysis must be viewed as important, and they must be considered in the same analysis approach (Figure 1.5). The main objective and problem of our work are to develop a combined safety and cybersecurity risk analysis approach, that

provides a comprehensive and holistic analysis without redundant and duplicated work [10], and that can be applicable to industrial control systems, particularly in the process industry (ICS process).

Recently, there has been a lot of interest and focus on developing approaches that combine safety with cybersecurity to address the problem of cybersecurity risks. A significant number of risk analysis approaches for safety and cybersecurity have been proposed. Each approach has distinct characteristics in terms of how it depicts the interdependencies between safety and cybersecurity, as well as the mechanisms for analyzing and evaluating the two categories of risks. Chapter 2 compares and categorizes roughly twenty existing risk analysis approaches that integrate safety and cybersecurity. The discussion of the results of this review aids us in defining the limits of the existing approaches and proposing our new model-based risk analysis approach based on the best characteristics in Chapter 2. The limits that will be defined from the existing risk analysis approaches will be at the levels of detail of the analysis process, the modeling of the system architecture, the definition of vulnerabilities and attack scenarios leading to undesirable events, the way to evaluate the likelihood of occurrence of combined risks. In our proposed risk analysis approach, we will model the system architecture in order to conduct a comprehensive risk analysis, we will attempt to simplify the methods for defining vulnerabilities and attack scenarios, and we will make the process easy to apply for users. In addition, we will assess the likelihood of occurrence of combined risks in such a way that the disparities between the likelihoods of each type of risk can be seen.

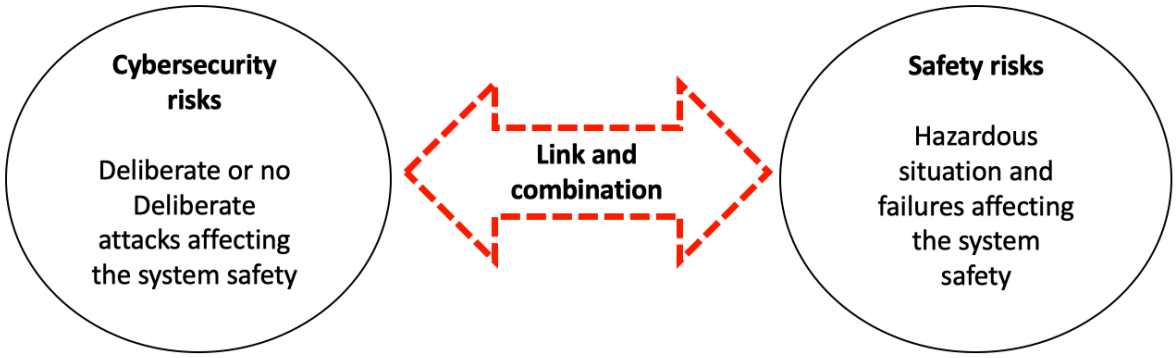

Figure 1.5 - The combination between safety and cybersecurity risks

1.6. Conclusion

The definitions of the two terms safety and cybersecurity, as well as their similarities, differences, and interdependencies, are presented in this chapter. We also go through the traditional risk analysis approaches and requirements for safety and cybersecurity. The second half of this chapter illustrates the connections between these two concepts within the Industrial Control System (ICS), including its architecture and various industrial levels in the CIM pyramid, as well as the new problems and cybersecurity issues that these systems face. The third section discusses several high-impact cybersecurity incidents that occurred around the world. Finally, we discuss the problem and objective of our research, which is to propose a risk analysis approach that incorporates both safety and cybersecurity into the same analysis process. The existing risk analysis approaches that integrate safety and cybersecurity are listed and presented in the next chapter, with a classification and a comparison between them in order to determine their benefits and limitations.

Chapter 2: Literature review of existing risk analysis approaches combining safety and cybersecurity

In the first section of this chapter, the state-of-the-art of the many existing risk analysis approaches is presented which propose processes considering that safety and cybersecurity must be tackled together. The offered risk analysis approaches are classified in the second section based on a set of criteria, followed by a comparison and discussion of the benefits and limitations of safety and cybersecurity risk analysis approaches. We conclude with a conclusion and an open view on our proposed risk analysis approach in the last section.

2.1. State of the art of risk analysis approaches combining safety and cybersecurity

Since the relevance of merging safety and cybersecurity in risk analysis in critical industrial systems has grown, a shift has occurred by proposing risk analysis approaches that include processes that address both safety and cybersecurity concerns. Many scholars worked on reviewing risk analysis approaches that combine safety and cybersecurity ([29], [30], [31], [32], [33], [11]). All these publications present several risk analysis approaches, their analysis processes, as well as a classification based on a set of criteria and a summary of the results. In this section, we will provide a border panorama of various mixed safety and cybersecurity risk analysis approaches, as well as the steps involved in defining and analyzing safety and cybersecurity risks and combining these two disciplines. Then, using some criteria from previous evaluations, we will classify them in order to determine the benefits and limits of the existing approaches.

In all of the existing approaches, the combination of safety and cybersecurity can take two forms: Sequential approaches in which the cybersecurity and safety risks analysis are performed in a specific order, a safety risk analysis is conducted first then the cybersecurity risk analysis, and the two analyses will be combined; Non-sequential approaches in which the safety and cybersecurity risks analysis are performed in a parallel way, the two types of risk are analyzed jointly. Based on the various ways and forms to integrate and combine safety and cybersecurity in risk analysis, we split and classify the risk analysis approaches into five categories, and each category will be described below with the approaches that correspond to it:

- Extension of classical safety risk analysis or cybersecurity risk analysis;
- Combination of existing safety and cybersecurity risk analysis approaches;
- Integrated approaches built from scratch to combine safety and cybersecurity;
- Extension of STPA approach, which is discussed in a separate section due to the nature of the STPA approach;

- Approaches based on or proposed from the existing safety or cybersecurity standards.

2.1.1. Extension of classical safety risk analysis or cybersecurity

This category of approaches aims to extend the existing classical safety risk analysis or the cybersecurity risk analysis to combine these two disciplines. There are two sub-categories in this category: Extension of classical safety risk analysis approaches towards cybersecurity; Evolution of cybersecurity risk analysis approaches. In these subcategories, the risk scenarios might be presented in a no-graphical forms (tables or texts) or in a graphical form (event graphs).

2.1.1.1. Extension of classical safety risk analysis approaches

This sub-category of approaches builds on traditional safety risk analysis approaches by including the cybersecurity aspect as a cause leading to dangerous situations. The most common approaches used are HAZOP [7], FMEA [4], FTA [34], and Bow-Tie [6]. Table 2.1 shows the risk analysis approaches that combine safety and cybersecurity belonging to this sub-category, organized by the way of presenting the risk scenarios.

No-graphical representation	Graphical representation
SGM (Adaptation HAZOP) Cyber HAZOP FMVEA (Adaptation FMEA)	SECFT (Adaptation CFT) Extended CFT (Component Fault Tree) Extension of FTA with security

Table 2.1 - Extended safety risk analysis approaches

- SGM

The SGM approach [35] is a HAZOP extension that incorporates the cybersecurity threats for each fault-type guideword in the HAZOP approach. The following steps involved in SGM:

1. Define the entities, as well as the data flow between them and the safety requirements;

2. Using the HAZOP approach, define a set of fault-type guidewords;

3. Based on a historical analysis, establish a list of the operational situations;

4. Identify the hazardous situations for each fault and function combination;

5. Instantiate the cybersecurity guidewords (Triggering, modification...) and identify the protection goals, by describing the cybersecurity threats for each identified fault in step 2. In this step, cybersecurity and safety are merged;

6. Determine the severity, the exposure, and the controllability of each identified hazard in accordance with ISO 26262;

7. Classify the cybersecurity threats using the severity value of related hazards based on the selected fault;

8. Define the safety and cybersecurity requirements based on the protection goals.

SGM enables a structural identification of the goal protection, which can be used in cybersecurity analysis.

- Cyber HAZOP

Cyber-HAZOP [7] is a HAZOP extension that analyzes the impacts of control system deviations on the system evolution. To add the cybersecurity aspect, the guidewords have been changed to include cybersecurity guidewords such as cyberattacks, faulty programming software, and so on. The system study is defined first, followed by a list of deviations, including the fault and the cybersecurity guidewords. The causes of each deviation, such as cybersecurity threats or dangerous situations, are outlined, along with their consequences, and the safety and cybersecurity prevention tools are identified and enumerated. If a preventive tool is vulnerable to attack, the cybersecurity risks will be assessed and a cybersecurity level or physical barrier will be proposed.

The difference between Cyber HAZOP and SGM is that the list of guidewords instantiated in Cyber HAZOP includes both fault and cybersecurity guidewords, and for each guideword, the hazardous situations and threats are identified. While in the SGM, for each fault guideword instantiated, the cybersecurity guidewords are instantiated.

- FMVEA

The FMVEA [36] approach is an extension of FMEA (AMDEC in French) that includes the cybersecurity concerns by integrating the vulnerabilities (V) as sources of causes of cyberattack scenarios that lead to dangerous situations. The following are the steps involved in FMVEA:

1. Identify the system's functionalities, as well as the components that must to be analyzed and protected;

2. Determine the failure modes and the threats (using the STRIDE threat model [37]) on the selected components;

3. Determine the direct effects of the threats and the failures on the components and the system;

4. Identify the causes and the attack scenarios that exploit vulnerabilities resulting in failure modes and the threats. The vulnerabilities are discovered using the Microsoft Security Development Lifecycle [38] and the CWE (Common Weakness Enumeration) [39] which is a detailed and community developed list of common software weaknesses;

5. Determine the severity of the final impacts, with the help of experts and particular scales;

6. Evaluate the likelihoods of the safety and cybersecurity events based on a list of cybersecurity criteria. The system accessibility and connection, the motivation and capacity of the attacker, and the resources required to exploit a vulnerability are all elements to consider;

7. Estimate a level for each risk scenario by multiplying the gravity and the likelihood.

- Extended CFT

CFT [40] is a safety risk analysis approach that models the failure modes on system components with the goal of identifying the safety basic events of accidental situations that occur on the important components based on the FTA, which depicts the sequence of events in a graphical form. A CFT extension [41] was proposed to add and incorporate the cybersecurity aspects to this approach and model the cyberattacks that could compromise the system safety. The first step aims to prepare and construct the CFT with the accidental situations and the undesirable events. Then, to add the cybersecurity aspect, the attack scenarios that can occur on the components are find defined using the STRIDE model [37], and those that can lead to the same undesirable events are attached to the CFT. The likelihood of occurrence of the undesirable event, the highest event level, is evaluated using a double scoring (P, R) which represents respectively the likelihood of safety and cybersecurity events.

- SECFT

SECFT [40] is an extension of CFT that includes cybersecurity problems as a basic cause. The steps for achieving this approach are the same as for the Extended CFT, but the way for evaluating the likelihood of the tree's top event is different. The top event can be limited to cybersecurity events only, or safety events only, or a combination of the two. To evaluate its likelihood of occurrence, the events are grouped into Minimal Cut Sets MCs, which represent the smallest combination of events leading to the occurrence of the top event. There are three different types of MCs: Safety MCs contain only safety events, Cybersecurity MCs contain only cybersecurity events, mixed MCs contain both safety and cybersecurity events that can be connected by the gates OR/AND. The likelihood of each set is evaluated based on some defined equations and scales from ICE 61025.

- Extension of FTA with security module

An extension of Fault Tree Analysis [42] was proposed to model risks introduced by the insertion of a cybersecurity module in the system analyzed. The safety hazards of the cybersecurity module are linked to accidental situations to this module, and the cybersecurity hazards of the cybersecurity module are linked to the attacks initiated on this module. Both safety and cybersecurity events are

modeled in the same tree. The safety events are presented in the FTA, and the malicious attacks leading to the same undesirable events as the safety events are attached to FTA. This approach increases the safety level of the system analyzed.

2.1.1.2. Extension of cybersecurity risk analysis approaches

This sub-category of approaches tries to improve existing cybersecurity risk analysis approaches by including safety considerations. There are not many approaches in this sub-category, since cybersecurity and the analysis of risks related to cybersecurity has lately been a hot topic. The extension of TVRA [43] exists here, and the risk scenarios are shown in tables.

The TVRA approach tries to identify the cybersecurity threats and to evaluate their likelihood of occurrence and their impacts based on a list of characteristics that affect the risks posed by these threats. An extension of TVRA was proposing to include the Safety Integrity level SIL as one of the criteria impacting the risks. The criteria that affect the risks are time, expertise, knowledge, opportunity, equipment, asset impact, and intensity. The likelihood of attacks is calculated based on the attack potential value, which is calculated using these criteria: time, competence, knowledge, opportunity, and equipment. The security threat impact is calculated using the asset impact value and the attack intensity. The impact calculation is extended by adding the SIL along with asset impact and the attack intensity. The values of SIL are defined in [43]. This extension does not take into consideration the failure modes, it aims to present the impacts of cybersecurity threats on system safety. An example representing the process of this approach is presented in Figure 2.1.

2.1.1. Combination of existing approaches

This category of approaches aims to combine a conventional safety risk analysis approach with an existing cybersecurity risk analysis approach. This integration aims to represent the connections between risks related to safety and cybersecurity. In this category, the risks scenarios might be presented in a no-graphical forms (tables or texts) or in a graphical form (event graphs). Table 2.2 shows the risk analysis approaches that combine safety and cybersecurity belonging to this category, organized by the way of presenting the risk scenarios.

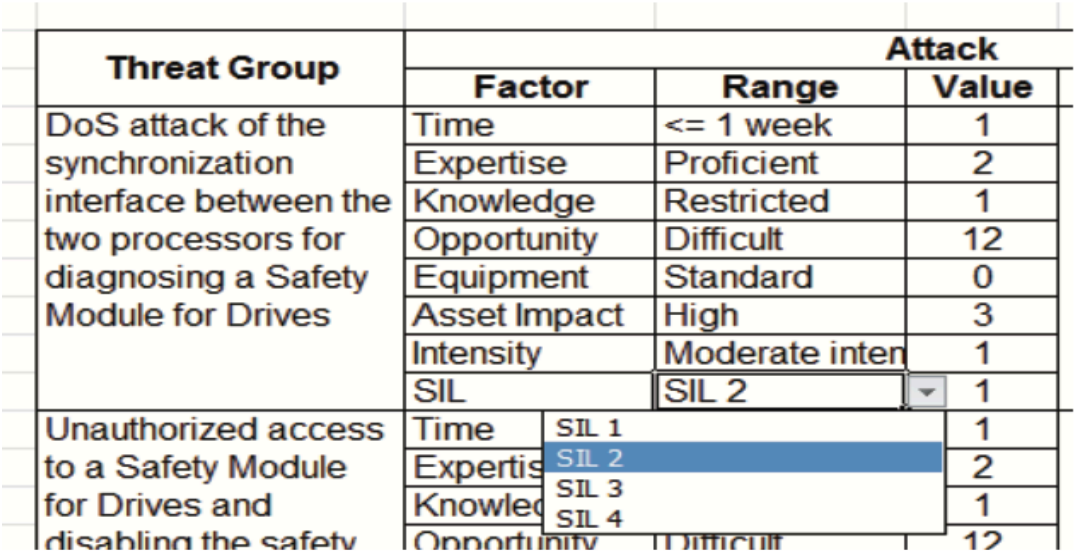

Figure 2.1 - An example of the extension of TVRA

No-graphical representation	Graphical representation
Combined STRIDE and FMEA SAHARA (HARA and STRIDE)	ATBT (AT and Bow-Tie) FACT Graph model (FT and AT) EFT (FT and AT)

Table 2.2 - Combined risk analysis approaches

- Combined STRIDE and FMEA

The proposed approach [44] is a combination of the existing approaches FMEA and STRIDE [37]. STRIDE is a threat modelling approach, it is an acronym for six cybersecurity threat categories: Spoofing, Tampering, Repudiation, Information Disclosure, Denial of service, Elevation of privilege. Figure 2.2 shows the steps required in this approach. The first step of this combination is to develop a system model, which is done by using a Data Flow Diagram to depict the components of the system and the interactions between them. The STRIDE approach is then used to build a cybersecurity threat catalogue containing the attack scenarios that impact the security objectives, while the FMEA is used to create a safety accident catalogue containing the failure accidents. The threat and failure catalogues are built and defined for each system's

elements and interactions. After combining these two catalogues, a risk evaluation is generated, which is based on the impact assessment on the cybersecurity side that can affect safety as well as the likelihood assessment on the safe side.

- SAHARA

The SAHARA approach [45] is a combination of HARA (based on ISO 26262) and STRIDE, initially developed in the automotive sector. By combining the security threats factors in a more systematic manner, the addition of the cybersecurity analysis using STRIDE improves the completeness of HARA. The steps of SAHARA are the following:

1. Identify the potentially dangerous events using HARA, classify them according to the Automotive Safety Integrity Levels ASIL, and estimate their gravity, likelihood, and controllability, as well as the proposition of some safety requirements;

2. Identify the cybersecurity threats using STRIDE and quantify them based on the required resources, expertise, and the criticality of the threat, in order to achieve a cybersecurity level SecL;

3. Considered the cybersecurity threats with a criticality of greater than two (>2) as events related to safety and add them to safety risk analysis.

- ATBT

The ATBT approach [46] enables the representation in the events related to the failures and the attacks in the same graphical model and propose a double scoring for the evaluation of likelihoods of the classes of events. The goal of ATBT is to get a broad picture of a variety of scenarios and to assess a safety level regardless of the cybersecurity level. The ATBT approach combines the Bow Tie (BT) [6] and the Attack Trees (AT) [9] to identify the causes related to the cybersecurity of the described scenarios in safety risk analysis. The steps of realization are the following:

1. Construct a BT, related to safety risk analysis, for the physical undesirable events, identified by PHA [5], the BT represents the causes and consequences of the analyzed undesirable events;

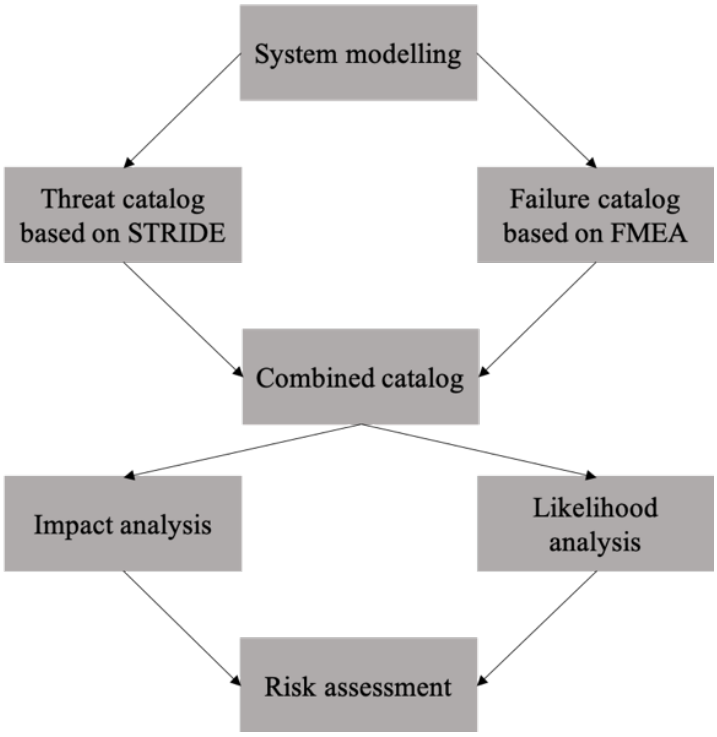

Figure 2.2 - The process of the combination of FMEA and STRIDE

2. Construct the AT, related to cybersecurity risk analysis: for each basic event of BT – such as a a failure of a component in an ICS (sensor drift, valve closure…) – identify if there are any cybersecurity incidents that can cause the same event and describe the steps and the vulnerabilities exploited by the attacker. The events are connected using the logical gates OR/AND;

3. Evaluate the various scenarios using a two-dimensional vector (L_s , L_f), that reflect representing respectively the likelihoods of cybersecurity and safety events, this step is completed with three steps:
   3.1. Determine the minimal cut sets (MCs) of the ATBT model: these are the smallest combination of safety and cybersecurity events (scenarios) leading to the occurrence of the undesirable event. The MCs can be made up entirely of safety events, entirely of cybersecurity events, or a mix of both;
   3.2. For each MC, characterize the likelihood of each elementary event, using specified scales to evaluate the likelihood;
   3.3. Determine the likelihood of the vector couples for each MC by

resolving just the events linked by the AND gate, by taking the minimum value of likelihood of the events that make up the couple, and classify the couple's based on a given scale.

- FACT Graph

The FACT approach [47] is based on the Fault Tree and the Attack Tree, it aims to merge the safety and cybersecurity lifecycles and their risks into a unified model, and to present the safety and cybersecurity artifacts and their relationships. The construction of FACT graph is involved by the following steps:

1. The safety failures and hazards are identified and presented in the FT, it is possible to have several interconnected FTs connected using AND/OR gates providing a complete view of the system failures;

2. Attach the safety countermeasures identified to the failures that they are intended to prevent on the FACT graph;

3. The attack trees depicting the attack scenarios are linked to the associated safety failures on the FACT graph, indicating that a failure could be caused by either accidental failures or cyberattacks;

4. The cybersecurity countermeasures are attached to any node of the attack tree on the FACT Tree.

The relations between safety and cybersecurity demonstrate how critical it is for safety and cybersecurity analysts to collaborate in order to detect all the system malfunctions.

Another approach, the EFT [48], was devised, which combines the FT with the AT, using the same procedures as the FACT graph. The safety failures are constructed with the FT, and the attack trees leading to the safety failure are attached to the FT. In addition to the FACT graph, the likelihood of occurrence of safety failures is evaluated based on a defined formula.

2.1.2. Integrated approaches

This category contains the risk analysis approaches that have been proposed from scratch to incorporate the risks related to safety and cybersecurity. This category includes the following subcategories: Model-based approaches, generic approaches, approaches favoring the quantitative aspect. During our review, each sub-category is outlined below, along with the existing approaches.

2.1.3.1. Model-based approaches

This type of approach consists to model the system architecture to be analyzed, by representing the functional and no functional aspects, as well as the components and their connections, and adding and exploiting different information in the risk analysis process. The goal of this criteria is to gain a thorough understanding of the system's functionality and to discover critical data required to generate the risks (vulnerabilities, cyberattacks, accidental situations). In large industrial systems with a large number of components and connections, it becomes difficult to model these systems. The approaches that exist in this sub-category are S-cube, Model-based safety and security assessment approach, CHASSIS, V-shaped model, SysML-Sec.

- S-cube

The S-cube [49] approach enables for a detailed modeling of the control-command system as well as the automatic generation of failure and attack scenarios. S-cube allows for the modeling of the system architecture, associated the safety and cybersecurity aspects, and automatically generates the possible risk scenarios that lead to physical undesirable events, which were discovered before using HAZOP. The phases of the S-cube approach are presented in Figure 2.3 and are the following:

1. Model and describe the system, the input data, such as the logical and functional architecture, the different zones, the connected machines, the software, and the data flow, based on a knowledge base S-cube KB as a Domain Specific Language, which enables to describe the components of industrial architectures, their associated attributes and the attacks and failures likely to happen on each component. The S-cube KB adopts the Figaro modeling [50], which is object-oriented and enables the inheritance mechanism to easily structure the knowledge and avoid redundancy. Then,

the experts define the security and safety aspects, and the metrics;

2. The system architecture is treated with S-cube KB to generate the results automatically, such as the attacks and failure scenarios, with an evaluation of the likelihoods, and a proposition of measures to enhance the system safety and cybersecurity and to minimize the likelihoods of occurrence;

3. Define a new quantitative or qualitative analysis, since the main system architecture is modified and new data inputs are produced.

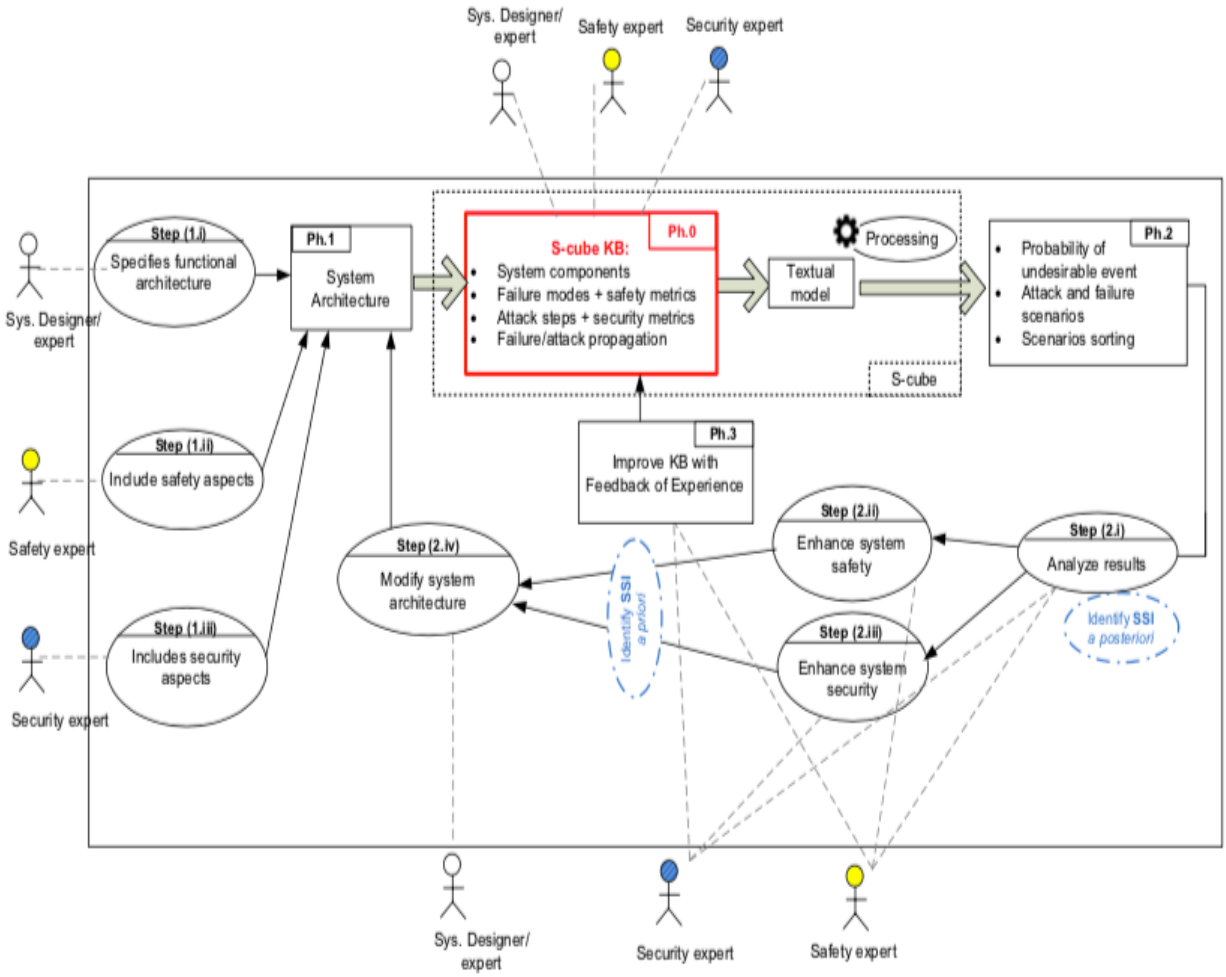

Figure 2.3 - The S-cube approach

- Model-based safety and security assessment approach

This model-based approach [51] was proposed to address the safety and cybersecurity of system architecture. It aims to model the system from three different perspectives because safety and cybersecurity engineering rely on specific tools: the system engineers model the system architecture using the Melody tool [52]; the safety and cybersecurity engineers model the safety and cybersecurity properties using extensions for cybersecurity of the Safety Architect tool, which is a tool for the risk analysis of complex systems using functional or physical architectures. These safety and cybersecurity properties contain the dysfunctional behaviors presenting how failures or cyberattacks are propagated in the system architecture, and the safety and cybersecurity requirements that the system architecture must validate and satisfy; the system architecture and the safety and cybersecurity model are combined into a single formal model called here Alloy model which is a language for expressing complex structural constraints and behavior in a system and it provides a simple structural modeling tool. This formal model aims to generate a formal validation of the safety and cybersecurity properties of the system architecture. This proposed approach is complex to apply it since it is based on many different tools to be achieved.

- CHASSIS

The Combined Harm Assessment of Safety and Security Information System [53] is an approach proposed for presenting the safety and cybersecurity assessments in a unified manner using UML notations such as use cases, misuse cases, and sequence diagrams. The first step in the CHASSIS process is to describe the functional needs of the system as a basis for the elicitations of safety and cybersecurity requirements. The users, the system functions, and services are described and modeled using use case diagrams. The contents of the use case diagram, are refined and the objects and their interactions are modeled using the sequence diagrams. The second step aims to define the safety and cybersecurity requirements, the safety and cybersecurity experts identify the potential misuses of the system, it can exist more than one misuse case per use case. The misuse cases are identified by combining the names of use cases with HAZOP guidewords to obtain the potential misuse cases of the system. They include all the factors leading to failure scenarios such as the external systems connected to the internal parts of the system, the authorized or unauthorized human users.

Based on the identified scenarios, the misuse case diagram is drawn, and it can contain safety and cybersecurity misuse cases.

- V-Shaped model

The proposed V-shaped [54] is based on the conventional V-model by including cybersecurity considerations and measures. It is a development process that depicts the relationships between the different lifecycle phases of a system. The V-shaped model aims to examine the threats and failures situations that may occur on a system in order to determine the safety and cybersecurity requirements, as well as to model the system design. The safety and cybersecurity requirements such as the tools, the cybersecurity algorithms, and tests, the attack test, are added to the system design in order to improve the safety of the system throughout its life cycle phases. The steps in in the V-shaped model are depicted in Figure 2.4.

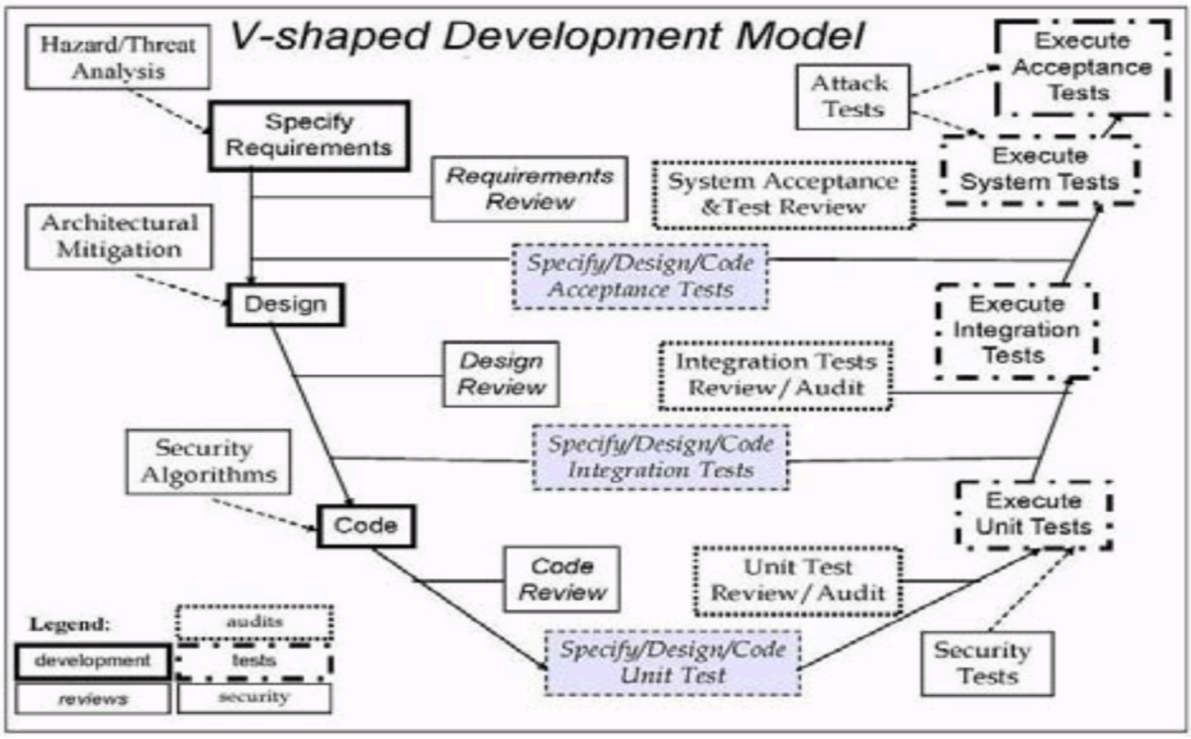

Figure 2.4 - The V-shaped model

- SysML-Sec

SysML-Sec [55] is a model-driven engineering approach for developing safe and secure systems that is based on SysML. SysML is a modeling language that is an extension of a subset of the UML. Based on the three steps of SysML: system analysis, system design, and system validation, the SysML-sec approach assesses the impact of cybersecurity requirements on system safety. The cybersecurity requirements and their relationships are modeled using requirement diagrams during the system analysis stage, and the attack scenarios that could occur are modeled using attack diagrams. At this stage, the system is also modeled by graphs to represent the assets and the system functionalities, as well as their relationships. In the system design stage, the cybersecurity mechanisms and properties are defined based on the cybersecurity requirements defined in the analysis stage. The goal of the system validation stage is to improve if the cybersecurity properties have been confirmed and if the system is safe and capable to face cyberattacks.

2.1.3.2. Generic approaches

The generic approaches study the security and safety at the level of each component [13] in the system design or the risk assessment. The approaches of this sub-category are proposed from scratch, and their processes are a list of standard steps to analyze the safety and cybersecurity risks. The approaches existing in this sub-category are Unified security and safety risk assessment method, Combined safety and security engineering process, Safety-security lifecycle process.

- Unified Security and Safety Risk Assessment method

This approach [56] considers both safety and cybersecurity risks in a unified process. The following are the steps involved in this approach:

1. The targeted system is defined, by identifying the hardware, software, and users, as well as defining the system functionalities, its criticality, and sensitivity of data;

2. Based on historical system attacks and failures, such as risk analysis reports, safety and cybersecurity requirements, and test results, the hazard and threat scenarios, as well as vulnerabilities are identified. The

relationship between safety and cybersecurity is determined here using the vector π *(v, t, h)*, where the value of this parameter is 1 if a vulnerability "v" is exploited by a threat "t" initiating an event that causes a hazard "h", and 0 if a vulnerability "v" is exploited by a threat "t" that does not affect the system's safety and does not cause a hazard "h";

3. Define the Critical Digital Assets (CDA), which can be either hardware or software and are the targets of the risk assessment. Then, using a defined equation and based on the safety integrity level defined in IEC 61508 and NEI 08-09 to determine the safety levels, and based on cybersecurity levels defined in IEC 61226 to determine the cybersecurity levels, determine the control risk (CR) for each CRA, which is the risk level associated with safety and cybersecurity design;

4. Determine the threat level based on the seriousness and the uncertainty of the consequences based on the motivation of threat source, the vulnerability, and the current controls;

5. Determine the hazard level by taking into consideration whether the hazard is independent of the threat or not, based on some established ranges of likelihoods;

6. Determine the asset impact for each CDA based on defined values;

7. Determine the safety and cybersecurity risk level using a defined equation and based on the values defined above;

8. Provide the control mechanisms and measures to reduce the risk level.

- Combined safety and security engineering process

The engineering process [57] is proposed to combine safety and cybersecurity risk analysis. It can be accomplished in six subsequent steps, which each step may necessitate a modification of the previous step. The steps are the following:

1. Identify the important assets that must be protected from harm;

2. Identify the harms that can occur on the assets identified;

3. For each identified harm, identify and analyse the failure and hazards situations for safety and the attacks and the threats for the cybersecurity that may cause harm;

4. Determine the vulnerabilities on each asset that can be exploited to carry out an attack;

5. Develop the safety and cybersecurity requirements, as well as some effective countermeasures to ensure that the assets can be protected from harm.

- Safety-security lifecycle model

The safety-security lifecycle model [34] was proposed in order to have a safe and secure pre-design phase for critical industrial systems. The first step of this model (see Figure 2.5) is to identify the functionalities and the scope of the system. After the identification of the hazards and the associated risks, the second step aims to identify the safety requirements to reduce the risks levels using the safety lifecycle from IEC 61508. After a safety investigation and the identification of the assets that need protection, the cybersecurity threats and the associated risks are identified, and the cybersecurity requirements are specified from the Common Criteria security project standardized as IEC 1508 in the third step. In steps 4 and 5, the commonalities and conflicts resulting from the integration of safety and cybersecurity are identified. The next step aims to realize the safe-secure system including the software and hardware. The use phase of this model consists to install the safety and cybersecurity requirements, to evaluate and validate them, by taking into consideration the whole system and the overall interactions among all the system components.

2.1.3.3. Approaches favoring the quantitative aspect

The approaches of this sub-category are built on and use advanced mathematical tools in order to improve the quantitative likelihoods of occurrence. There are two approaches for safety and cybersecurity risk analysis: Joint safety and security using BBN, Integrating security in BDMP.

- Joint safety and security using BBN

Bayesian Belief Network is used in this approach as a mathematical tool, which is a direct acyclic graphical model of nodes and arcs. It represents the conditional likelihood distribution of a set of random variables by nodes and arcs. BBN has traditionally been used for safety risk assessment, which includes uncertainty in risk evaluation and decision making, but some approaches were new approaches have lately been proposed to include safety and cybersecurity risk assessment. According to one of these approaches proposed in [54], each node can be considered as a safety or cybersecurity incident, or requirements and the interrelationships between them are depicted by arcs linking the nodes. It aims to identify the impacts of each node on each other and on the system reliability, such as the impact of safety accidents on the cybersecurity aspects and the impact of breaking the cybersecurity requirements on the safety-related events. This approach seeks to quantify the likelihoods in order to evaluate whether the safety and cybersecurity requirements are well realized in the system.

- Integrating security in BDMP

Boolean logic Driven Markov Process is a formal graphical model proposed initially for safety risk assessment, that combines the fault tree analysis FTA with the Markov process, by adding a dynamic feature to be modelled with a new type of connection, “the triggers”. This combination aims not only to provide good readability and hierarchical representation of failure events but also advanced quantification capabilities. The BDMP has been adapted to include cybersecurity attacks [58], by associating the Markov process with each leaf of an attack tree and introducing the use of triggers. It enables to graphically model the different failures (safety leaves) and attacks (cybersecurity leaves) scenarios that result in the same undesirable events. Once the BDPM is built, each cybersecurity basic event (leaves) is associated with a parameter based on the estimation of the time it takes for an attack to succeed, as well as the safety basic events based on the time it takes for an attack to fail and the likelihood of occurrence of undesirable events. These estimations are identified by safety and cybersecurity experts and aim to analyse the model qualitatively and quantitatively.

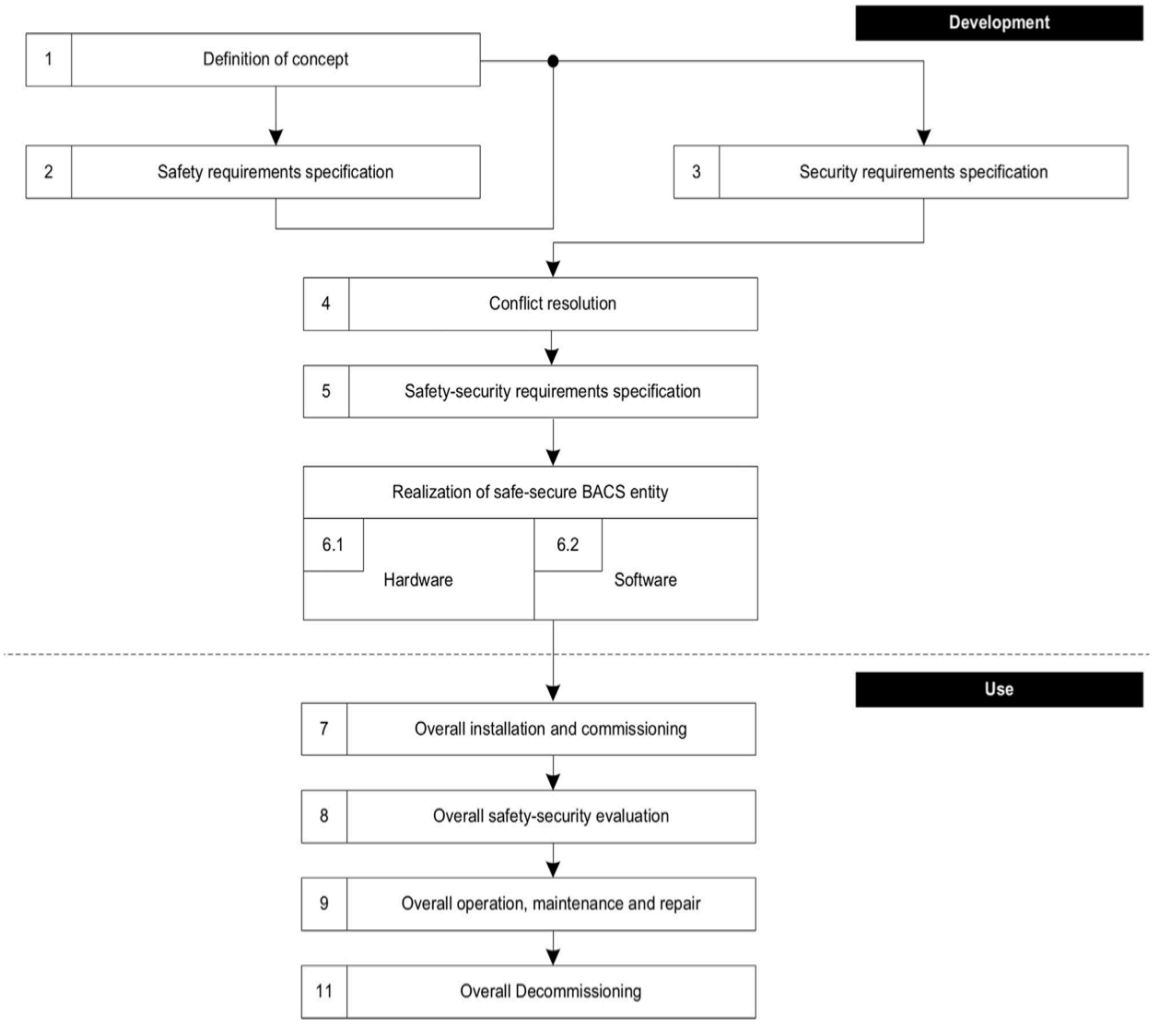

Figure 2.5 - The security-safety lifecycle model

2.1.3. STPA based approaches

Many recent developments are based on the STPA [59] [60], which was originally designed for safety risk analysis. In comparison to other safety analysis approaches such as FTA, HAZOP, FMEA, and so on, STPA requires a different analysis process. STPA is a safety analysis technique based on STAMP, which is an accident causality model based on system theory [61], and it analyzes the accidents and losses as a dynamic control problem, in which the accident occurs as a result of a behavior fault on the control rather than the consequence of a failure (which can always be assumed to be possible).

STPA is divided into four main steps (see Figure 2.6):

1. The definition of the system losses, hazards, and the system boundary;

2. The modeling of the control structure representing the interactions of the components using STAMP to build the control loop of the system;

3. The identification of the potential Unsafe Control Actions (UCA) for each control loop, and the associated safety constraints;

4. The identification of the potential loss scenarios related to the UCAs and the generation of safety requirements.

To add and integrate the cybersecurity to analysis, several authors have proposed extensions of STPA, or have been based on STPA. STPA-Sec [62] [63] was the first STPA-based approach for analyzing and assessing just the cybersecurity risks, it follows the same steps as the STPA process, but in STPA-Sec, it is possible to identify insecure control actions connnected to cyberattacks. The various approaches in this category are STPA-SafeSec, Combination of STPA-Sec with FMVEA, Combination of STPA and STRIDE.

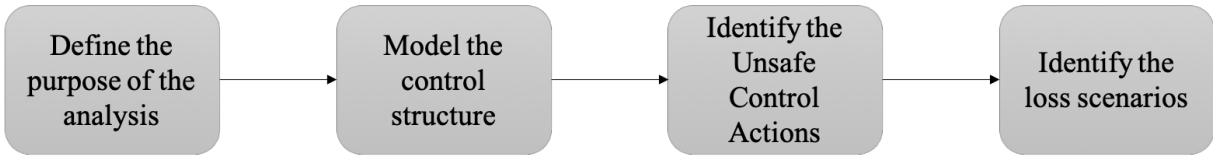

Figure 2.6 - The STPA process

- STPA-SafeSec

STPA-SafeSec [64] is the combination of STPA for dangerous events analysis and safety evaluation and the extension STPA-Sec for cybersecurity risk analysis. In STPA-Sec, the impact of Information Technology (IT) security on the control loop is investigated. STPA-SafeSec provides in-depth guidance of safety analysis on critical components and integrates the results with the safety analysis. Hazardous situations and attacks are considered control problems, and for each

one, there is a collection of conditions and guidewords that can be used to identify the scenarios of loss. STPA-SafeSec has two loops: one that represents the applied system as an iterative system for managing the modifications and the mitigation strategies, and another that manages the system complexity. The steps of STPA-SafeSec are as follows:

1. Identify the systems accidents and losses which have high impact levels;

2. Identify the safety and cybersecurity constraints;

3. Construct the control layer, which is a graphical representation of the control loop and the interactions between the controllers;

4. Define for each loop the control and hazardous actions (unsafe and insecure);

5. Map the control layer to the component layer, to identify the software, network, and algorithms for each physical component;

6. Refine and map the safety and cybersecurity constraints to the component layer, and add specific constraints if they exist;

7. Identify the hazard scenarios;

8. Guide a detailed cybersecurity analysis to the components that must be analysed in priority;

9. Identify and implement effective mitigation strategies for the system.

- Combination de STPA-Sec with FMVEA

A new safety and cybersecurity co-engineering approach, Systems-theoretic Likelihood and Severity Analysis (STLSA) [65], was proposed and it aims to combine the STPA-Sec with FMVEA because the STPA-Sec process results in the identification of failure or threat modes but does not provide further guidance on how to address those scenarios and to evaluate them in terms of severity and likelihood of occurrence. The loss scenarios for each unsafe/insecure control action identified by STPA-Sec are evaluated and the risk level of each scenario is assessed using FMVEA. Each scenario is seen as a failure mode with an effect, and each effect has a severity associated with it, the value of the severity is determined using a predeterminate scale. Each scenario is assigned a likelihood

of occurrence, and the likelihood of safety and cybersecurity loss scenarios are rated on two different defined scales.

- STPA and STRIDE

An extension of STPA [66] was proposed using the STRIDE threat model [37] in order to have a more comprehensive security analysis and a complete risk analysis. The extension in this approach appears in the last step of STPA, the identification of the loss scenarios, by identifying additional ones using the STRIDE threat model. The first two steps of the proposed are identical to those of the basic STPA. In the third step of identifying Unsafe Control Actions, the phrase Hazardous Control Actions is used because the control actions can be unsafe or insecure. New activities have been added to the fourth step of the identification of loss scenarios of STPA (see Figure 2.7):

1. Identification of STRIDE loss scenarios: Since the STRIDE model requires the Data Flow Diagram (DFD) of the system as an input, which describes the interactions between systems elements, the mapping of the structural control, which is the result of the second step of STPA, to DFD was proposed. After the mapping, the DFD is then modeled and used as input for the next step, which is to identify the threats on each interaction and component of the DFD using the STRIDE model, and after the threats are identified, the vulnerabilities on each interaction and component are defined. Following that, the scenarios, causal factors, and requirements for the hazardous control actions are determined;

2. Identification of physical loss scenarios: this activity attempts to identify the vulnerabilities and threats of physical cybersecurity since the assets of a system can include people that can play an important role in the execution of a loss scenario;

3. Verification of redundant loss scenarios: this activity removes the redundant scenarios from STPA or STRIDE leading to the same Hazardous Control action and it aims to create a list of consolidated loss scenarios.

2.1.4. Approaches based or found in standards

This category of approaches entails adapting existing standards for safety or cybersecurity risk analysis in order to incllude and integrate the other missed

aspects. In this category, two approaches exist ISA-62443-2 [16] and Framework for threat analysis and risk assessment inspired by ISO 26262 [67].

- ISA-62443-3-2

For security risk analysis, ISA-62443-3-2 is an extension of the standard IEC 62443, which is a set of "International standards of industrial communication networks – IT security networks and systems". This approach intends to conduct a cybersecurity risk assessment for the automated control system in order to improve the system safety and the target security level for the system under construction, as well as to define the safety and cybersecurity requirements specification to guide the system design. The steps involved in this approach are depicted in figure 2.8. The first step is to identify the system architecture, followed by a preliminary cybersecurity risk assessment using the existing safety risk analysis and risk matrix. Based on the first risk assessment, the system is partitioned into zones and conduits, because some assets systems may have the same cybersecurity and similar cybersecurity measures to mitigate risks. A comparison of the initial risks with the tolerable risks will be made, if it exceeds the tolerable risk, a full security risk analysis will be performed (the identification of threats, vulnerabilities, likelihoods, impacts, the proposition of countermeasures, the target cybersecurity level). Finally, the documentation for cybersecurity requirements enhancing the system safety is explained, which includes all the above-mentioned outputs in order to gain approval for the results of risk assessment.

- Framework for threat analysis and risk assessment inspired by ISO 26262

This framework was proposed to integrate the threat analysis and risk assessment inspired by ISO 26262, which is an international standard for functional safety for road vehicles that is based on the safety standard IEC 61508. This framework integrates nicely with the existing safety engineering processes and assures the functional safety of automotive systems. The workflow of this framework is depicted in figure 2.9, which begins with the definition of the system under evaluation, its full architecture, entities, and functionalities. After the system has been described, the cybersecurity threats that lead to safety risks will be analysed. This will be accomplished by identifying the assets that require security protection and the identification of the threats that may occur on these

assets. The asset/threat pairs are analysed and evaluated in terms of their likelihood of occurrence and severity of impact during the risk assessment step in order to estimate and determine the Security Level SL, which is a measure of the protection level required for an asset and aids in determining the cybersecurity countermeasures that must be implemented to reduce the risk level. SL is similar to the Safety Integrity Level used for functional safety. Finally, the cybersecurity requirements will be identified, and the countermeasures will be put in place. The proposition of a cybersecurity risk assessment aligned to existing safety analysis, this framework addresses the identification of all properties relevant for safety or cybersecurity.

They exist other safety and cybersecurity risk analysis approaches, but they are not widely used or recognized, and they are not included in the above defined categories. Some examples of these approaches are the Six-Step Model [68], Extension of SAFE [69], Extension of CARDION [70], Modelling safety and security concerns in AADL [71]. In the following section, the presented approaches are classified based on the following criteria: Phases of the risk analysis process, quantitative or qualitative analysis, application fields, and a discussion of the classification and the processes of the approaches given.

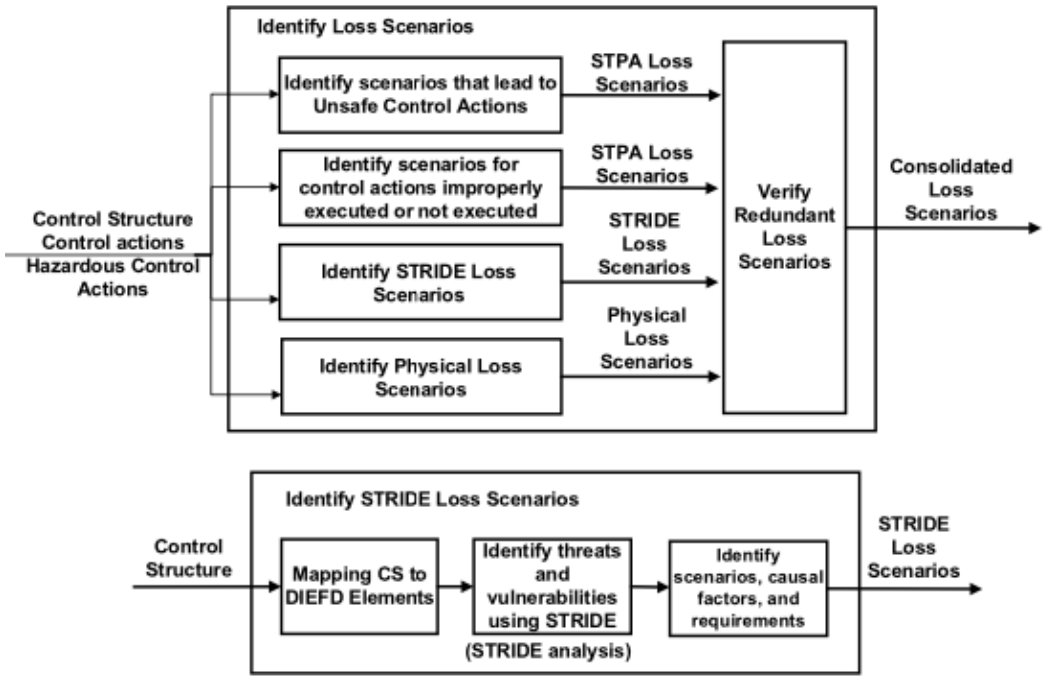

Figure 2.7 - The extended step to identify loss scenarios

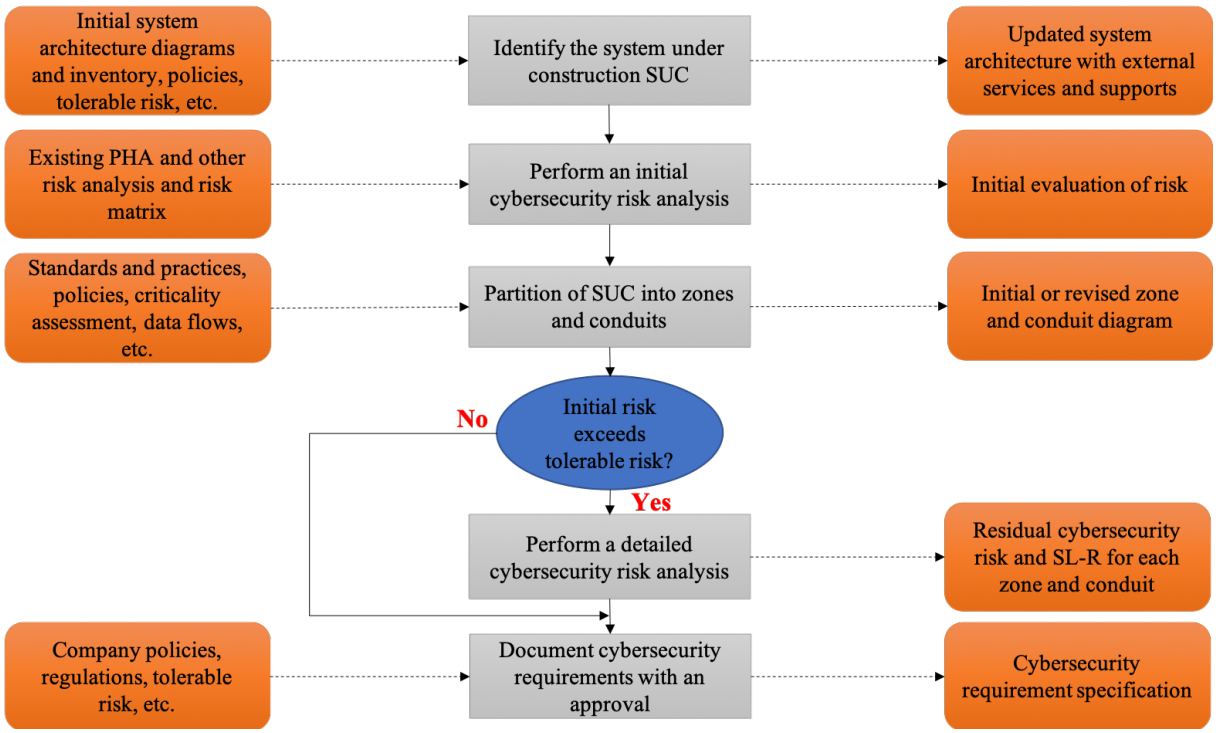

Figure 2.8 - The ISA-62443-3-2 process

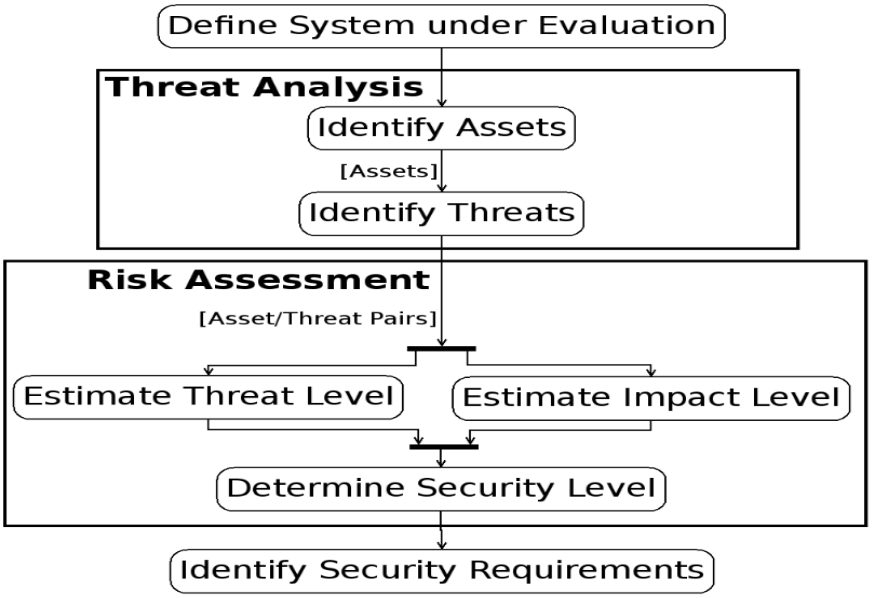

Figure 2.9 - The workflow of the framework inspired by ISO 26262

2.2. Classification and discussion

The risk analysis approaches are classified based on the steps of the risk analysis process that are covered in ISO 27005 standard [1] and shown in Figure 2.10. These steps are the following: The risk identification process which describes the risk scenarios that can harm the environment and people; The risk analysis process which includes the likelihood analysis and the impact analysis and serves as an input to risk evaluation and decision whether risks need to be treated; the risk evaluation which assist in the decision-making about which risks should be treated first. The risk can also be evaluated using quantitative or qualitative analysis depending on the available data, and the system analysed. A qualitative analysis subjectively evaluates and documents the risks using predeterminate rating scales, and expert data and elicitations. It considers all of the identified risks during the analysis process. On the other hand, a quantitative analysis evaluates the risks based on the feedback data or the historical databases. It is applied generally for the risks that have significant impacts. A qualitative analysis is usually included in the safety and cybersecurity risk analysis approaches that include a quantitative analysis. The approaches of this review are classified based on these criteria in Table 2.3.

The application domain criteria help us to understand the type of application and the corresponding domains of the safety and cybersecurity risk analysis approaches. The majority of the presented approaches are generic and cab be used in any domain, including industrial control system. A large number of risk analysis approaches are developed for the automotive domain or improved with an application of an automotive case study like SGM, FMVEA, SAHARA, CHASSIS, STPA-Sec with FMVEA the framework inspired by ISO 26262. Other approaches are generic and improved with the use of a case study in the domains of chemical, electricity, power and utilities, automation building, and aviation, including ATBT, FACT, STPA-SafeSec, Safety-security lifecycle model, Model-based system engineering. The remaining approaches are generic without their applications on a case study in their publications.

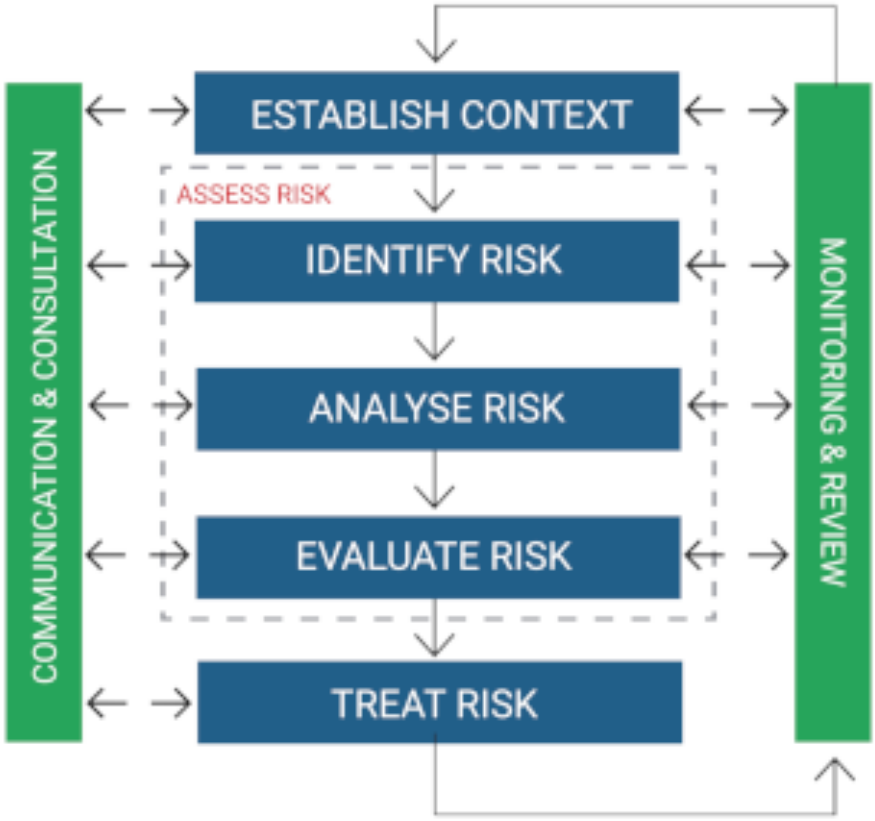

Figure 2.10 - The process of the risk assessment (ISO 31000)

The combined safety and cybersecurity risk analysis approaches are divided into five categories as seen above. In the first category, we have two sub-categories: (i) the extension of safety risk analysis to include cybersecurity; (ii) the extension of cybersecurity risk analysis to include safety. All publications focus more on exploring the influence of cybersecurity on safety, which explains why there are more approaches that have been extended to include the cybersecurity aspects than the cybersecurity approaches to include the safety aspects. This type of approach is more useful and may be used by personnel who are not professionals in the cybersecurity field, because they are based on well-known traditional safety risk analysis approaches. The limit of this type of approach is that only evaluates the impacts of cybersecurity on safety and vice versa when analysing dependencies between the two. While the approaches in the second category of combining existing safety and cybersecurity risk analysis consider the influence of cybersecurity on safety and vice versa in order to build safe and secure systems. The combination of approaches is based on well-known

safety and cybersecurity risk analysis approaches; hence, this type of approach can be used by employees who are not professionals in the cybersecurity field.

In the third category, the model-based approaches, unlike the generic approaches, are more practical for modelling the system architecture (components and functionalities) using specific tools, with the goal of analysing the safety and cybersecurity risks in a systematic process. The model-based approaches require more system expertise from the analysts, and thus are more difficult to implement in large industries with numerous components and connections. The generic approaches are easier to implement because the steps of their processes are conventional and understandable, most of these approaches include qualitative analysis. The approaches that emphasize the quantitative aspect produce good quantitative skills for estimating the likelihood of occurrence of safety and cybersecurity scenarios. However, this type of approach has many limits when it comes to dynamic modelling of complex systems related to their readability and computation time [11]. The approaches in the fourth category, which are based on the STPA concept, present a new way to perform safety and cybersecurity risk analysis based on control actions. These entirely qualitative approaches are aimed at identifying the causal factors of the hazard analysis related to the control structure and the interactions between the components. They intend to give a very large level of analysis, which is insufficient for identifying all the interactions between the safety and cybersecurity risks.

Following the classification of the risk analysis approaches into categories, it aims to show how the traditional safety risk analysis approaches are completed to include the cybersecurity aspects, such as the FMEA by including the vulnerabilities exploited to execute an attack as a cause of failure mode, the HAZOP by integrating the cybersecurity guidewords into its process, and the Bow-Tie by integrating the attack scenarios to the failure nodes. Furthermore, based on the representation of the approaches, it appears that the STRIDE threat model and the Attack tree are the most commonly used as cybersecurity risk analysis approach, in order to complete and integrate them to include the safety aspect. This classification also aims to present how the STPA process is extended or combined with other existing approaches to add the cybersecurity considerations. Moreover, it appears that the model-based approach from the integrated approaches category is the best option for a complete approach, although these approaches are rarely used and difficult to implement.

Risk analysis approaches	Risk analysis		Risk analysis process		
	Qualitative	Quantitative/ qualitative	Risk identification	Risk analysis	Risk evaluation
Extended approaches					
SGM	X		X	X	
Cyber HAZOP	X		X	X	
FMVEA	X		X	X	
Extended CFT		X	X	X	
SECFT		X	X	X	
Extension of FTA with security module	X		X		
Extension of TVRA		X	X	X	
Combined approaches					
Combination STRIDE and FMEA		X			X
ATBT	X		X	X	
SAHARA		X	X	X	
FACT	X		X		X
Integrated approaches					
S-cube		X	X	X	X
Model-based safety and security assessment approach	X		X		
CHASSIS		X	X		
V-shaped model	X		X		
SysML-sec		X	X		
Unified Security and Safety Risk Assessment method	X		X	X	X

Combined safety and security engineering process	X		X		X
Safety-security lifecycle model	X		X		
Joint safety and security using BBN		X	X	X	
Integrating security in BDMP		X	X	X	
STPA based approaches					
STPA-SafeSec	X		X		
Combination of STPA-Sec with FMVEA	X		X	X	
STPA and STRIDE	X		X		
Standards-based approaches					
ISA-62443-3-2		X	X	X	X
Framework for threat analysis and risk assessment inspired by ISO 26262	X		X	X	X

Table 2.3 - Classification of the presented risk analysis approaches

Each approach from each category has its own specificities and its limits in the system modelling, the way to integrate the safety and cybersecurity, the way to generate the hazardous scenarios, and the way to evaluate the risks analysed. To respond to the needs of the safety and cybersecurity risk assessment on industrial

installations and to enable the design of safe and secure critical industrial systems, it appears that an approach integrating the best characteristics and analysis process sorted from the existing approaches must be proposed and studied. For these reasons, we proposed a new model-based risk analysis approach that provides a new way to generate the cyberattacks scenarios encountered on industrial systems, as well as an evaluation of their likelihood and their combination with the safety risks that result in the same physical undesirable events.

2.3. Conclusion

In this chapter, we show the existing solutions for merging safety and cybersecurity risks in the same analysis. Approximately twenty approaches are divided into five categories: the extension of existing approaches, the combination of existing approaches, the integrated approaches, the STPA based approaches, the approaches based on existing standards. Each of the presented approach has advantages and is good to apply, despite its limits. We conclude that the most significant limits can be found in:

- The system modeling: In order to conduct a thorough, formal, and systematic risk analysis, it is crucial to model the system architecture and its components. This is not the case in most existing approaches.

- The level of complexity and detail: Some approaches are complex to apply in terms of time and steps, and they use specific tools in their analysis processes.

- To define the steps of a cyberattack scenario, the identifying of vulnerabilities presents a key step in risk analysis. The majority of the existing approaches do not leverage the vulnerabilities as entry data to determine the cyberattacks scenarios in their risk analysis processes.

- Some approaches do not explain the steps to conduct a cyberattack on an industrial system in their analysis processes, instead they identify the types of cyberattacks that can occur.

- Some of the existing approaches do not evaluate the likelihood of occurrence of the combined risks, despite the fact that this step is vital in treating severe risks.

Due to these limits, it is not possible to cover all the cybersecurity risks during the analysis process. Therefore, to address these limits, we offer a new model-based risk analysis approach that takes into consideration the links between safety and cybersecurity risks during the analysis process. It includes a step for modeling the components of the industrial system with a list of attributes that can present a source of vulnerability to the system. A list of generic vulnerabilities that can exist on any industrial system was generated in our proposed approach to be used in the generation of cyberattacks scenarios, and the possible cyberattack scenarios that can be encountered on all ICS levels of any industrial site were generated in a new way and in form of meta-models. The list of vulnerabilities and the meta-models of attacks scenarios serve as guides and catalogs, and they are used to input data into the application of our approach. These meta-models are then used in a computerized code in order to generate automatically the exiting attack scenarios on case study under investigation. The main objective of our approach is to make the risk analysis steps easier and more straightforward to apply with an appropriate degree of detail, depending on the amount of time and knowledge of users in the cybersecurity field. The steps of our proposed safety and cybersecurity risk analysis approach are presented in detail in the next chapter.

Chapter 3: The new model-based risk analysis approach that generates attacks and combines them with safety risks

In this chapter, we develop a new model-based risk analysis approach that combines the safety risks with the cyberattacks related to the cybersecurity risks in the same risk analysis. It introduces a new way to generate cyberattacks systematically based on the modelling of the system architecture and a list of generic vulnerabilities found in industrial systems. In this chapter, the steps for gathering data and generating the attack scenarios are described. In the next chapter, we will go over the rest of the steps of merging the risks.

3.1. Introduction

As stated in chapter 1, the problem was that cybersecurity became an important matter in the critical industries and their risk analysis, and the need of combining safety and cybersecurity risks in the same analysis grew. A vast range of safety and cybersecurity risk analysis approaches have been proposed and developed, as highlighted in chapter 2. Following the problematic and the limits of the existing approaches, in this chapter, we offer our new proposed model-based risk analysis approach, which helps in the generation of the cyberattacks, their combination with safety risks, and simplifies the steps of the risk analysis process. The main steps of our approach are:

- The construction of a model that depicts the industrial installation.
- The proposition of a guide to defining and searching for the vulnerabilities.
- The proposition of new meta-models to represent the cyberattacks in order to capitalize the knowledge Base KB required for the step of the automatic generation of attack scenarios.

Each step of our approach will be modelled in a UML diagram in order to show the relationship between the steps of the approach (each step is described further below) and, in particular, to illustrate the meta-models generated during the approach. It is a model-based approach since we use models to display the industrial facility, the data needed to generate the incidents related to the cybersecurity, and a KB to generate the attack scenarios. Thus, the system architecture is modelled during the process of the approach, and the attacks scenarios are given in meta-models. The process of our approach is based on data collected from the industrial system to be analyzed such as the existing classical hazard study, the system mapping, the organizational policies applied. This proposed approach covers the best characteristics and analysis processes of the previous approaches in order to achieve the necessary and desired criteria. The different objectives of the proposed approach are the following:

- It is applicable to the industrial control systems, especially in the process industry (ICS process);

- It presents the connections between the attack's scenarios and the hazardous situations that lead to the same undesirable events;

- It is a guided, formal and systematic approach, based on the modeling of the system architecture;

- It is detailed enough in terms of system architecture modeling, attack scenarios, and the hazardous situations;

- It is simple and quick to implement in terms of time, steps, and for non-expert users in the field of cybersecurity;

- It automatically generates the attacks scenarios from generated data and meta-models;

- It aims to simplify and combine many risk analysis process steps. It can reduce the cost for the application of risk analysis approach.

In order to present the proposed approach for combined safety and cybersecurity risk analysis, this chapter is organized as follows: Section 3.2 presents the contribution and the principle of our proposed approach. Section 3.3 explains how to collect data and generate the attacks scenarios in order to deal with our objective of joint safety and cybersecurity risk treatment; Section 3.4 presents a discussion of our approach as well as a conclusion. The following chapter will present the remainder of the approach, which will include the combination of risks as well as the ways for evaluating and treating them.

3.2. Contribution and principle of the proposed approach

In this section, we present first the contribution and the principle of our proposed approach. The risk analysis approach is relying on a Knowledge Base KB, that gathers the generic list of vulnerabilities defined in Section 3.3.1.3, as well as the cyberattack scenarios generated in meta-models in Section 3.3.2 and

Annex A. The generic data and meta-models of the KB, as well as the system architecture (components and attributes) defined in Section 3.3.1.2 provide the inputs for automatically generating the cyberattacks scenarios, which are the outputs of the computerized approach.

Figure 3.1 depicts the principle of the approach. The automatic generation of the existing attack scenarios on a case study results from the processing of an algorithm using data produced from the meta-models of attack scenarios and the other inputs (system architecture and list of vulnerabilities). The contribution here in our approach is the automatic generation of attack scenarios using the data generated in the KB. The attack scenarios generated are then merged with safety risks in the same graph as the process of the most common approaches.

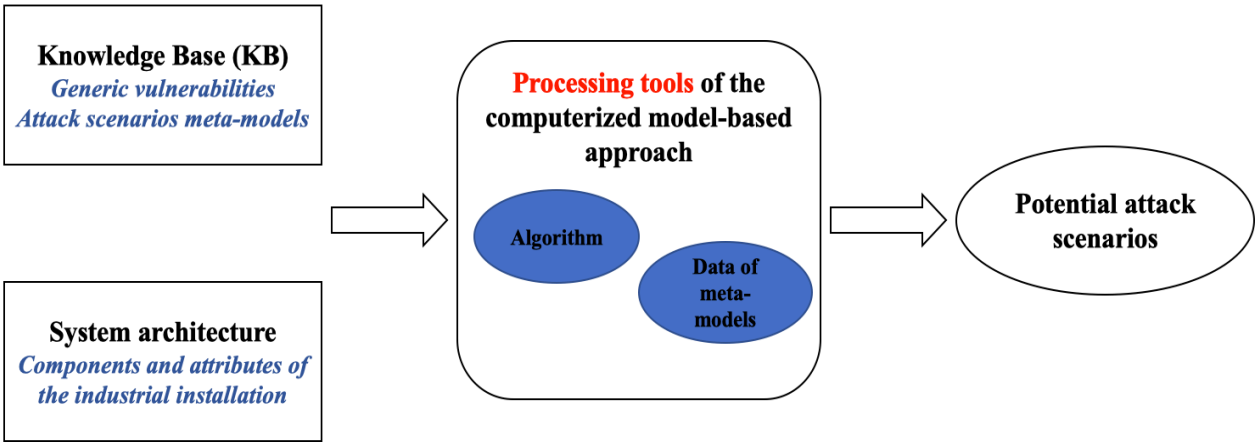

Figure 3.1 - The principle of the proposed risk analysis approach

Finally, we have three different types of models in our approach. The first type: As inputs, the attack scenarios generator model and the vulnerabilities checklist that reflects the KB. The second type is that we have a model that describes the system architecture, as well as the state of the existing vulnerabilities. The third type of models: The outputs of the approach include the existing attack scenarios, which are combined in the same meta-model with safety risks (cyber Bow-Tie) in order to represent the risk analysis and the occurrence of undesirable events. In order to collect all necessary data and to have a comprehensive risk analysis approach, our approach proposes seven steps. The steps for gathering data and

generating the meta-models of attacks scenarios are outlined in the next section. The rest of the approach, such as the combination of safety and cybersecurity risk and their evaluation are detailed in the next chapter.

3.3. Proposed approach for combining safety and cybersecurity risk analysis

Before beginning the presentation of our proposed approach, the UML model is introduced. The UML is a graphical modeling language with the goal of representing the real-world objects in the form of classes and objects. A class is an abstraction of the real-world that gathers a whole of objects that have common characteristics and behaviors. An object is an instance of a class, that inherits the characteristics of the class to which it belongs. The UML was extensively used in several cases of system modeling and risk analysis [72]. In our approach, we use the UML, because it is a means to formalize a model, in order to model each step of the approach into classes and display the relationships between them. It also for the creation of a database as information that can be used to automatically generate the attacks scenarios, as well as information for future learning from the accidents [72]. The next section outlines and describes the different steps of the proposed approach.

The proposed approach consists of seven steps divided into three big parts. In this chapter, the first two parts are covered in detail respectively in Sections 3.3.1, 3.3.2. The rest of the approach, which includes the combination of safety and cybersecurity risk, as well as their likelihood evaluation and treatment, will be covered in the next chapter. The diagram in Figure 3.2 depicts the general structure of our risk analysis approach. The first part of data collection seeks to compile a list the physical undesirable events that pose significant threats to the system, with their sources ranging from safety to cybersecurity, model the system architecture, and look for vulnerabilities. These collected data from the industrial installations represent the inputs for the second part of the search for the possible attacks, which aims to generate automatically the attack's scenarios and to create a catalog for attacks scenarios. The final part seeks to combine the hazardous situations related to safety risks and the attacks related to cybersecurity risks. Usually, the risk analysis approaches contain the same concept of defining, analyzing the risks, evaluating and treating them. The contribution of our work is

on the way of modelling the system architecture, providing a list of vulnerabilities, and automatically generated the possible attack scenarios. The details of each step with the UML diagram are given in the rest of this section.

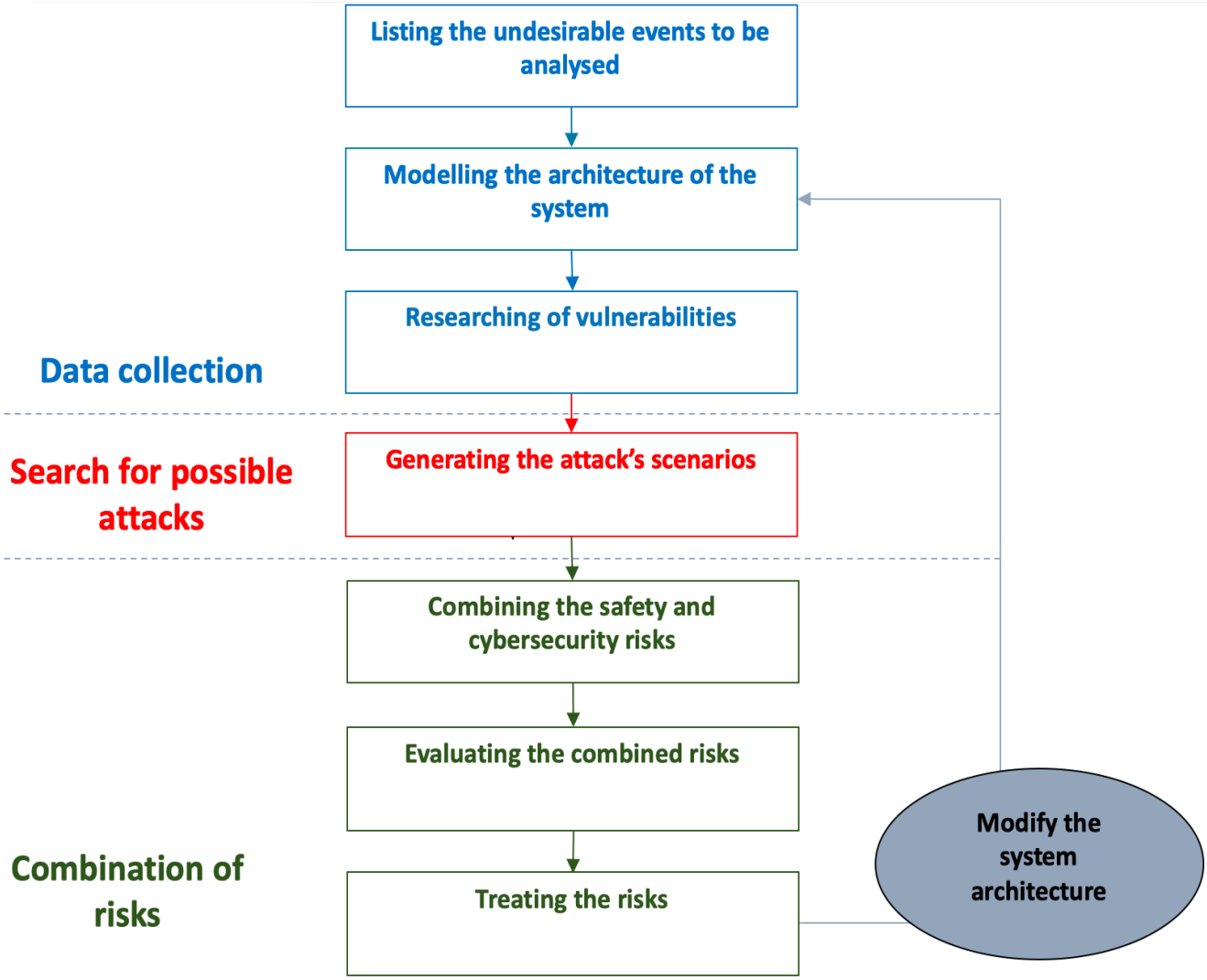

Figure 3.2 - The Overall schema of the proposed risk analysis approach

3.3.1. Data collection

In this section, we will go through the first three steps of the proposed approach, which include modeling the system architecture and gathering some

necessary input data for the rest of the process. Section 3.3.1.1 explains how the physical undesirable events are searched and listed. Section 3.3.1.2 covers how to model the system architecture. Finally, Section 3.3.1.3 explains how to look for potential vulnerabilities that can exist in an industrial system.

3.3.1.1. Listing the undesirable events

This step identifies the list of undesirable events that could occur in the studied industrial system. It is a vital step that is included in almost every analysis approach. It helps to gather the necessary data for the step of combining safety and cybersecurity risks. The definition of undesirable events in our approach are described below, as well as how the list of these events will be searched.

a- Definition of undesirable events

The undesirable events are the physical events whose occurrence poses risks to a system and must be considered during risk analysis. The occurrence of each undesirable event, such as an explosion, a fire, a toxic release, and so on [73] is the result of a sequence of events that, if uncontrolled, will result in undesirable consequences (harm) to the industrial system. Figure 3.3 depicts the process of occurrence of a physical undesirable event. This schema is a Bow-Tie diagram [6], and it might be called “Cyber Bow-Tie” since it includes the cyberattacks as sources of initiating events with the hazardous situations. It will be used in the steps of combining the safety and cybersecurity risks.

An initiating event is the first root cause of occurrence, and it disrupts the normal processes of the system, resulting in undesirable outcomes, such as human error and machine failure. In our approach, an initiating event can occur as a result of one or more hazardous situations (natural accidents, failure modes) relating to safety risk, or as a result of one or more cyberattacks, or as a result of a mix of both linked by using AND/ OR gates. Therefore, a physical undesirable event can occur due to one or more initiating events. In the case of many initiating events, if any of these events can cause the undesirable event, the Or operator is used; if many events are required for the occurrence of the undesirable event, the AND operator is used. It appears that in some circumstances, an initiating event is followed by one or more secondary events that serve as complementing events to the occurrence of the physical undesirable event. In the next section, the way for listing and searching the physical undesirable events is described.

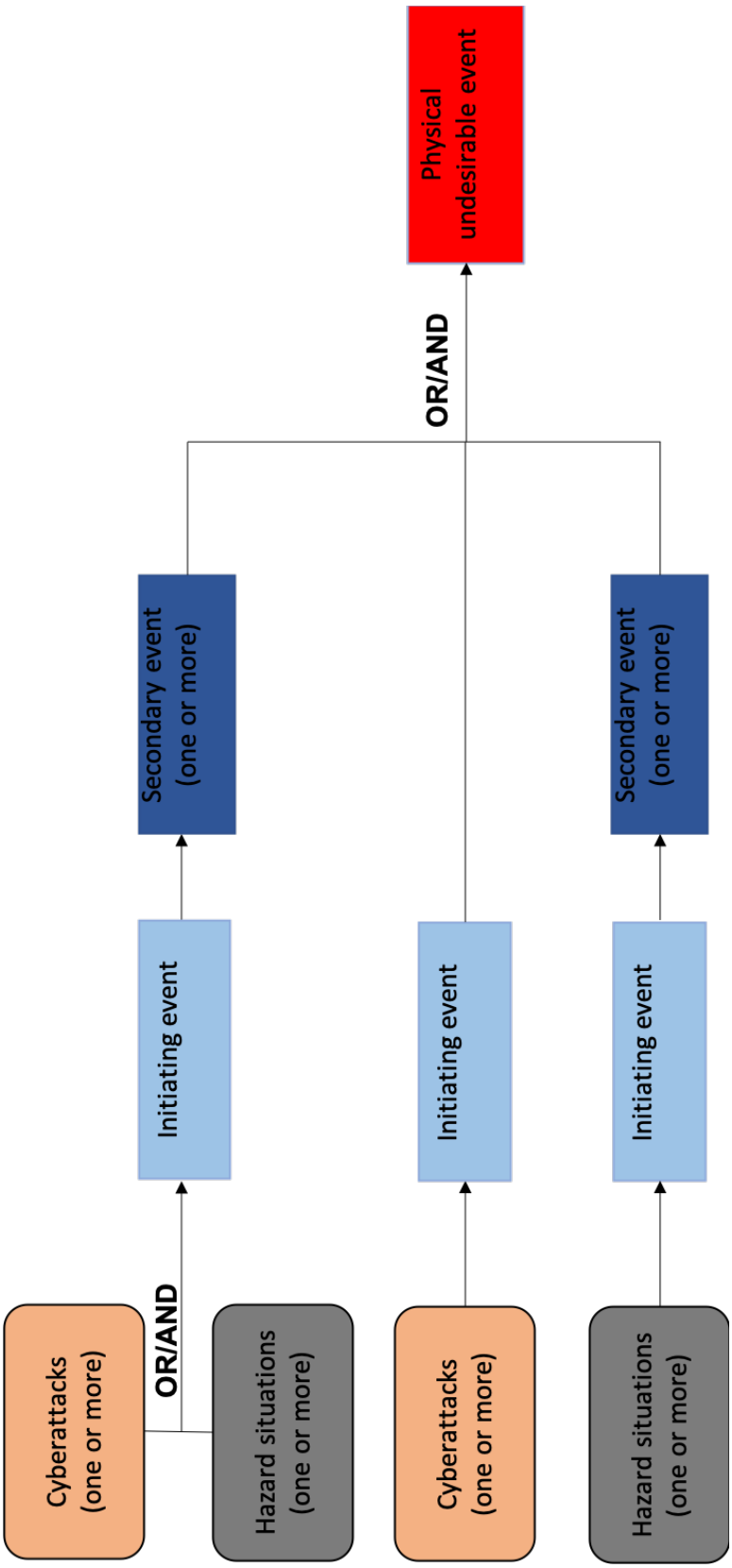

Figure 3.3 - The schema of the occurrence of an undesirable event

b- How to list and search the physical undesirable events?

Typically, critical industrial systems all over the world are forced to apply a hazard risk analysis study (safety risks). The most classical hazard risk analysis approaches used and known are the Bow-Tie, the HAZOP, the FMEA, the PHA, and other approaches. These hazard studies can define in a preliminary or detailed analysis the hazardous situations, the initiating and secondary events that can lead to the occurrence of undesirable events. In our approach, the physical undesirable events are searched and listed in the following steps:

- List based on the existing classical hazard study applied to the analyzed system, the physical undesirable events and their sources of occurrence. If this is not the case, the list of all of these events can be created by safety experts.

- Indicate the hazard situations leading to each initiating event listed, as well as whether the source of occurrence might also be from cyberattacks, since these cyberattacks are not included in the classical hazard study. This step can be completed by cybersecurity or safety experts.

- Identify if there are any other undesirable events with initiating events that can only occur as a result of a cyberattack and are not included in the classical hazard study. These events can be defined by experts in the domain of cybersecurity or safety.

List the initiating events for each gathered and defined physical undesirable event, as well as their possible sources of occurrence (cyberattack or hazard), and the secondary events, if any exist. Then, using the existing classical study or the pre-defined French matrix of the severity levels shown in Table 3.1 [74], define its level of severity. A severity level reflects the level of the impact of the occurrence of an undesirable event on the overall system, as well as how the service levels are affected by the current state of the system. There are five levels of severity in the scale in our approach: Disastrous, which is the highest level of impact, Catastrophic, Important, Serious, and Moderate, which is the lowest level of impact.

During our risk analysis approach, we must examine any physical undesirable events that provide a high level of risk to the industrial system and have a level of severity more than or equivalent to Serious. A list of physical undesirable events with their levels of severity, their initiating events with cyberattacks or hazard sources, and the secondary events are the outputs of this step. Following the generation ofthe attacks scenarios in the following steps, these undesirable events will be presented in the next step in order to demonstrate the combination of safety and cybersecurity risks.

Level of severity	Designation	Description of the consequences
5	DISASTROUS	Serious impacts on 10,000,000 people. Permanent loss of a critical infrastructure.
4	CATASTROPHIC	Serious impacts on 1,000,000 people. Temporary loss of a critical infrastructure. Permanent loss of a major infrastructure.
3	IMPORTANT	Serious impacts on 100,000 people. Disruption of the national economy. Temporary loss of a major infrastructure.
2	SERIOUS	Serious impacts on 10,000 people. Disruption of the national economy.
1	MODERATE	Serious impacts on 1,000 people.

Table 3.1 - The scale of severity levels for physical undesirable events

The UML diagram in Figure 3.4 describes the step of listing the physical undesirable events and the relationships between them and their initiating and secondary events. Its goal is to construct a database for future risk analysis and backups for the physical undesirable events that have already occurred on an industrial system. When this step is applied to a case study, these data of events will be filled in Excel sheets by the user who is using the approach. Using the UML model for this step, all the relationships between all the classes of events and the list of severity levels from Table 3.1 are provided in Excel sheets. The classes in the UML are shown below, the yellow class indicates that the data of this class are predefined and fixed for all the cases studied in our approach:

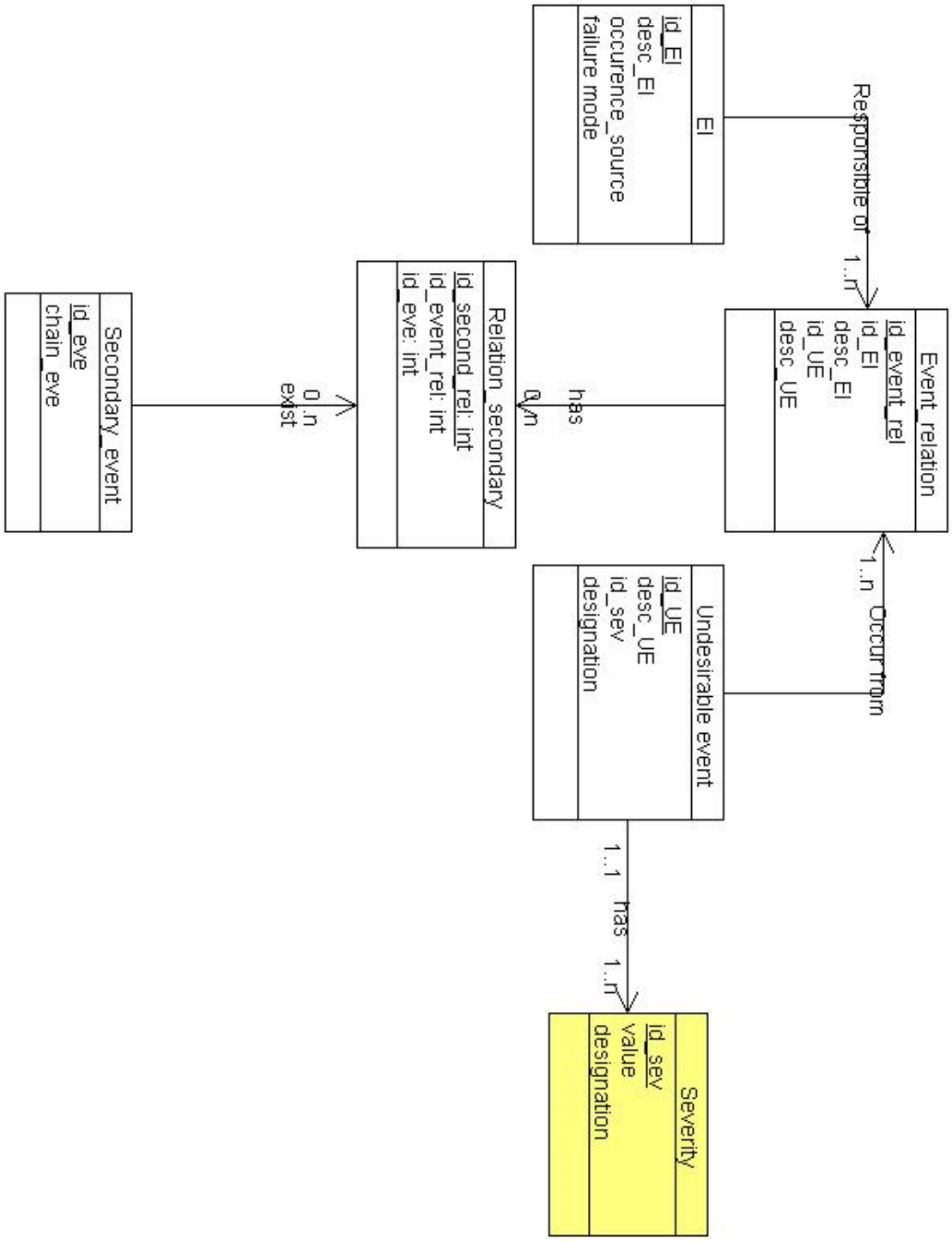

Figure 3.4 - The UML diagram for the undesirable events

- The “Undesirable event” class displays the different physical undesirable events that might occur on an industrial system, each undesirable event has a unique identifier, description, and value of severity from the “Severity” class.

- The “Severity” class displays the possible values of severity level from Table 4.1, with an identifier, a value, and a designation for each level.

- The “EI” class has the list of initiating events that lead to the occurrence of undesirable events, each EI has an identifier, a description, sources of occurrence, and the hazard situations from a classical hazard study.

- The occurrence of an undesirable event can arise as a result of one or more initiating events, the class “Event relation” represents this relationship, which is connected by AND/OR gates and contains an identifier, the undesirable event, and their initiating events.

- The “Event relation” is linked to the class “Secondary event” which provides a collection of secondary events. Because there is a sequence of one or more secondary events following the initiating event, the class “Relation secondary” is created to represent this relationship.

Our risk analysis approach begins with the step of listing the undesirable events because, in the following step of modeling the system architecture, only the components and equipment that are responsible for the occurrence of these undesirable events will be modeled. In the following section, the steps for modeling the system are provided.

3.3.1.2. Modeling the system architecture

In this section, the architecture of the analyzed system is modeled. This step happens after the step of the undesirable events, because in this approach we just model the systems responsible for the occurrence of the physical undesirable events, as indicated in the section below on “How must be modeled from the system”. The physical architecture (sensors, valves, pumps, actuators, servers, computers, etc.) and the IT architecture (software, communication protocols) are both modeled. The goal of system modeling is to understand the system’s

functionality, and it aids us defining, in a systematic and formal manner, the vulnerabilities that exist on the system components and are responsible for the occurrence and the generation of the attacks scenarios in the following sections. Modeling a system aids in a thorough and holistic risk assessment, by analyzing the possible number of scenarios that can affect each part and component of the system. Most of existing approaches do not model the architecture of the system in their processes, hence this step is required for the rest of the approach process.

The data for this step of modeling are gathered via the system mapping and inventory, both of which are already present in most industrial systems. The goal of system mapping and inventory is to depict the system's functionality (sub-systems) and behaviors, as well as their components and interactions. For example, in an industrial site of beer production, there are two sub-systems with different functionalities: the production system and the sterilization system. For each sub-system, sensors, valves, actuators interact with each other for production and communicate with a PLC control and the SCADA system. All the relations and communication between the components must be depicted in the system inventory and mapping.

What must be modeled from the system?

Modeling all of the physical and IT components in complicated and large industrial systems with a lot of physical components and software becomes challenging and time-consuming. For these reasons, in this step, the components that are responsible for the occurrence of the initiating events of the physical undesirable events (section 3.3.1.1) are modeled, that is, the components whose failure or abnormal functionality due to an accidental situation or a cyberattack can cause to the occurrence of the initiating events. Therefore, the components of the sub-systems or systems, which their failures are the sources of the initiating events or which are affected by the consequences of the initiating events, are chosen to be modeled in this step.

How the system components are modeled?

The components are modeled into tables with a list of defined attributes. These attributes are presented below in Table 3.2:

Attributes	Description
Component type	It can be a sensor, valve, or PLC, server, etc.
Physical access	If the component exists in a location with secure physical access or not, the access is through a closed door, with badges, or keys, etc., and if the component can be accessed by access from employees, visitors, service companies to components is well managed.
Internet connection	If a component has a connection to the internet, the user can access to worldwide websites and applications.
Remote access	If a component can be accessed remotely from outside the industry by an employee through his computer or his smartphone to control the physical process.
Removable media	If on a component a removable media such as a USB drive, a Hard disk, etc., can be plugged.
Email reception	If a component which is a computer station and can receive emails from outside the industry.
Software	The critical software implemented on the component, the software that can have security bugs, like anti-virus, operating system, automates, etc. The possible vulnerabilities that can exist from this attribute can be extracted from CVE which is a database listing the public disclosed cybersecurity vulnerabilities from different products

	and software [39]. For example, if a computer is implemented by Windows 10, this vulnerability CVE-2021-40460 from the database can exist on that component.
Other attributes	There are specific attributes for components in a case study and can represent a source of vulnerabilities, such as an intelligent sensor with a Bluetooth option, a vulnerable communication protocol used, a vulnerable mark of products (the vulnerabilities can be extracted here also from the CVE database), etc.

Table 3.2 - The list of attributes to model a component

The list of described attributes was chosen because they can significant sources of vulnerabilities. In order to choose these attributes, a research of the modeling approaches and the most frequent sources of cyberattacks was conducted. The Viable System Model VSM [75] is a modeling tool created by Stafford Beer with the goal of demonstrating the importance of modeling the environment surrounding all levels of industrial systems, which communicates and exchanges data with the internal and external systems, and represents a critical source of cyberattacks and hazards, such as the internet connection, physical and remote access from competitors, maintenance companies, employees. Furthermore, according to a report on cybersecurity statistics and trends [76], remote workers continue to be a target for cybercriminals, moreover 95% of cybersecurity breaches are caused by human errors, 88% of organizations and industries worldwide are exposed to phishing emails [77] (the attributes of emails reception), and so on. These components and their attributes aid in the next steps in defining the existing vulnerabilities and generating the attack scenarios.

Each component is linked to one of the three ICS levels described in Chapter 1: Field level, control level, and supervision level. The next section requires us to break down each ICS level into zones in order to find vulnerabilities (Figure 3.5).

The field level contains the physical components zone; The control level contains the PLC zone and the automate programming and configuration stations zone; The supervision level contains the supervision stations zones and the computer stations zone. Other zone, if any, can be creating depending on the system being analyzed. Therefore, each component is associated to a zone of an ICS level.

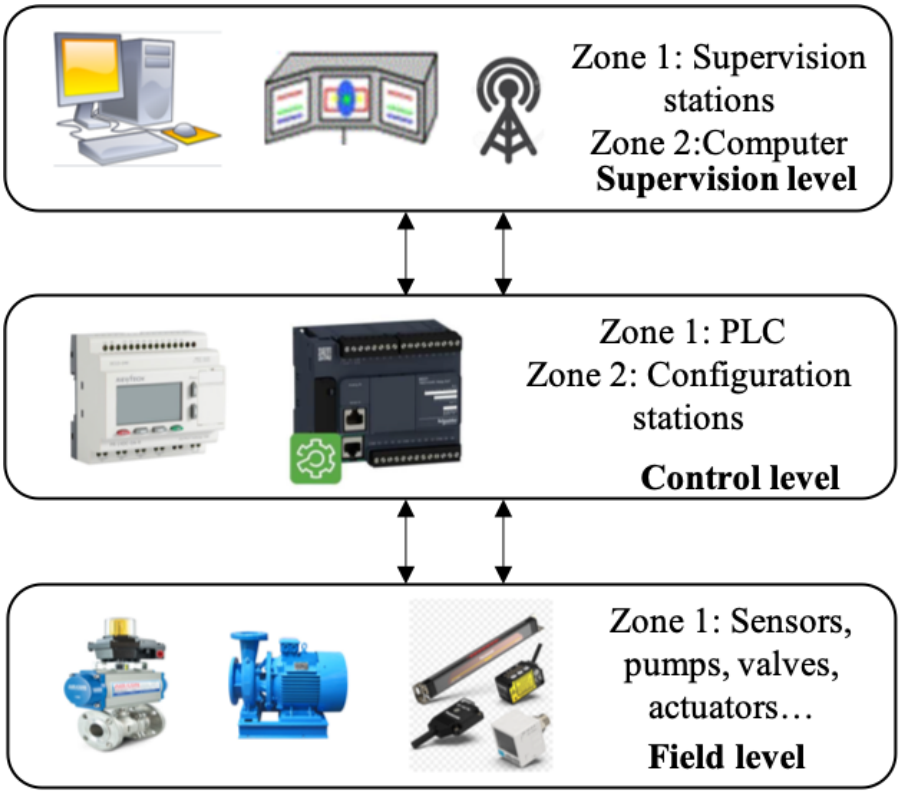

Figure 3.5 - The architecture of ICS levels and zones

The UML diagram in Figure 3.6 depicts a database of the modeled components and their attributes, as well as the relationship between the modeling step and the previous step of listing the physical undesirable events. When this step is applied to a case study, these data of components will be filled in Excel sheets by the user who is applying the approach. Based on the UML model for this step, all of the relationships between all the classes of components, the relationship with the initiating events, and the list of different ICS levels zones are presented and predefined in the Excel sheets. The following are the classes in the UML:

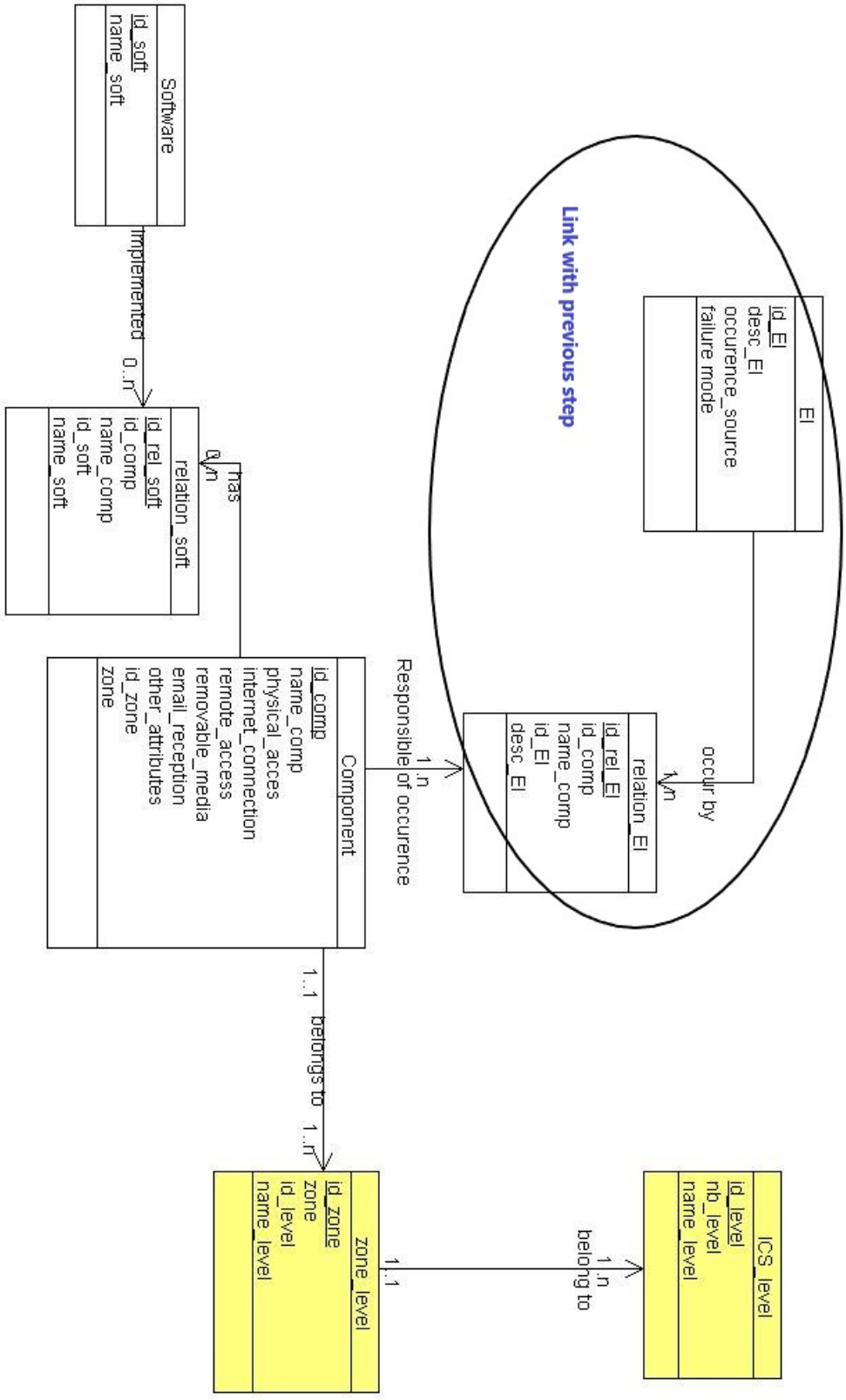

Figure 3.6 - The UML diagram for the system modelling

- The “Component” class displays the list of components that need to be modeled as well as their attributes. Since only the components responsible for the occurrence of initiating events are modeled, this class is linked to the class “EI” from the previous step. The class “relation EI” was created to represent this relationship between a component and one or more initiating events.

- The “Component” class is linked to “software”, which is a list of software that are implemented on the component. Because a component might be implemented by one or more software, the “Relation Soft” class was built to represent this relationship.

- The “Zone” class displays the list of zones defined and connected to the “Component” since each component is associated with a zone. The “ICS level” class represents the three different industrial levels presented in Chapter 1, each of which can be decomposed into one or more zones.

The next section will describe how to find and define the vulnerabilities that may exist on components and their attributes, as well as on a zone of ICS level, as stated in the section of system modeling. The following section presents the ways for searching the vulnerabilities.

3.3.1.3. Searching for vulnerabilities

A vulnerability is a weak point in a system, and the successful exploitation of at least one vulnerability, which can be technical, human, or organizational [1], is required for an attack to cause damage to an industrial system. Figure 3.7 depicts, in a schematic manner, the reality of how attackers target a system by exploiting its vulnerabilities.

The vulnerabilities in our proposed approach provide crucial information for generating the attack scenarios that result in the occurrence of undesirable events. In most existing approaches, this step is missing, the vulnerability is not identified and used as input data to find the possible attack scenarios that can occur. To accomplish this step, and search the existing vulnerabilities on the investigated system, a list of generic vulnerabilities that can be encountered on industrial systems has been established. This list was created based on a research of the most

frequent vulnerabilities found on industrial systems [78] and has been tested and validated on visits to industrial sites, one of which is a chemical platform that is looking to integrate cybersecurity into its risk analysis.

The list of vulnerabilities is transformed into a list of organizational policies and security barriers that can be implemented on a system. For example, the antivirus software is a security measure installed on a computer station to prevent the execution of a virus or malicious code, but, if the antivirus is not up to date or contains a security issue, it might pose a source of a vulnerability to the industrial system. This list is divided into several categories: Awareness and responsibility; Physical access to the system; Digital access to the stations, computers, and PLCs; Control of equipment; Automate configuration; Remotely access and connection to the internet; Backups and continuity. Table 3.3 presents this list of organizational policies and barriers, as well as how they are transformed into vulnerabilities.

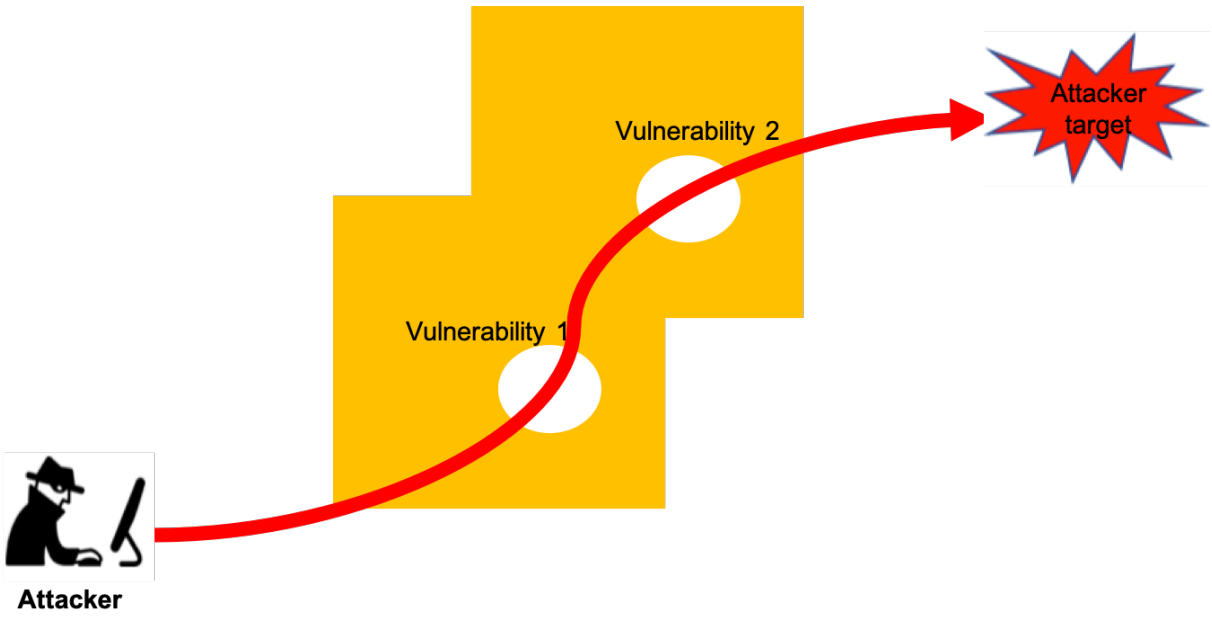

Figure 3.7 - The way to execute an attack

For each policy and barrier, an applicability level will be defined, this applicability level will show if there are sufficient tools and rules to implement the policies and the barriers in a good condition and manner. The security barriers and the organizational policies are assessed in the following way: There are five levels of applicability presented on a qualitative scale in Table 3.4. These applicability values will be used in the step of evaluating the likelihood of cyberattacks. The level "1" is the highest level of applicability, while "N/A" indicates that the policy or the barrier does not exist. For example, if there is no way to use and connect a USB key on a component, the level of applicability of the management policy for using the removable media will be "N/A". Level "4" is the lowest level of applicability and the greatest source of vulnerability. Depending on the values of applicability levels, each policy might be regarded as a vulnerability or not. The vulnerabilities that can arise as a result of the implementation of policies and barriers are shown in Table 3.3.

Organizational policies and barriers	**Vulnerabilities**
Awareness and responsibility	
The awareness of internal employees to the security	*The employees are not well formalized about cybersecurity*
The responsibilities of employees are attributed and defined	*The responsibilities are not well attributed and defined*
The awareness of employees (how they interact with the phishing emails)	*The employees are not well formalized to interact with emails*
Physical access	
The accesses to equipment are secured with badges and keys	*The accesses are not with badges and keys, or the accesses are not well secured*
The accesses from outside the industry are accompanied during a visit	*The visitors from outside are not accompanied during the visit*
Digital access	
The digital accesses are secured (authentication)	*The digital accesses are not through an authentication*
Passwords management (periodic modification, generation)	*The passwords are not too strong, or there is no periodic modification*

Accounts management (habilitation)	*The access to the user's accounts is without restrictions*
Control of equipment	
The management of using the removable media (USB, Hard disk)	*No management for use of removable media, or not well applied*
Alert in case of the modification of equipment configuration	*No alert in case of modification*
Detection mechanisms: anti-virus software	*Anti-virus software does not exist, or is not well configured or up to date*
The software implemented and used are secured	*Software with security bugs, or not up to date*
Robustness of operation systems	*A vulnerability on the operating system, or not up to date*
Automate configuration	
The modification of PLC automate is managed	*No alert in case of modification of PLC automate configuration*
Code backup management	*There is no backup for the code or no periodic backup*
Remotely access and connection to the internet	
Restrictions on the parts connected to the internet	*No restrictions for the connection to the internet (access to all kinds of websites and applications)*
The connection to the internet is protected by firewalls	*No firewall used, or firewall not well configured*
The communication protocols are secure	*The use of vulnerable communication protocols (no data encryption…)*
The wireless connection is managed	*No restrictions on Wireless connection*

The remotely accesses are controlled and managed	*The remote access is not well managed*
Filtering the received emails	*The received emails are not filtered*
Anti-spam software	*Anti-spam software does not exist or is not well configured or up to date*
Backup and continuity	
Backup and restoration of data	*There is no backup for data or no periodic backup*

Table 3.3 - The list of generic organizational policies with the corresponding vulnerabilities

Level of applicability	Designation
4	No existing rule and dispositive
3	Rule and dispositive partially applied
2	Sufficient rule and dispositive applied systematically almost everywhere
1	Sufficient rule and dispositive and well applied systematically (complete and well-adapted)
N/A	Not Applicable

Table 3.4 - The scale of applicability levels for organizational policies

To apply this step to a case study, this list will be taken and if other specific vulnerabilities for the case study exist, coming from a specific attribute on a component and it can present a source of vulnerability, such as an intelligent sensor with a Bluetooth option, a vulnerable communication protocol used, a vulnerable mark of products (they can be extracted from the CVE database), they will be added on the vulnerabilities list to the corresponding category. For each organizational policy, the applicability level will be determined. These policies

and their applicability levels will be considered vulnerabilities for the next section of generating the attack scenarios. For example, the beer production system, on the field level and the zone of physical equipment (sensors, valves), the policy of the access to this zone is secured with badges and keys is with an applicability level 3, the access with the keys is not well managed, and thus this policy will present a vulnerability on this zone.

Because a policy or a barrier can be applied on one or many zones, and in different ways, there is a relationship between the policy and the different zones at the previous level, the ICS levels were divided into different zones. In addition, a policy or a barrier might be applied in different ways with varied levels of applicability for different components from the same zone, implying that there is a relationship between the components and the policies.

The model of the vulnerabilities and their relationships with the components are represented in the UML diagram in Figure 3.8 by the two classes “Relation zone” and “relation comp”, which represent respectively the policies applied on each zone level with an applicability level, and the policies that can be applied on a component level with an applicability level. The “policies” class represents the list of policies from Table 3.3, and it is linked to the “Vulnerabilities” class, which represents the vulnerabilities from Table 3.3, because each policy might be a source of vulnerability if it is not applied correctly. The “Applicability level” class represents the possible levels of applicability from Table 3.4. The relationships between the classes “Zone” and “component” are represented by the link to the previous step of system modelling. When this step is applied to a case study, the list of policies is defined in Excel sheets, and the user can choose which ones are applied with an applicability level (the list is defined in an Excel sheet).

This step produces a list of existing vulnerabilities on the system to be analyzed, together with an applicability level for rules and supports for policies, if applicable. The sections that follow illustrate how the attacks scenarios are generated and presented in meta-models in order to create a generic catalog of cyberattacks, as well as how to automatically generate the attacks scenarios that exist on the investigated industrial system.

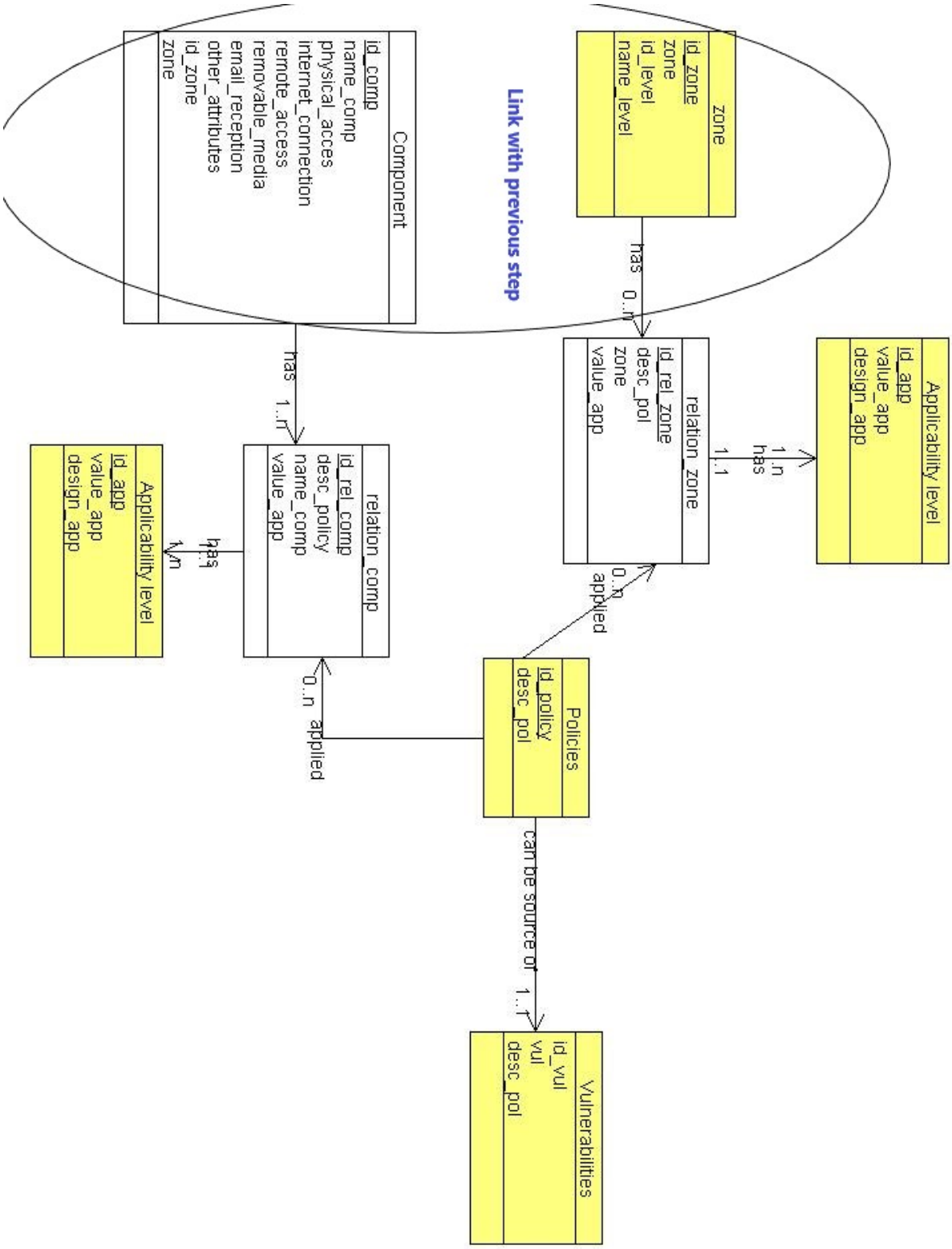

Figure 3.8 - The UML diagram describing the model of vulnerabilities

3.3.1. Searching for possible attacks

This section presents the meta-models of the attack scenarios for the Knowledge Base. In this section, we will detail how to generate the possible attack scenarios for an industrial system based on the output data from the previous steps, and how to combine them with the safety risks leading to the same physical undesirable event (from section 3.3.1.1). When the approach is applied to a real case study of an industrial system, these generic attack scenarios can be generated automatically, this generation will be presented in Section 3.3.2.2.

The main objective here is to identify the generic attacks that can be found on industrial systems worldwide, as well as how to generate them automatically. Usually, it is difficult when generating the scenarios of cyberattacks to cover all the scenarios, because the sources of attacks are not well-known by the analyst [12], there is also the 0-day vulnerability that can be a source of unknown attacks and no one knows about it except the attacker [79], and the attackers have various profiles (lucrative, ideological, state control, playful, technical, pathological, etc.) and different motivations (snooping, invasion, propaganda, sabotage, fraud, neutralization, etc.) [80]. In our proposed approach, the most frequent cyberattacks scenarios that can be encountered on industrial systems are generated. The generation of attacks scenarios is based on the data obtained from the previous steps (vulnerabilities and attributes of components) and a database of scenarios. The goal of this step is to offer a new model for describing the cyberattacks. Because, there are numerous scenarios with varied levels of vulnerability and different likelihoods of occurrence, the attacks scenarios will be generated on each ICS level and each zone.

3.3.2.1. Meta-model of attack scenarios

To carry out a cyberattack, the attacker must go through one or more phases to achieve its objective. A starting point for a cyberattack is the attacks surfaces presented on the components or zones of each industrial level. A successful attack with the objective of stealing or damaging the target system often consists of four phases [81]:

- Enter the system physically, remotely, through the internet or using software;

- Move inside the system to get unauthorized access to its different elements;
- Cause damage to software or hardware;
- Reach the objective of the attack (use information, retrieve data, etc.).

Based on the attributes of components specified previously, we choose for our approach five surfaces. These five surfaces can be sources of vulnerability leading to the execution of cyberattacks (Figure 3.9). Using these surfaces, an attacker can carry out all the four phases of its attack. The knowledge and comprehension of the attack surfaces aim in the step of risk treatment to limit the exposition to risks [82]:

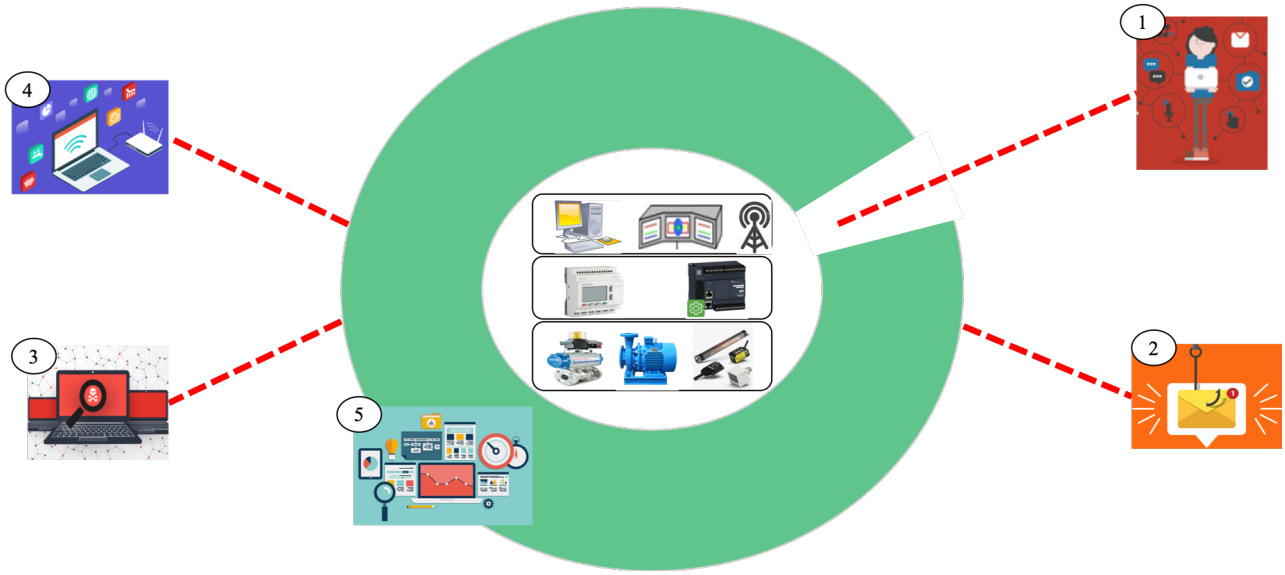

Figure 3.9 - The possible surfaces to execute an attack

1- **Physical access:** Using physical access, if the applied policies on the physical access are vulnerable, an attacker can gain unauthorized access to perform its attack.

2- **Email reception**: if components from various ICS levels receive emails from outside the industry, and there is a vulnerability in the filtering of the

received emails, an attacker using emails phishing can get unauthorized digital access or execute malware.

3- **Remote access**: if components from various ICS levels can be accessed remotely and there is a vulnerability in the management of remote accesses, an attacker can get unauthorized access and execute malware.

4- **Internet connection**: if components from different ICS levels are connected to the internet, and the internet access is vulnerable, an attacker acquire access to the system and carry out its attack.

5- **Software** implemented on components at different ICS levels can be a source of vulnerability for launching an attack, particularly if the software has a security flaw and is not up to date.

The attacks and cybersecurity risks targeting the ICS systems can be categorized in three main aspects as:

- Attacks on hardware;
- Attacks on software,
- Attacks on communication.

These aspects are taken into consideration because ICS systems, as described in Chapter 1, are made up of software packages that run on the hardware, and they are carried out via specific software services, and they are implemented by new communication technologies [83]. At least, one of these types of cyberattacks can affect the entire ICS system and pose very serious risks. These types of attacks are listed below, along with the many attack surfaces that lead to each type:

- Attack on hardware: The most important issue with this type of attack is through unauthorized physical access to the location of the hardware (physical equipment), or the attacker after the physical access to a station, for example, can acquire unauthorized digital access, and can quickly do harm to the operational procedure. This type of attack can occur through the surface attack of the physical access.

- Attack on software: This type of attack can be carried out in a variety of ways, such as through an implemented software vulnerability or a code

source that can be exploited for malicious purposes, or through the Buffer Overflow vulnerability during data transfer in the network traffic applications, or through SQL injection vulnerabilities, or through Cross-Site Scripting vulnerabilities. This type of attack can occur by having unauthorized access to one of the attack surfaces of email reception, connection to the internet, remote access, and software. An attacker on hardware can lead to an attack on software.

- Attack on communication: this type of attack usually occurs through the attack surfaces of the internet connection and remote access, such as an attacker can send malicious code to capture data through the existence of unnecessary ports and services, or an attacker can through a communication protocol with lack of encryption intercept the exchanging data. An attack on communication can serve as starting point for an attack on software.

There are several possible ways and steps to execute all these types of attacks on an ICS system and gain unauthorized digital or physical access through the different attack surfaces outlined above. These steps and ways are presented in the catalog of attacks scenarios, which is presented and generated afterward.

In the following section, the way for generating the attack scenarios is provided. The scenarios are depicted in meta-models; the meta-model contains the attack surface that exist on each zone of ICS level, as well as the different steps to execute an attack through this surface. The output of this section is a catalog of cyberattack scenarios that could occur on any industrial site, which will be used to apply to any industrial case study. Figure 3.10 presents and explains this meta-model.

This schema represents the sequence of events involved in carrying out an attack (red block). For each zone of ICS levels (grey block), each attack surface from the five defined above will be considered (if exists) in order to identify the possible attacks scenarios, and so on, to generate the attack scenarios that can occur on all zones and from all the attacks surfaces.

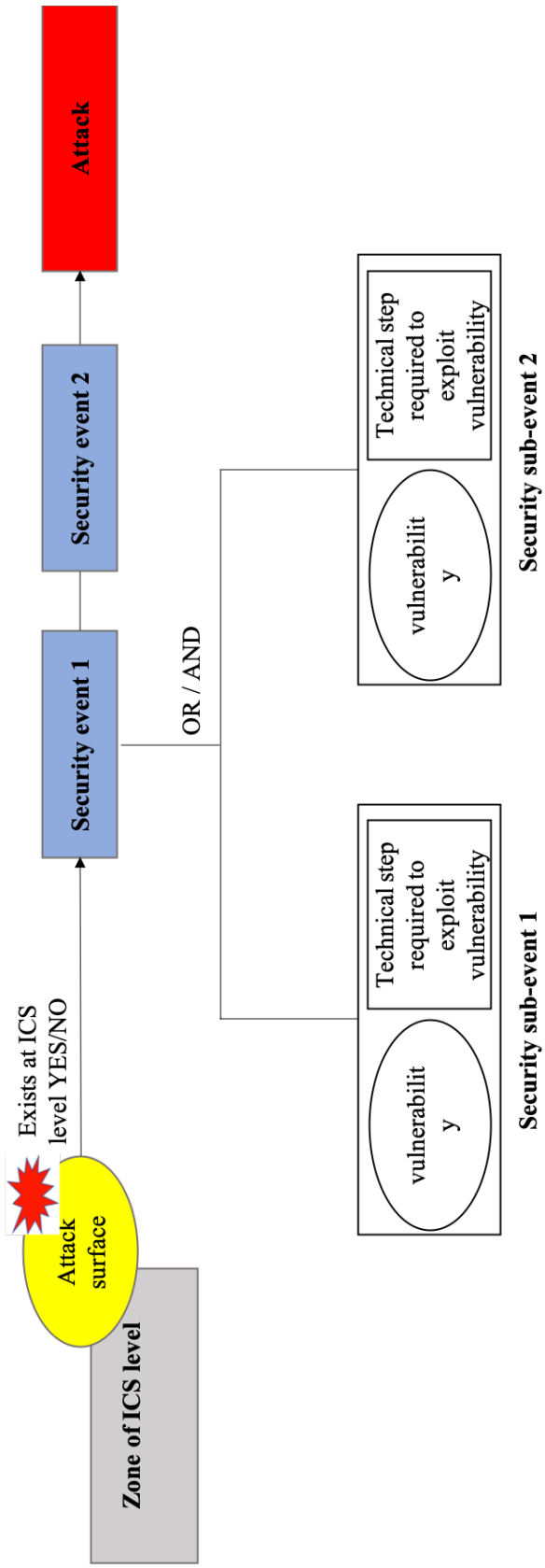

Figure 3.10 - The meta-model representing the sequences of an attack scenario

- During the execution of an attack, one or more sequence of security events may occur. The security event can occur as a result of the occurrence of one or more security sub-events connected by the gates OR/AND, or it can simply occur as an initiating event of the attack or a complimentary event.

- The security sub-event in this meta-model is a combination of two criteria: Vulnerability (organizational policy applied with applicability levels from the previous section) and the technical step required by the attacker in order to exploit the vulnerability, the technical step aims to demonstrate the required level of expertise or difficulty to exploit an existing vulnerability. Table 3.5 shows a qualitative scale for the different levels of difficulty of exploiting a vulnerability [84]. These values of level will be combined with the applicability levels in order to evaluate the likelihood of occurrence of security and sub security events and attacks afterward.

Qualitative scale	Difficulty level	Designation
Technical difficulty to exploit a vulnerability	1	**Trivial (T):** Little technical skill required
	2	**Moderate (M):** Average cyber hacking skills required
	3	**Difficult (D):** Demands a high degree of technical expertise
	4	**Very Difficult (VD):** Beyond the known capability of today's best hackers

Table 3.5 - The qualitative scale to characterize the difficulty of exploiting a vulnerability

Based on this meta-model, for each attack surface and each zone of ICS levels, the generic attacks scenarios are generated and presented in **Annex A.** To ensure that all the known attack scenarios are taken into consideration through the five attack surfaces, our research was based on the MITRE ATTACK framework,

which is a curated knowledge base and model for cyberattack (lifecycle of an attack) and attacker behaviors [85]. All of these scenarios will be used as a guide and catalog to apply our approach to a case study, taking into consideration whatever vulnerabilities may exist on the investigated system, as well as whether there are any other attacks coming from specific vulnerabilities.

Figure 3.11 represents the UML diagram for the step of searching the possible attacks, it aids in the creation of a database for all the attacks scenarios generated in the meta-models in **Annex A,** as well as the definition of input and output data to automatically generate these attacks scenarios for a case study in the following section. The different colors of classes in the UML diagram will be also employed in the following step of the automatic generation of attack scenarios in the next section. The yellow classes show the different relationships between the security and sub security events, as well as the occurrence of attacks for all the attacks surfaces and for all zones obtained from the meta-model presented in Figure 3.10. In general, the data inn the yellow classes represent the generic data for all the industrial systems. The link with previous steps is by taking the policies applied to components or zones to be connected to the technical step. In this step, the policies applied to zone and components with different applicability levels (if any) are consolidated into a single class called "zone`-comp". The remaining classes (green and orange) represent data related to the case study from the investigated system (explained in detail in the following part of the automatic generation).

3.3.2.2. Algorithm for the automatic generation of attack scenarios

The main objective of the automatic generation of attack scenarios is to make the step of searching for the possible attack scenario easier, when applying the proposed approach to a case study, especially for users who are not experts in the domain of cybersecurity. This generation makes it to apply the analysis process with a sufficient level of detail for the attack's scenarios while keeping the risk analysis complexity and time cost under control. To carry out this step, some input data needed from the KB is required in order to run an algorithm and obtain the possible attack scenarios as an output.

There are two types of input data for the process of searching the possible attacks and its UML diagram:

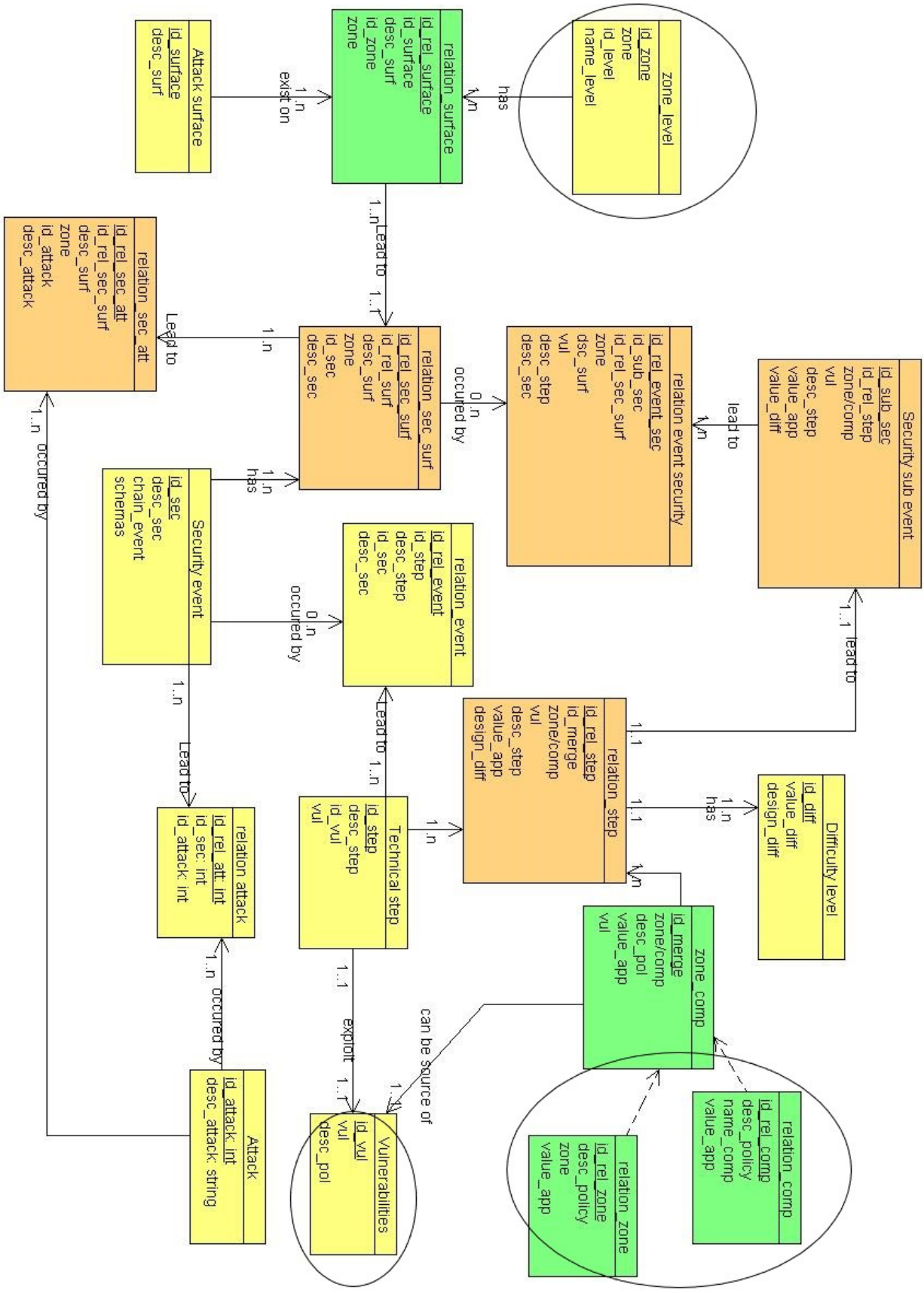

Figure 3.11 - The UML diagram of attacks scenarios generation

- The data of meta-models, which are fixed data and identical across all the cases studied (**yellow classes** in the UML diagram in Figure 3.11). The following data is included:

  - The different zones of ICS levels, that are presented in the section of system modeling (Physical components level, PLC zone, Programming and supervision zone, Supervision stations zone, and Computer stations zone).

  - The list of policies defined in the section of vulnerabilities, as well as the list of vulnerabilities that relate to the policies.

  - The different attack surfaces: Physical access, remote access, internet connection, an email reception, and software.

  - All the different sequences of security events and schemas from the generated attack scenarios for each zone and each attack surface. Each object of security event has a description (Unauthorized physical access…), a chain number, a schema number, as well as the zone and attack surface.

    - The chain number represents the sequence of different security events in an attack scenario which can have one or more security events.
    - The schema number represents the different scenarios to execute an attack on an ICS level via an attack surface.

    For example: Taking the attack scenario in Figure 4 from Annex A, in Table 3.6, the different sequences of security events are provided, and so on for all the attack scenarios generated.

  - The sub security events are represented by a combination of the technical step and the vulnerability exploited in all the different above-mentioned attacks scenarios. An example from Figure 4, the technical step of connecting unauthorized equipment by exploiting the vulnerability that there is no management for the use of removable media, and so on, in order to illustrate all the possible combinations.

- The relationships between the security and the sub security events show which combinations of technical steps and vulnerabilities cause whatever security event to occur.

- The list of attacks that can be carried out at the end of each of the above-mentioned attack scenario above (Disconnection of equipment, Modification of configuration, etc.).

- The connections between the security events that lead to the occurrence of the attack. All the possible ways to carry out the attack from the attack's scenarios provided above are listed.

Description	schema	Chain	Zone	Attack surface
Unauthorized physical access	1	1	Stations zone	Physical access
Unauthorized access to authentication data	1	2	Stations zone	Physical access
Unauthorized digital access to stations	1	3	Stations zone	Physical access
Unauthorized physical access	2	1	Stations zone	Physical access
Removable media with malicious content	2	2	Stations zone	Physical access
Malware execution	2	3	Stations zone	Physical access

Table 3.6 - Example of some input data for security events

- The second type of data is that which the user must enter when applying the risk analysis approach. The user must fill out for the step of generating the attacks scenarios these following data in an Excel file according to the case study (**green classes** in the UML diagram in Figure 3.11):
    - The policies that are applied at each zone of ICS level (from a predefined list), or at each component with its own level of applicability (the step of searching the vulnerabilities).

    - The attacks surface that exist at each zone of ICS level (the list of zones and attack surfaces are predefined in the Excel file). Therefore, even if the users are cybersecurity specialists, they can easily implement this technique.

These two types of input data are converted into data interchange format files in order to use them in the developed Java code to automatically output the existing possible attack scenarios in the same format as the input data. To validate the developed code with the input data of metamodel data and the case study data, we used a case study of a polymerization system from INERIS to fill the data needed for the input data, the policies applied on each zone, and the existing attack surface. As output (**orange classes** from the diagram in Figure 3.11) are the existing attacks scenarios on this case study. For example, here the programming and configuration stations do not receive emails from outside the industry, thus there are no attack scenarios through the email receiving attack surface. The output is all the sequences of security events for each zone and each attack surface, as well as all the attacks that can occur through these sequences of security events on this case study with all the possible combinations between technical steps and the exploited vulnerabilities (sub security events) for each security event at each zone and attack surface.

Till this section of the approach, the undesirable events that can occur on an industrial site are listed with the failure modes that represent the safety risks, and the list of cyberattacks that can occur on an industrial site is generated. In the following chapter, the procedures to combine the safety risks with the cybersecurity risks represented by the attacks generated, leading to the occurrence of the same undesirable events, will be described with the steps of evaluating and treating the combined risks.

3.4. Discussion and Conclusion

A model-based risk analysis approach is proposed to include the safety and cybersecurity risks in the same analysis process for industrial systems. Its process differs from that of other existing approaches, in the way for generating the list of vulnerabilities and the attack scenarios. The attack scenarios are generated in meta-models and automatically when applying the approach to a case study. Different data is required and collected from different steps in order to properly complete the analysis process and the automatic generation of attacks. Therefore, seven steps are proposed, which are divided into three parts:

- Data collection from the industrial installation: Listing the physical undesirable events; Modeling the system architecture; Researching of vulnerabilities based on the implemented organizational policies and security barriers.

- Search for possible attacks: Generating the attack scenarios in meta-models and automatically using an algorithm.

- Combination of risks: Combining the safety and cybersecurity risks that lead to the occurrence of the same undesirable events; Evaluating the combined risks; Treating the combined risks.

We described in this chapter the first two sections of our proposed risk analysis approach. To implement these steps to a case study, the analyst will collect data first from the industrial installation, and the step of automatically generating the attack scenarios will be computed aided and based on a KB and will be done using a computer code. Our approach provides a comprehensive risk analysis for industrial systems, as well as a new and simple manner of covering all the safety and cybersecurity issues that might affect the industrial installations and infrastructure. Thanks to the hierarchical levels of an industrial system, in our approach, we finished by identifying the different attacks scenarios for each level and component.

The application of our approach is based on generated guides, meta-models, and automatic attack scenarios generation in order to assist users in quickly apply

it in an easy way on a case study with a sufficient level of detail. In addition, the results of the application can be saved as historical data for future risk analysis. We present in the next chapter the steps of combining the safety and cybersecurity risks, evaluating the combined risks (likelihoods and gravities) to estimate their levels of criticalities on an industrial site, and treating them in order to minimize their criticalities.

Chapter 4: The combination of safety and cybersecurity risks with their evaluation and level computation

In this chapter, we present how to combine the safety and cybersecurity risks in the same analysis. Then, using a double quotation comprising the likelihood of safety and cybersecurity events, we present how to evaluate the likelihood of occurrence for each type of events, as well as the likelihood of combined risks. In the last section of this chapter, we present how to treat the combined risks in order to reduce their levels of criticality on an industrial site, by proposing safety and cybersecurity barriers and measures.

4.1. Introduction

The analysis of safety and cybersecurity risks jointly in the same process has become increasingly relevant for industrial systems as the attacks surface on the industrial installation has grown. Furthermore, in risk analysis, evaluating the likelihood of occurrence of safety or security events represents is a key step in determining whether a risk is acceptable or not for an industrial site. In this chapter, the first half will focus on how to combine the safety and cybersecurity risks in the same analysis and graph, which will be referred to as the cyber Bow-Tie. The second part evaluates the likelihood of occurrence of safety/cybersecurity risk scenarios based on the cyber Bow-Tie generated from the proposed approach. Depending on the available data, the analysis of likelihood can be quantitative or qualitative; a qualitative analysis is based on expert elicitations, while a quantitative analysis is based on historical data. Because it is difficult to quantify the likelihood of occurrence of an attack or a hazardous situation in this work, qualitative scales are used here. This evaluation will be carried out using a methodology that employs a double quotation of likelihoods values to represent safety and cybersecurity events respectively.

The last step of our proposed approach is to treat the unacceptable risks and reduce their criticalities. This step seeks to propose new effective safety and cybersecurity measures and barriers. This step is important in any risk analysis since it tries to prevent the future risks to happen and to protect industrial sites. This chapter finishes with a discussion of the steps covered here, as well as a conclusion.

4.2. Combination of safety and cybersecurity risks

This section presents the meta-model of the cyber Bow-Tie for combining the safety and cybersecurity risks. As previously explained in Section 3.3.1.1, the initiating events of the physical undesirable events might be occurred from a source of hazard situations, or a source of cyberattacks, or a combination of the two. Our approach aims to combine the safety and cybersecurity to provide a holistic representation of risk scenarios by mapping, on the same schemas, the safety ad cybersecurity events that can lead to the same undesirable events. This combination and the analysis of these two types of risks together will help to

understand how attackers can take advantage of the system weakness and create damages in addition to the hazardous situations. In this section, the links between safety and cybersecurity risks are given and merged in a single graph. The processes of evaluating the likelihoods of occurrence of the combined risks, as well as how to treat them, will be detailed in the next chapter.

By including the cyberattacks, the combination of safety and cybersecurity risks is based on the classical bow-tie concept. The "cyber Bow-tie" schema for describing the safety and cybersecurity events is demonstrated by the following meta-model in Figure 4.1.

The cyberattacks from the meta-models created before in the process of generating the attack scenarios are joined with the safety events found in the steps of looking for the undesirable events, resulting in the occurrence of the same initiating event of an undesirable event. An initiating event might occur purely form safety source, or purely from cybersecurity source, or from a mix of the two. On this cyber Bow-tie, the security and safety barriers that are implemented and exist on an industrial system can also be exhibited here, and their application can lead to a variety of undesirable events. The dysfunction of these barriers can be caused by one or more attacks, or by one or more hazardous situations, and are considered in our approach as secondary events. Once, the cybersecurity and safety events have been aggregated and integrating into a single graph, their likelihoods of occurrence and severities may be evaluated and treated. The following sections will go over these two steps in detail.

4.3. Likelihood evaluation of combined risks

In this section, the way for evaluating and analyzing the likelihoods of occurrence for safety/cybersecurity risk scenarios is described. As we discussed in Chapter 1, there are distinctions between safety and cybersecurity terms. The sources of cybersecurity threats are not well-known; there can be a wide range of attack scenarios with a wide range of attacker behaviors and objectives, as well as a rapid shift in threats and vulnerabilities. Hazardous situations, on the other hand, are more well-known and accessible. Furthermore, in comparison to the likelihood of cause related to cybersecurity, the likelihood of a cause related to safety is quite low. Therefore, the evaluation of the likelihoods of safety and

cybersecurity events should be done separately, using different scales of likelihood for each.

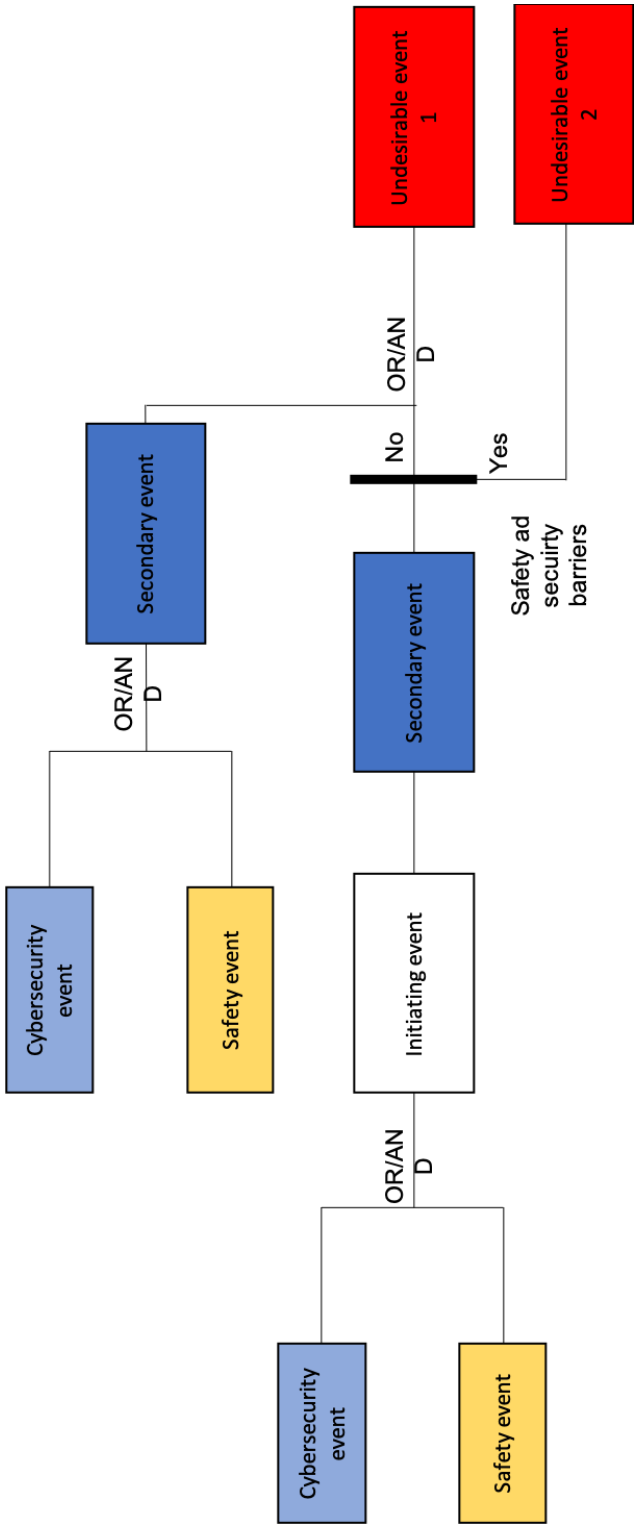

Figure 4.1 - The cyber bow-Tie to combine safety and cybersecurity risks

By altering the way to evaluate the likelihood of cybersecurity events, the qualitative likelihood evaluation methodology presented in [46] is applied to evaluate the likelihoods. This methodology employs a double quotation with two term likelihood portions, one for cybersecurity and the other for safety, as well as the concept of Minimal cut set MCs, which represents the smallest combination of safety and cybersecurity events that leads to the risk of undesirable events. The steps in this likelihood evaluation methodology are as follow: Determining the likelihoods of safety risk events separately from cybersecurity risk events; evaluating the likelihoods of cybersecurity risk events separately from safety risk events; determining the list of MCs; and finally calculating the likelihoods of each MC. The following sections go over each of these processes in depth.

4.3.1. Determining the likelihood of safety events

This section seeks to determine the likelihood of occurrence of each safety event from the cyber bow-tie shown in the previous section. The qualitative scale used to determine the values of likelihoods of occurrence is taken from the French ministerial order dated 29/09/2005 related to the risk evaluation, and is shown in Table 4.1.

Qualitative scale	Likelihood level for safety	Designation
Likelihood	N/A	**Not applicable:** The event is purely related to cybersecurity and not to safety
	E	**Very unlikely:** the event can be assumed to not occur in equipment service life
	D	**Unlikely:** it is possible that the event occurs in equipment service life
	C	**Moderate:** the event occurs sometimes in equipment service life
	B	**Likely:** the event occurs several times in equipment service life
	A	**Very likely:** the event can often occur in equipment service life

Table 4.1 - The scale to determine the likelihood of occurrence for safety events

The level "E" reflects the lowest level of likelihood, whereas the level "A" represents the highest level of the likelihood of occurrence of a safety event. The level "N/A" was introduced to the scale to indicate that the event is a cybersecurity event and not a safety event, and this level is used after for the combination of the likelihoods of safety and cybersecurity events. The values of likelihoods can be retrieved from the classical existing hazard study from the first step of searching for the undesirable events, or if it is not the case, the likelihoods are estimated by experts in the domain of safety and industrial installations using the scale indicated above.

4.3.2. Evaluating the likelihood of cybersecurity events

In this section, the likelihood of occurrence of attack related to cybersecurity events from the cyber Bow-tie on an industrial system is assessed. In the context of cybersecurity risk analysis, the likelihood of occurrence of an attack depends on the capability of an attacker to exploit a vulnerability or a group of vulnerabilities to carry out his or her attack and achieve its objective. Thus, the likelihood here is a function of two values: the level of vulnerability based on the applied organizational policies and the level of difficulty of an attacker to perform attack. In our work, to evaluate the likelihood of occurrence of an attack, we use the meta-model of an attack scenario illustrated in Section 3.3.2. in Figure 3.10, in order to take into consideration, the likelihoods of the different schemas to perform an attack. The processes to assess the likelihood of occurrence of an attack that can have scenarios (shown in meta-models) are the evaluation of the likelihood of security sub-evens, then of security events, and finally the likelihood of the attack. These steps are outlined below in detail:

- Step 1: The first step is to assess the likelihood of occurrence of the security sub-events represented by the combination of the vulnerability and the technical step required to exploit the vulnerability as presented in the meta-model of Figure 3.10. Therefore, the likelihood of a security sub-event is determined by taking into consideration the two different criteria presented as follow:

    - The vulnerability level: As previously said, if an organizational policy or a security barrier is not properly applied to an industrial

system, it might result in a vulnerability. Thus, the vulnerability level here is represented by the applicability level of the organizational policies and barriers. In Table 3.4, a scale for many levels of applicability of an organizational policy or a security barrier was provided. Using the example of the password generation on a computer station, if this generation proposes to generate passwords with four digits that are not strong passwords, this policy is assigned an applicability level of "3" (Rule and dispositive partially applied), and this station is considered vulnerable.

- The difficulty of technical step: An attacker must follow technical steps and have knowledge of the systems being attacker in order to exploit an existing vulnerability. To provide a level of difficulty of the technical step required, the scale from Table 3.5 is used [84].

The likelihood of occurrence of a security sub-event is calculated by combining the vulnerability level represented by the applicability level of organizational policies with the difficulty level of the technical step required by the attacker to exploit the vulnerability on the same scale. Table 4.2 shows the results of this combination.

Likelihood levels		**Technical step difficulty levels**			
		T	**M**	**D**	**VD**
Applicability levels of policies	**4**	4	4	3	2
	3	4	3	3	1
	2	3	2	2	1
	1	2	2	1	1

Table 4.2 - The combination of the criteria of vulnerability level and the difficulty level of technical step

These combined values are assigned to the designations presented in Table 4.3 in order to determine the likelihood of occurrence of a sub-security

event. The value "4" denotes the highest level of occurrence, and the industrial system is an easy target. While the value "1" represents the lowest level of occurrence and the industrial system is secured by effective security measures and barriers. The additional level "N/A" indicates that the event is not related to cybersecurity, but related to safety. The "N/A" level is used when combining the two values of likelihoods for safety and cybersecurity.

Qualitative scale	Likelihood level for cybersecurity	Designation
Likelihood	N/A	**Not applicable:** The event is purely related to safety and not to cybersecurity
	1	**Low:** the event is highly unlikely to occur, due to effective countermeasures applied
	2	**Moderate:** the event is possible to occur, with existing countermeasures applied
	3	**High:** the event is likely to occur, with limited countermeasures applied
	4	**Strong:** the event is almost certainly to occur, and the system is an easy target

Table 4.3 - scale to determine the likelihood of occurrence of cybersecurity events

An example of how to determine the likelihood of a security sub-event from an attack scenario depicted in the meta-model is presented. Based on the meta-model of Figure 4 (Annex A), the likelihood of occurrence of the security sub-event associated to the coupling of the vulnerability of "No management for the use of removable media" with the technical step of plugging a removable media with malicious content (See Figure 4.2). Let's assume there is a rule and restrictions against using the removable media on a computer station, but they are only partially enforced, therefore the level of applicability of this policy is "3". The attacker to exploit this vulnerability just needs to insert in a USB drive or other removable media containing malicious content, which requires some technical skills, thus, the level of difficulty of the technical step required is "2" with the

designation "T". The combination of these two values is "4" meaning likelihood of occurrence of this security sub-event is Strong.

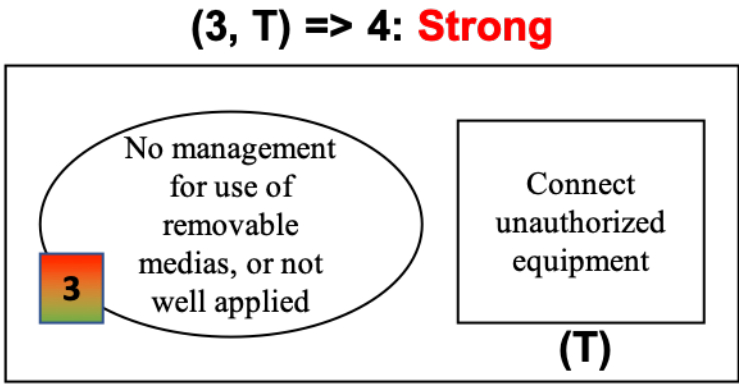

Figure 4.2 - An example of determining the likelihood of a security sub-event from an attack scenario

- Step 2: The second step is to assess the likelihood of occurrence of security events existing in an attack scenario represented by a meta-model. As previously stated, the security event can occur as a result of one or more security sub-events connected by OR/AND, or as a complementary event in a sequence to perform an attack. The different ways in which a security event can arise from security sub-events are depicted in Figure 4.3, as well as the likelihood of a security event arising dependent on the likelihood of the security sub-events arising.

  (a) A security event can occur from a single security sub-event with the same value of likelihood.

  (b) A security event can occur as a result of any of the many security sub-events connected by the gate OR. The maximum value of the likelihoods of the security sub-events is taken here and given to the security event.

  (c) A security event can occur as a result of many security sub-events connected by the gate AND. The minimum value of the likelihoods of the security sub-events is taken and given to the security event as shown in Figure 4.3.

If a security event does not occurr due to security sub-events, but it is a complimentary event of a sequence of events to perform an attack, such as the security event "Unauthorized digital access to station" in Figure 4 (Annex A), the likelihood of this security event is equal to the likelihood of occurrence of the previous security event. If the previous security event is one or more security events connected by the gate OR, such as the security events "Malware execution" in Figure 7 (Annex A), the maximum value of the likelihood of the security events is taken and given to the evaluated security event.

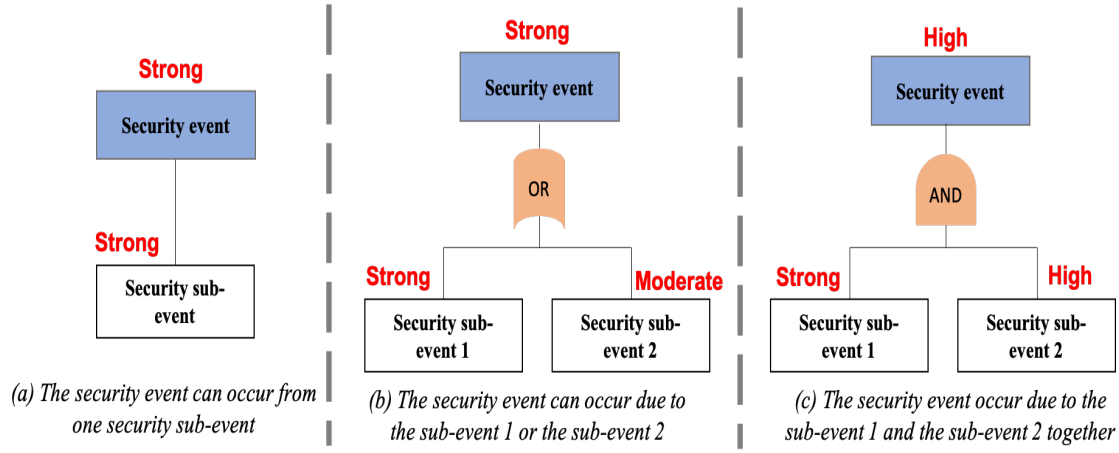

Figure 4.3 - The different ways for the occurrence of a security event with examples of likelihood values

If the security event is formed by one or more security sub-events and occurs in a sequence of events, as shown in Figure 4.4, the minimum value of likelihoods (the value in red in figure 4.4) is given to the security event evaluated.

- Step 3: The final step is to determine the likelihood of occurrence of an attack based on the value of the last security event in the attack scenario. If only a security event preceding the attack, the likelihood of the attack is equal to the likelihood of this security event. If several security events precede the attack and are connected by the gate OR (like the attack in

Figure 4 from Annex A), the likelihood of occurrence of the attack is the maximum value from the likelihoods of occurrence of the security events.

After these steps of evaluating the likelihoods, the likelihood of each attack scenario can be estimated. As we notice in the different attack scenarios, the same attack can occur owing to many attack scenarios. For these reasons, when combining the attacks with the hazardous situations in the same graph, to evaluate the likelihood of occurrence of an attack, the maximum value of likelihoods of the attacks from different scenarios is selected and used. In the next section, the combination of the likelihoods of safety and cybersecurity risks is provided with the notion of the MCs and the double quotation of likelihoods.

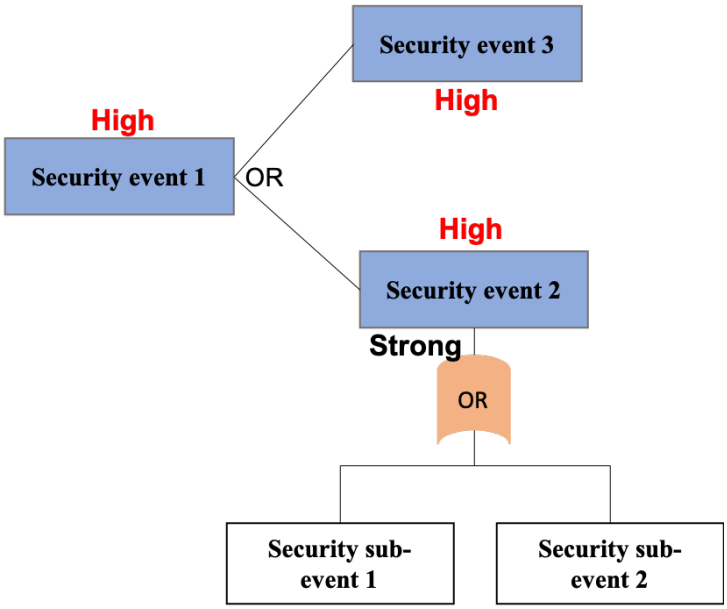

Figure 4.4 - The way to evaluate the likelihood of security event in an attack scenario

4.3.3. Determining the list of Minimal Cut sets

A Minimal Cut is represented by the smallest combination of events that produces the occurrence of the physical undesirable event. An MC set can contain one or several events, and it represents the different possibilities in which events, alone or in combination with others, cause the occurrence of the undesirable

physical event. In this work, the MCs are derived using rules of Boolean algebra [86]. Thus, each MC set is made up of AND gates that contain a set of basic events required to cause the top event [87], which is in our work, the undesirable event in the cyber Bow-Tie. There are three types of minimal cut sets, which are presented as follow:

- MCs are purely concerned with safety, and they contain a set of events that occurred only as a result of hazardous situations.

- MCs are purely related to cybersecurity, containing a set of events that occurred only as a result of cyberattacks.

- MCs contain a mix of both safety and cybersecurity events resulting from cyberattacks and potentially hazardous situations.

The relevance of having these different types of MCs is to find the weakness of the system analyzed, with a pure cybersecurity MC being a weak point due to the high likelihood of occurrence of cybersecurity causes [46]. This explanation stems from the difference between describing the likelihoods related to safety events and the likelihoods related to cybersecurity events. In the next section, the way for evaluating the likelihood for each MC, as well as the combination of the two values of likelihoods are presented.

4.3.4. Calculating the likelihoods of MCs

As previously stated, there is a difference between evaluating the likelihood of safety and cybersecurity events, the different ways for evaluating the likelihood were discussed in the sections above. For these reasons, a double quotation of likelihoods is used, with two different scales (L_s , L_f) representing respectively the different scales of the likelihood of cybersecurity and the likelihood of safety stated in Table 4.3 and Table 4.1. Each event is characterized by the couple (L_s , L_f). Therefore, a couple of likelihoods for the events purely connected to safety is ($N/A, L_f$); a couple of likelihoods for the events purely linked to cybersecurity is (L_s , N/A). While, the initiating and secondary events from the cyber Bow-Tie, which can be from safety and cybersecurity events, have this couple of likelihoods (L_s , L_f). Until now, the likelihoods of the input events, and

the initiating and secondary events (from the cyber Bow-tie) can be evaluated, and each event has its couple of likelihoods.

The likelihood of each MC is now calculated in order to assist decision-makers in proposing the right countermeasures and treating the MCs with the highest likelihood (in the next section of treating the combined risks). The AND gate must be solved to calculate the likelihood on an MC, and the minimal rule is used to solve the AND gate. The AND gate indicates that if all of its input events occur, the output of undesirable events occur. If an MC comprises *n* input events EV_i , i = 1, …, n, the output likelihood is calculated using the following equation [88] [89]:

$$L\ (AND_{out}) = min\ [L\ (EV_i)]$$

$$= (min\ [L_s\ (EV_i)],\ min\ [L_f\ (EV_i)])$$

$$= (min\ [L_s\ (EV_1),\ \ldots,\ L_s\ (EV_n)],\ min\ [L_f\ (EV_1),\ \ldots,\ L_f\ (EV_n)])$$

Where $L\ (EV_1),\ \ldots,\ L\ (EV_n)$ represent the likelihood of occurrence of the input events of the MC. Finally, in order to establish the overall likelihood of an MC, the two determined likelihoods for safety and cybersecurity are merged together in the same scale presented in Table 4.4 for each MC. The level "L" represents the lowest level of likelihood of occurrence, while the level "VH" represents the highest level of likelihood.

Likelihood levels		**Likelihood of safety events**					
		E	**D**	**C**	**B**	**A**	**N/A**
Likelihood of security events	**N/A**	VL	L	M	H	VH	
	4	VL	L	M	H	VH	VH
	3	VL	L	M	H	H	H
	2	VL	L	M	M	M	H
	1	VL	L	L	L	L	M
VL: Very Low; **L**: Low; **M**: Moderate; **H**: High; **VH**: Very High							

Table 4.4 - The overall combined likelihood scale

Figure 4.5 shows an example of how to define the list of MCs and how to calculate their likelihoods of occurrence. Two MCs can be determined from Figure 4.5, each of which can lead to the occurrence of an undesirable event. The first set of MC1 includes the following three events: Cybersecurity 1, Safety1, and Safety 2. The second set of MC2 includes three more events relating to safety and cybersecurity: Cybersecuity2, Safety 1, and Safety 2. Using the proposed approach for evaluating the likelihood of occurrence for safety and cybersecurity events, each event is evaluated with its likelihood based on the double quotation and the scales from tables 4.1 and 4.3, as shown in Figure 4.5. These likelihoods are then propagated across the MCs. Therefore, the undesirable event has two values of likelihoods through each MC. From MC1, its likelihood is (3, C), with a "Moderate" value (from Table 4.5), based on the minimal value of likelihood of safety and cybersecurity events respectively. The same for MC2, its likelihood of occurrence is (2, C), with a "Moderate" value. Once the likelihoods of occurrence of undesirable events are prepared through each MC, together with their levels of severity (from Section 3.3.1.1), the risks associated with the undesirable events can be treated. The following section describes the step of treating the risks.

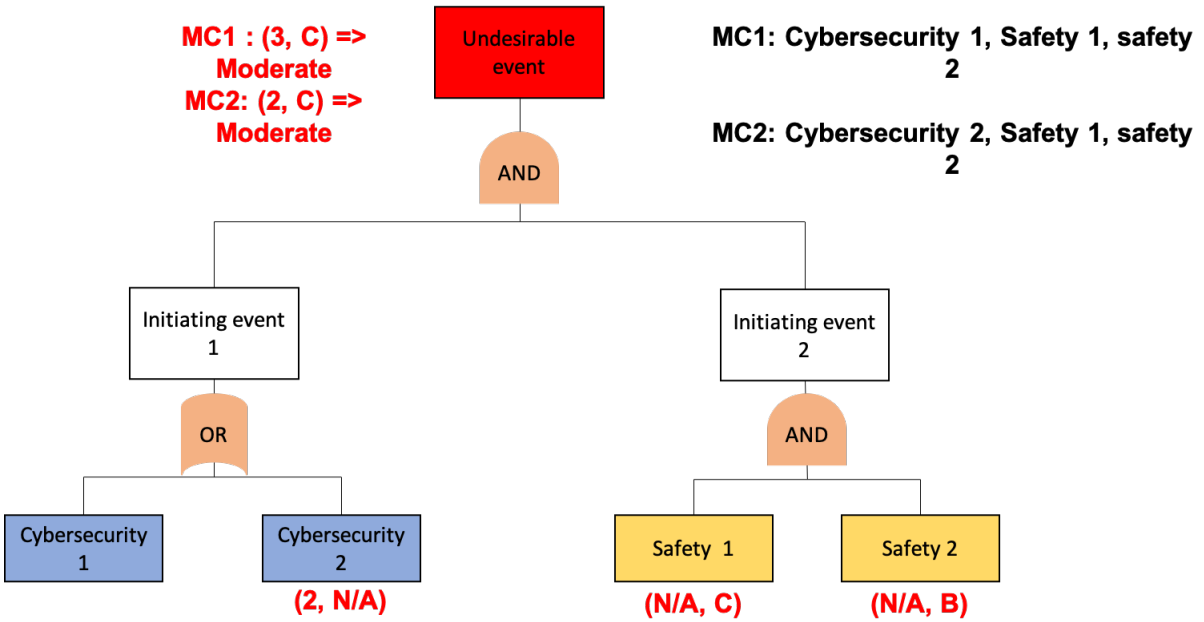

Figure 4.5 - An example of how listing the MCs and calculating their likelihoods

4.4. Treatment of combined risks

At this point, the list of risks associated with the occurrence of physical undesirable events has been established. In this section, the level of these risks is calculated in order to determine which risks are acceptable or not, and then the unacceptable risks are treated in order to reduce their levels of criticality by proposing effective safety and cybersecurity measures. This step is critical in the risk analysis process because it tries to avoid the risks from occurring again, or, if they do, to mitigate their impacts and protect more the industrial system more.

To associate and estimate qualitatively a level for a risk associated with a physical undesirable event, a couple of likelihood values (from the previous section) and the level of severity (from Section 3.3.1.1) are used. Because we used the concept of MCs in our approach, and because many sequences of events might lead to the occurrence of undesirable events, a level of risk is estimated through the likelihood of each MC. The decision-risk matrix is the scale that is used to determine whether the risk is acceptable or not, depending on the likelihood range and severity class shown in Table 4.5 (it can be called also *Heat Map* [1]). The risk matrix employed in this step is used by the French authorities in order to determine if the risk posed by a facility in a given environment is acceptable. In this risk matrix, there are three levels of acceptability:

- Acceptable risk: A risk is acceptable when its level is low and the likelihood-severity relationship leads to an acceptable level of criticality.

- Risk to be reduced: The risks are reduced by implementing a set of policies and procedures (explained after in the phase of treating the risk).

- Unacceptable risk: An unacceptable risk might have serious consequences on the industrial installation (unavailability, modification of the infrastructure).

Severity	Likelihood				
	Very Low VL	**Low** L	**Moderate** M	**High** H	**Very High** VH
Disastrous					
Catastrophic					
Important					
Serious					
Moderate					

Acceptable	Risk to be reduced	Unacceptable

Table 4.5 - The decision-risk matrix

Following, we will look at how to treat the risks by lowering their levels of criticality and reducing the vulnerabilities in the industrial system. Usually, the risks that need to be reduced and the unacceptable ones are treated. This is accomplished by proposing and implementing measures that interact and influence the likelihood of occurrence and the severity. The choice between the different measures relies on the level of the risk and the strategy of the industrial system, which should aim to minimize the costs while maximizing the efficiency. There are numerous types of measures that can be distinguished: Technical measures, such as antivirus software, firewalls; organizational measures, such as the procedure to generate passwords, and so on; Measures related to human skills and behavior, such as the awareness of how to interact with emails, and so on. These measures can be also classified based on their potential to influence to the occurrence of the undesirable event being addressed:

- A preventative measure that interacts with the value of likelihood to prevent the occurrence of the undesirable event. Anti-virus, Firewall, secured architecture, and so on are some examples.

- A risk-reduction strategy that involves detecting the occurrence of abnormal events as soon as they occur. Intrusion detector, alarm, and other similar devices are examples.
- A protection measure that can reduce the impact of an occurred undesirable event. For instance, data backup, redundancy of a component, and so on.

There are several lists and standards of generic measures that can be used in the risk analysis. These measures are classified by types and themes (for safety, or cybersecurity), and the choice of measures, as previously said, is based on the risk level and the strategy of the industrial site. The following are some standards for measures:

- The standard ISO 27002 (ISO/IEC 2013) [90];
- The guide ANSSI, dedicated to ICS [91] [92] [93];
- The guide NIST SP800-53 (NIST 2013) [94];
- The standard IEC 62443-2-5 (ISA 2018), dedicated to ICS [95] ;
- The guide NIST SP 800-82, dedicated to ICS [96].

Furthermore, in this phase, the combined risks from safety events and cybersecurity events are treated, and the interdependencies between safety and cybersecurity measures should be taken into consideration. Despite the mutual reinforcing of safety and cybersecurity measures [12], they can weaken each other and cause conflicts, and a cybersecurity measure can decrease the safety of the system and vice versa. For instance, consider a door with limited access for a production process in an industrial installation [97] [98]: for cybersecurity, the door must be locked and accessible with keys and badges to prevent unauthorized access, while for safety, the door must be always unlocked to respond in the case of a fire caused by a hazardous situation. Thus, during risk analysis, a safety or cybersecurity measure should be effective in protecting the industrial system from potentially hazardous situations or cyberattacks, without conflicting with safety or cybersecurity.

In addition, it is preferable that the analyst, in this step, lists the causes (safety and cybersecurity events) leading to the occurrence of the undesirable event and selects the best measures to make the process of selecting the proper measures

easier. After the step of treating the combined risks, which includes the proposition and the implementation of new measures, the initial architecture of the industrial system can be adjusted in accordance with the proposed safety and cybersecurity measures. Therefore, the new architecture must be processed using the overall proposed approach in order to assess the impacts of the changes and the new risks analysis results (arrow linked between the step of listing the undesirable events and the step of risk treatment in Figure 3.2). In the following section, a discussion of the steps described in this chapter is offered, followed by a conclusion.

4.5. Discussion and conclusion

The use of technology in critical industrial systems exposes the safety of the system to cybersecurity events related to cyberattacks. The need of combining the safety and cybersecurity events in the same risk analysis is highlighted here, with as is the requirement for a thorough and effective safety risk analysis. Currently, the majority of the existing approaches for industrial risk analysis neglect the risks related to the cybersecurity. As a result, this chapter shows how to combine these two types of risks in the same analysis using the proposed approach. The Bow-Tie analysis is used to display and analyze the safety risks. The cyberattacks generated with a new concept in the previous chapter are combined and added to the Bow-Tie with the safety risks, resulting in the occurrence of the same physical undesirable events. The “cyber Bow-Tie” meta-model was created to include the cyberattacks into the traditional bow-Tie.

In addition, in this chapter, the likelihood evaluation of the combined risks is explained. Quantifying the likelihoods of occurrence of cyberattacks is difficult, and there are differences between the types of likelihood for safety and cybersecurity events. For these reasons, two different scales for likelihood are recommended to describe respectively the likelihoods of cybersecurity and safety events. The concept of MC is used in order to illustrate the different sequences of events with different likelihood scales. Thus, there are MCs that are purely concerned with safety, cybersecurity, or both. To assess the likelihood of each MC, a qualitative mathematical equation is used.

The outputs of the proposed approach show significant results in terms of depicting the various risk scenarios from different sources connected to safety or cybersecurity, as well as evaluating their likelihoods. The differentiation between the event sequences that lead to the occurrence of undesirable events aids in understanding the origins of risk and providing the right control measures, which is illustrated by the step of treating the combined risks in this chapter. The risk level is calculated from the likelihood of occurrence of each sequence of events (MCs) and the severity of the physical undesirable event that can occur through each sequence of events. There are three levels of risk: acceptable risk, risk to be reduced, unacceptable risk. In order to reduce the criticality of high-impact risks, effective safety and cybersecurity measures must be proposed, with the interdependencies between safety and cybersecurity measures taken into consideration. In the next chapter, the steps of the proposed approach are applied and illustrated to a chemical case study from INERIS.

Chapter 5: Application of the risk analysis approach integrating the safety and cybersecurity to a case study

In this chapter, we use a critical case study of a chemical reactor to demonstrate the proposed risk analysis approach in order to improve its ability to model the system architecture and assess the relevant safety and cybersecurity risks. The following steps of the proposed risk analysis process are applied and presented: the listing of undesirable events, the modeling of system architecture, the searching of vulnerabilities and different attacks scenarios from the generated meta-models, and the combining of the different risks with their evaluation and treatment.

5.1. Introduction

The contribution of this chapter is to demonstrate the steps of the proposed risk analysis approach in a real-world case study. This case study illustrates the critical implementation of a polymerization system in order to run chemical reactions. A cyberattack or a safety accident on the industrial process of this polymerization system could result in serious consequences risks, such as an explosion or a toxic release. Thus, the need of implementing a security policy appears in order to protect the industrial process from malicious and safety accidents, as well as to avoid the occurrence of important risks. Following that, it is critical to use a risk analysis approach that considers both the safety and cybersecurity risks.

For these reasons, we use this case study in order to demonstrate the applicability and the capability of the proposed approach to provide a comprehensive and simple joint safety and cybersecurity risk analysis. The first section of this chapter describes this case study, in order to understand the process of the polymerization system and to define all the ICS levels and components on each level, as well as their attributes. The application of the proposed approach is also provided, along with different steps. The next section discusses an improvement of the approach with some discussions. This chapter finishes with a conclusion.

5.2. Case study

5.2.1. Description of the case study

In this case study, the steps of the proposed for merging safety and cybersecurity in risk analysis are illustrated, which may be applied to any industrial site. The case study is about an industrial site of a polymerization process that aims to perform a high exothermic chemical reaction that can result in toxic releases into the atmosphere as the pressure of a reactor increases. Thus, the risks associated with this case study can have serious impacts and should be thoroughly investigated. The process of the chemical reaction is made up of two reactors, R1 and R2, that work in series and in the same way.

In order to accomplish the operations in the best conditions (pressure and temperature, a production system to feed the reactors, an agitator, a cleaning system with water circulation, a heating system, and a cooling system, interact between them. All the physical components of this system (sensors, valves, actuators, and so on) are controlled by two PLC1 and PLC2. These two reactors have of security features such as a rupture disk that restricts the increase of the pressure, an inhibitor injection system, and the valves closure system (responsible for the introduction of reactive and catalyst) that stop the reaction when the pressure threshold is exceeded. These barriers are controlled by a security PLC. The different data collected and measured during the industrial process, as well as the functioning of the valves and pumps, are elevated to the supervision level. At this level, there is a supervision station with a SCADA server, as well as computer stations that receive emails from outside the industry and are connected to the internet and may be accessed remotely. Figure 5.1 shows the architecture of the industrial system under investigation, and the structure of the polymerization process is detailed after.

An ICS system, as previously discussed in Chapter 1, is divided at three levels: Filed level, Control level, and supervision level. For this case study, these levels are shown along with their components.

- **Field level:**

Reactors feed:
Reactor R1: Injection of different reactive and catalyst to perform a chemical reaction, using:

- Sensors S1 and S2 to measure respectively the quantity of reactive and the catalyst to introduce them in R1.
- Regulation valve V1 and TOR valve VT2 to inject the reactive, and two others V2 and VT1 to inject the catalyst.

Reactor R2: Transfer of the product from R1 to R2 with a catalyst injection, using:

- Draw-off valve V4 and a pump P1 to extract the product from R1.
- Sensor S3 to measure the needed quantity of catalyst introduced in R2.
- Regulation valve V3 and TOR valve VT3 to inject the catalyst in R2.

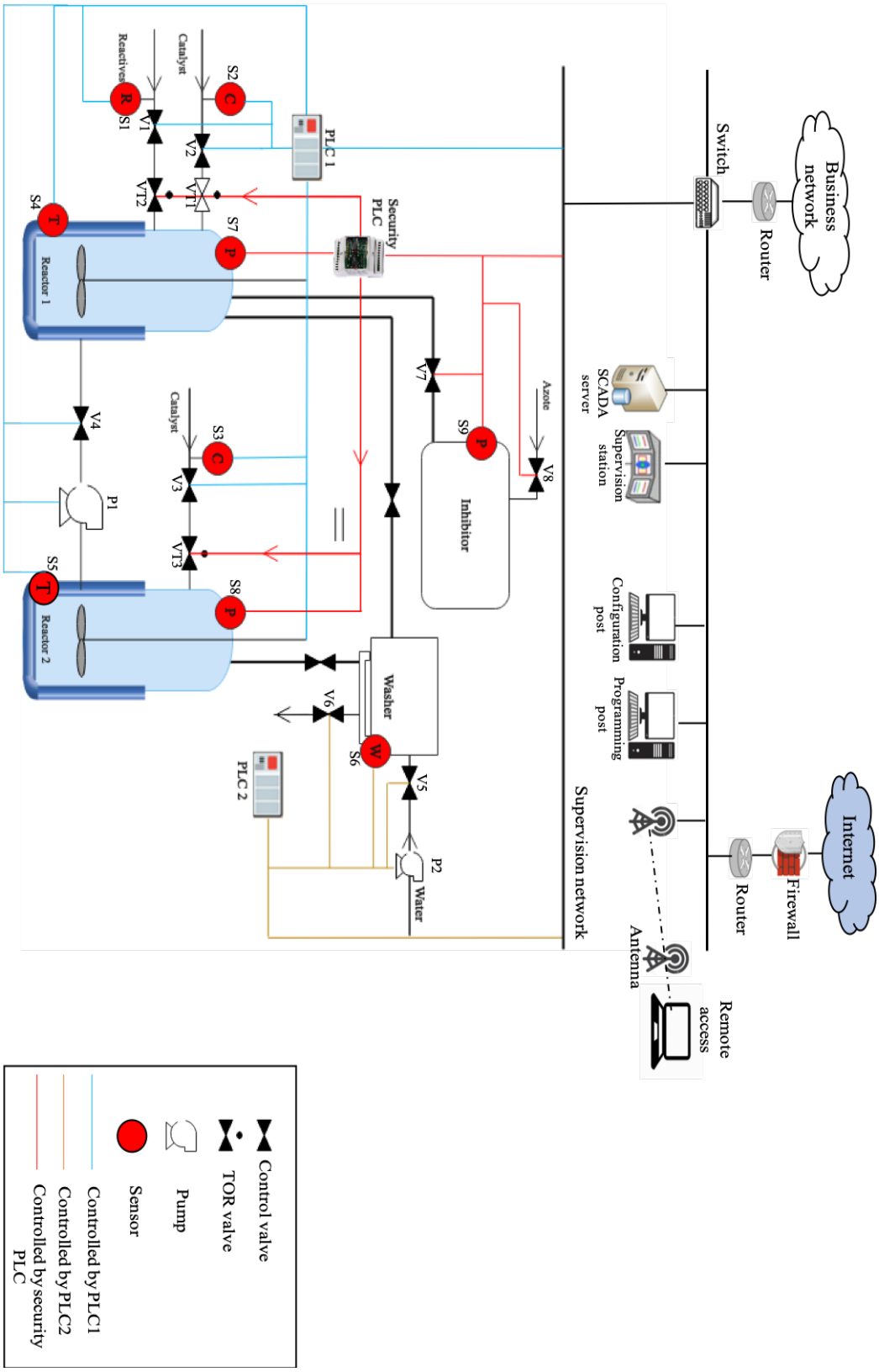

Figure 5.1 – The structure of the polymerization system of this case study

The feed is controlled by PLC1, the sensors (S1, S2, S3) send collected and measured data to the PLC1, which sends control signals to all the valves to introduce the reactive and the catalyst into the two reactors. V4 and P1 are controlled also by PLC1 to transfer the product.

Heating system on both reactors: Sensors S4 and S5 are used to measure the temperature of reactors. The collected data are controlled by PLC1, and in case of high temperature, PLC1 sends a signal to cool the reactors.

The Reflux management system aims to cool the reactors and reinject the condensates. In addition, an agitator in the two reactors with a backup power supply is controlled by PLC1.

The security barriers:
Rupture disk that limits the increase of the pressure in the reactor. The releases at the rupture disk pass through the cleaning system to prevent toxic dispersion.

Inhibitor system with nitrogen injection, composed of:

- Safety sensors S7 and S8 to measure the pressure respectively in the two reactors.
- Sensor S9 and valve V8 to measure the quantity of nitrogen and to inject it into the inhibitor system.
- Valve V7 to inject the inhibitor in the reactor whose pressure is increased.

When the pressure is increased, the security PLC sends a signal to the valves that control the introduction of reactive and catalyst, and they close and go into a rest mode. The security PLC is in charge of all the data collected as well as the actions of security barriers. On the field level, all the components can be accessed by internal employees (technicians, operators, etc.), as well as by service providers such as the maintenance company and visitors.

Washing system: This system is with water circulation for the two reactors, the data collected in this system are controlled by the PLC2:

- Valve V5 and pump P2 to inject the water into the cooling system.

- Sensor S6 to measure the quantity of water in the cooler and the waste concentration level to renew water.
- Purge valve V6 to empty the polluted water.

- **Control level:**

  - Two PLCs control the physical process (PLC1, PLC2).
  - A security PLC to control the security barriers.
  - Programming and configuration stations to develop the code source of PLCs and to configure them.

  The components, at this level, can be physically accessed by internal staff (technicians, operators, etc.), service providers, and visitors. The stations, at this level of control, may be accessed remotely, and are implemented by anti-virus software and a development tool. The control level is connected to the supervision level via a switch

- **Supervision level**

  At this level, there is a supervision station with a SCADA server and computer stations (configuration stations or the physical components and station connected to the SCADA server). Additionally, the components can be physically accessed by internal or external personnel. The computer stations are connected to the internet via a router through the use of a firewall, they can be accessed remotely, and receive emails from outside the industry. They are also implemented by software like an anti-virus and an operating system.

All ICS levels are interconnected, and a cyberattack on any level can increase the pressure of the reactors and compromise the safety of the overall industrial system. Therefore, for this case study, the combination of safety and cybersecurity risks should be taken into consideration.

5.2.2. Application of the proposed risk analysis approach

In this case study, the most likely undesirable scenario with the highest consequences due to the overpressure in reactors is examined for risk analysis. This scenario can result in many physical undesirable events with varying levels of severity, and it can occur as a result of cyberattacks or accidental situations. In the below section, we apply the different steps of the proposed approach to this case study.

5.2.2.1. Data collection

Step 1: Listing the physical undesirable events

For this case study, the current classical hazard study is a classical Bow-Tie developed by INERIS. The list of physical undesirable events, along with their initiating events and the sequence of secondary events, can be derived from this Bow-Tie. The existing security barriers for this case study are given in this Bow-Tie. For this case study, Figure 5.2 depicts the classical Bow-Tie. Due to the presence of the security barriers, three potential undesirable events outcomes with different levels of severity (scale in Table 3.1) can occur. If all goes well, the inhibitor system will limit and controls the overpressure in reactors. If not, the pressure in the reactors increases, the barrier of the rupture disk functions and opens to prevent the reactors from exploding, and the limited toxic release occurs due to the barrier of the washing system, whereas an important toxic release occurs if the washing system does not work properly. The physical undesirable events, along with their levels of severity are the following:

- UE 1: Explosion of one of the reactors, with a Disastrous severity level.
- UE 2: Limited toxic release in the atmosphere, with a Serious level.
- UE 3: Toxic release in the atmosphere, with a Catastrophic severity level.

The initial step of the occurrence of these undesirable events is the occurrence of one of the initiating events (Table 5.1) with the sequence of secondary events presented in Figure 5.2. We determined whether each initial event has a source of occurrence of safety or cybersecurity. EI1, EI2, EI4, and EI5 can all be triggered by safety or cybersecurity events, but EI3 is only triggered from safety events.

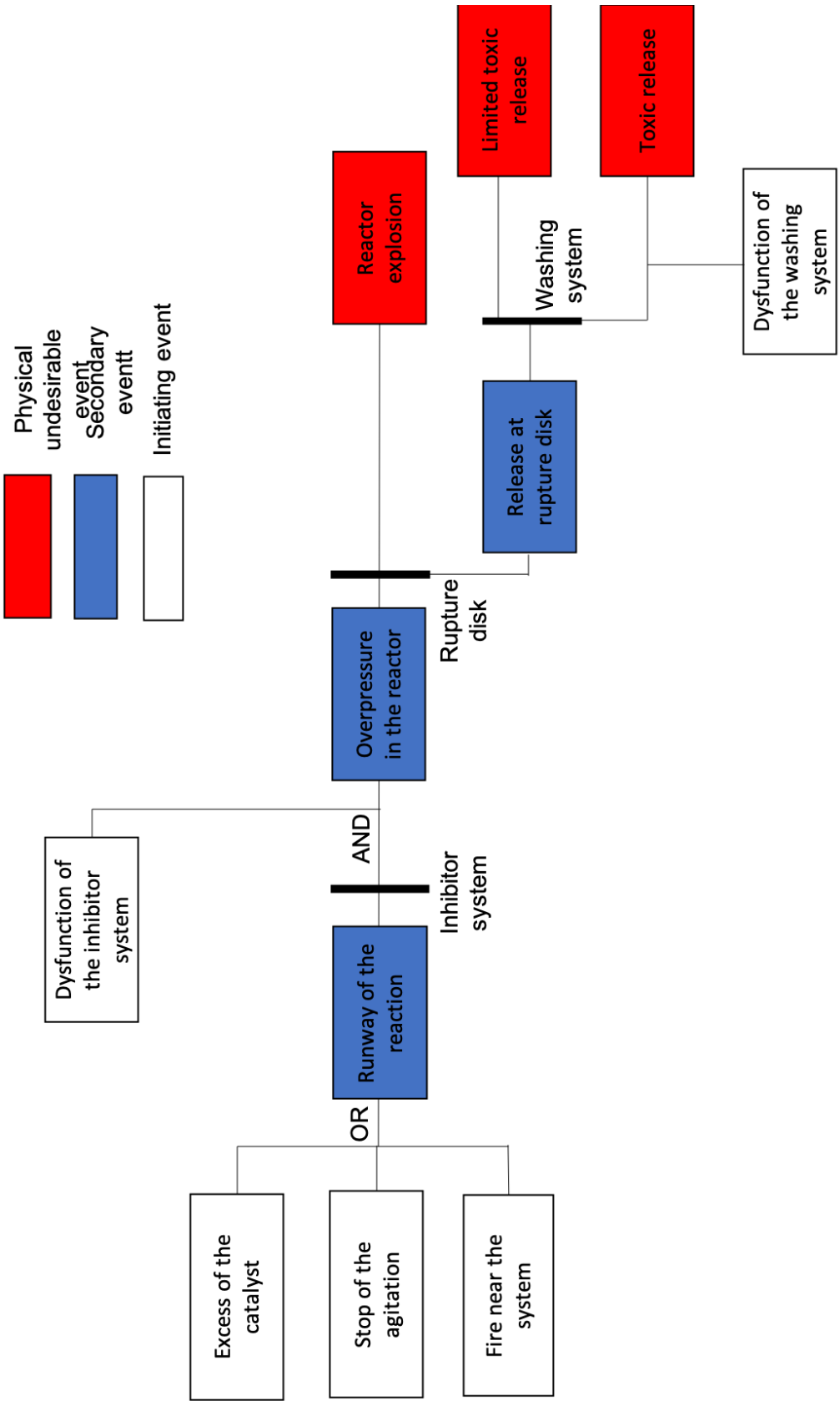

Figure 5.2 - The Bow-Tie of the polymerization system

Initiating events	Safety source	Cybersecurity source
Excess of catalyst (EI 1) related to the reactor's feeds	• A failure of one of sensors S2 or S3 responsible pf the measure of the quantity of catalyst in reactors (an error in the measured data by these sensors). • A failure in PLC1 managing the processes of the introduction of the catalyst leading to the modification of the function of valves responsible for the introduction of the catalyst. • A failure in one of the valves of the system of the introduction of the catalyst.	Yes
Stop of the agitation (EI 2) related to the agitation system	• A failure in PLC1 managing the process of the agitation, sending a command to stop the agitator. • Loss of power supply on the agitator.	Yes
Fire near the system (EI 3)	• Events due to environmental or human factors.	No
Dysfunction of the inhibitor system (EI 4) related to the security barrier of inhibitor system	• A failure in the security PLC (stop or fall-back position) leading to the dysfunction of V7 and V8 responsible for the injection of nitrogen, and the sensor S9 measuring the quantity of nitrogen. • A failure in valves or sensors of the inhibitor system.	Yes

Dysfunction of the washing machine (EI 5) related to the washing system	• A failure in PLC2 controlling the process of washing, leading to a dysfunction of V5 and V6 and P2. • A failure in sensors, or valves, pumps of the washing system. • Loss of power supply on the washing system.	Yes

Table 5.1 - The different initiating events of the case study

Step 2: System modelling

The components responsible for the occurrence of initiating events defined in Step 1 are modelled with a list of attributes. Therefore, a failure or a cyberattack on a modelled component can cause the occurrence of an initiating event. In this case study, according to the description, the failure of components from the heating system does not lead to the occurrence of an initiating event and then the runway of the reactor. Thus, these components are not modelled. The components are depicted with their attributes in Table 5.2. The components are organized by the zone of ICS levels.

Step 3: Searching for vulnerabilities

To look for the existing vulnerabilities, we choose some examples for this case study from the organisational policies illustrates in Table 3.3, and establish their levels of applicability defined in Table 3.4. In the step of evaluating the likelihoods for attack scenarios, the levels of applicability for the other policies will be offered. The different policies applied with their levels of applicability are presented in Table 5.3.

Component	Physical access	Internet connection	Remote access	Removable media	Email reception	Software
Field level: physical components zone						
S1, S2, V1, V2, VT1, VT2	Yes	No	No	No	No	No
V4, P1, S3, V3, VT3	Yes	No	No	No	No	No
S7, S8, S9, V8, V7	Yes	No	No	No	No	No
V5, P2, S6, V6	Yes	No	No	No	No	No
Control level: PLC zone						
PLC1	Yes	No	Yes	No	No	No
PLC2	Yes	No	Yes	No	No	No
Security PLC	Yes	No	Yes	No	No	No
Control level: Stations zone						
Programming station	Yes	No	Yes	Yes	No	Anti-virus Programming software
Configuration station	Yes	No	Yes	Yes	No	Anti-virus
Supervision level: Stations zone						
Supervision stations	Yes	No	Yes	Yes	No	No
SCADA server	Yes	No	Yes	Yes	No	Windows server Anti-virus
Supervision level: Computer stations zone						
Computer stations	Yes	Yes	Yes	Yes	Yes	Anti-virus Anti-spam Windows OS

Table 5.2 - The modeling of the system architecture

Organizational policies and barriers	Applicability levels
Awareness and responsibility	
The awareness of internal employees to the security	**2**
The awareness of employees (how they interact with the phishing emails)	**2**
Physical access	
The accesses to equipment are secured with badges and keys	**2**
The accesses from outside the industry are accompanied during a visit	**4**
Digital access	
The digital accesses are secured (authentication)	**1**
Passwords management (periodic modification, generation)	**2**
Control of equipment	
The management of using the removable media (USB, Hard disk)	**2**
Detection mechanisms: anti-virus software	**2**
Remotely access and connection to the internet	
The connection to the internet is protected by firewalls	**1**
Anti-spam software	**4**

Table 5.3 - The list of some vulnerabilities for this case study

5.2.2.2. Searching for possible attacks

In the proposed approach, we have five attack surfaces: physical access, an email reception, internet connexion, remote access, and software. We define the existing attack surfaces on each zone of ICS levels:

- Physical component zone (field level): physical access
- PLC zone (control level): physical access, remote access

- Stations zone (control level): physical access, remote access, software
- Supervision station zone (supervision level): physical access, remote access, software
- Computer station zone (supervision level): physical access, remote access, internet connection, an email reception, software.

To determine the possible attack scenarios on each zone, we use the data the attack surfaces and the data from the generated meta-models of attack scenarios to run the developed algorithm. The results and outputs of the executed algorithm are the possible attack scenarios on the different zones with each existing attack surface, and they are automatically deducted from the generated attack scenarios (presented in Annex A): the different sequences of security events with the sub security events (vulnerabilities and technical steps), and the executed attack. For example, the programming and configuration stations are not connected to the internet, therefore there are no attack scenarios via the internet connection attack surface, but they are accessed remotely, and the attack scenarios via the remote access are one of the algorithm outputs.

5.2.2.3. Combination of risks

Step 1: Combining the safety and cybersecurity risks

The cyber Box-Tie in Figure 5.3 depicts the interaction of cyberattacks and safety events that lead to the initiating events of this case study. It is a typical Bow-Tie, the safety events are related to the accidental scenarios retrieved from the classical hazard study outlined in Step 1. The cyberattacks that cause the occurrence of the initiating events are added to the Bow-Tie, these cyberattacks are extracted from the previous step and are the security events. Each security event is an attack from an attack scenario, and each one can be carried out using the different attack scenarios generated in the preceding step. Throughout the rest of the approach, we will refer the security events as AE and the safety events as SE.

Step 2: Evaluating the combined risks

Determining the likelihoods of safety events:

The likelihoods of occurrence of safety events are determined from the scale in Table 4.1. the likelihood is defined for each safety event separately as follows:

- SE 1: (N/A, C)
- SE 2: (N/A, D)
- SE 3: (N/A, E)
- SE 4: (N/A, D)
- SE 5: (N/A, C)
- SE 6: (N/A, C)

Evaluating the likelihoods of cybersecurity events:

The different steps described in Section 4.3.2 are used to assess the likelihoods of cybersecurity events. Different scales are used: the level of applicability of policies (Table 3.4), the difficulty level of technical steps (Table 3.5), and the overall likelihood levels for cybersecurity events (Tables 4.2 and 4.3).

- AE 1: (4, N/A). This security event can only occur as a result of the attack scenario on the PLC zone through physical access. The likelihood of occurrence of AE 1 is presented in Figure 5.4.

- AE 2: (3, N/A). This security event of the modification of the PLC 1 configuration can occur as a result of one of four attack scenarios: the remote access on PLC zone (Scenario 1), the physical access to the configuration station (Scenario 2), the remote access to the configuration station (Scenario3), or the installed software on this station (Scenario 4). The likelihood of each attack scenario is evaluated separately in this case, and because these scenarios are connected by OR, the AE 2 takes the maximal value of likelihoods of the different attack scenarios. In Figure 5.5, the likelihood evaluation of Scenario 2 (High) is presented. The likelihoods of Scenario 1, Scenario 3, and Scenario 4 are respectively Moderate, Moderate, Moderate.

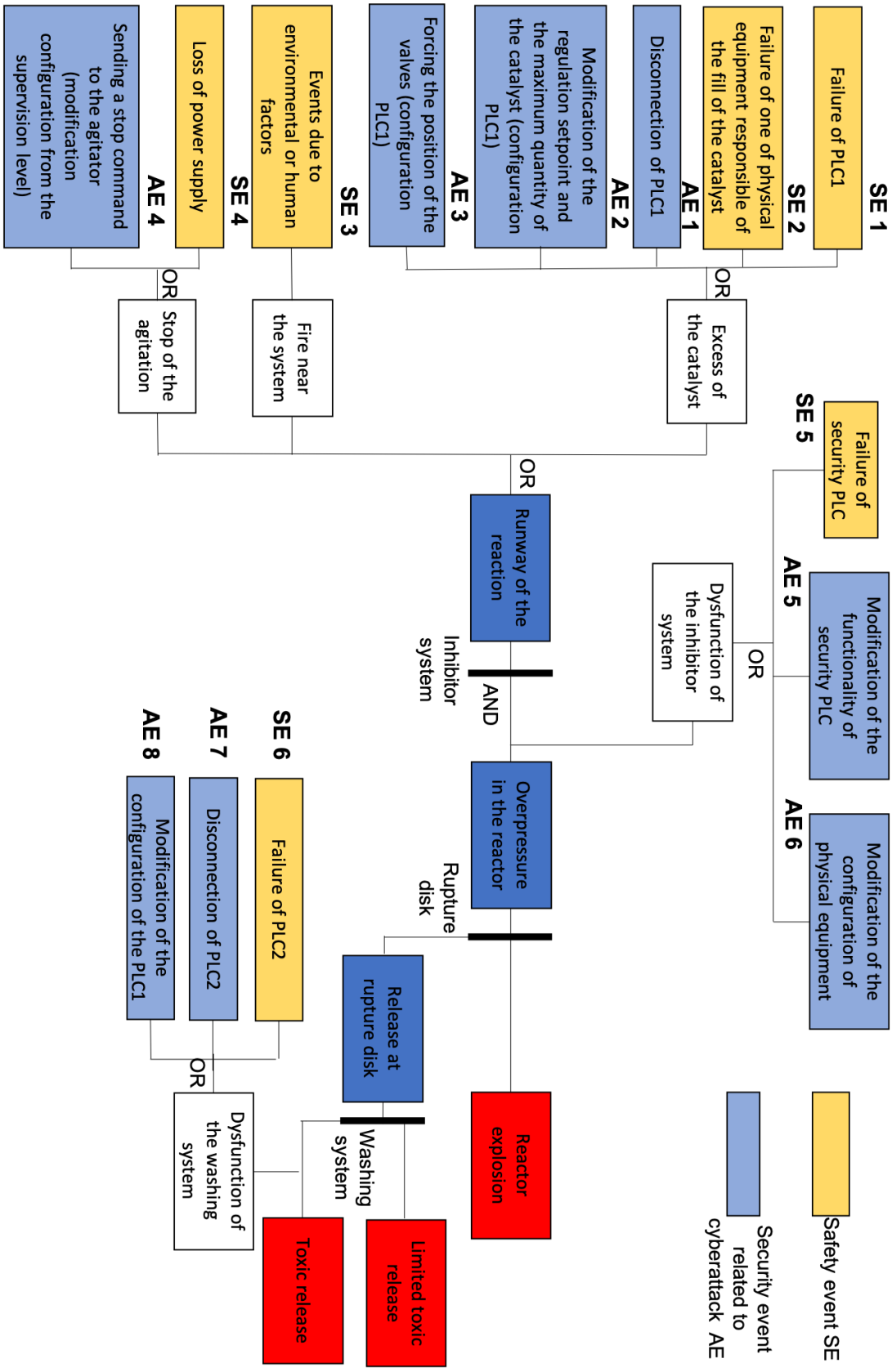

Figure 5.3 - The cyber Bow-Tie of the polymerization system

- AE 3: (4, N/A). This security event has the same scenarios as the security event AE 2.

- AE 4: (3, N/A). This security event can happen in one of eight attack scenarios: through the computer stations zone, with the five attack surfaces (physical access, remote access, internet connection, email reception, and software), or through the supervision stations zone, with three attack surfaces (physical access, remote access, software). The AE 4 takes the maximum value of the likelihood of the different attack scenarios. Figures 5.6 shows the likelihood evaluation of the attack scenario on the computer stations via the email reception which is High. Figure 5.7 depicts another attack scenario through the internet connection with a likelihood High. The likelihoods for the attack scenarios for these security events are High or Moderate.

- AE 5: (3, N/A). This security event is the modification of the functionality of the security PLC. Because in this case study all the PLC have the same attributes with the same level of applicability of policies. Therefore, the occurrence of this security event can be through the same attack scenarios as the security event AE 2 and have the same value of likelihood.

- AE 6: (3, N/A). This security event has the same scenarios as the security event AE 4.

- AE 7: (4, N/A). This security event has the same scenarios as the security event AE 1, because all the PLC in the control level in this case study have the same attributes and the same applied policies.

- AE 8: (3, N/A). The same case of the security event AE 3.

The likelihoods of all the safety and cybersecurity events provided in the cyber Bow-Tie are evaluated separately. These values will be combined after identifying the MCs.

Determining the list of MCs and calculating their likelihoods

Table 5.4 shows the list of MCs for the different scenarios of the occurrence of the three undesirable events in this case study, including safety events only, cybersecurity events only, or a combination of the two. The likelihood of each MC is assessed here, and each MC is assigned to a level from the combined scale of likelihoods in Table 4.4.

Step 3: Treating the combined risks

In this step, the levels of the combined risk scenarios are evaluated and treated. Each risk scenario is depicted by a MC from one or more safety events, or one or more security events, or a combination of the two types of events, leading to one or more physical undesirable events. We have established 82 risk scenarios (the number of MCs) in this case study, and we will examine some of them to demonstrate the process of this step. Table 5.5 shows the level evaluation of risk scenarios; the level scales are provided in Table 4.5. A scenario in Table 5.5 is represented by the MC leading to the occurrence of the undesirable event.

The unacceptable risk scenarios are prioritized and should be treated first in order to reduce their likelihood of occurrence and criticality. The safety and cybersecurity measures proposed for dealing with these scenarios are illustrated in Table 5.6, together with their current state in this case study. The risk scenarios are arranged in the descending level of risks criticality (the unacceptable risks then the risks to be reduced). These measures are inspired by the ANSII guide for good practices. To propose the measures, we base our recommendations on the causes of each safety or cybersecurity event in each scenario. Thus, all the scenarios with the same events are treated by the same measures.

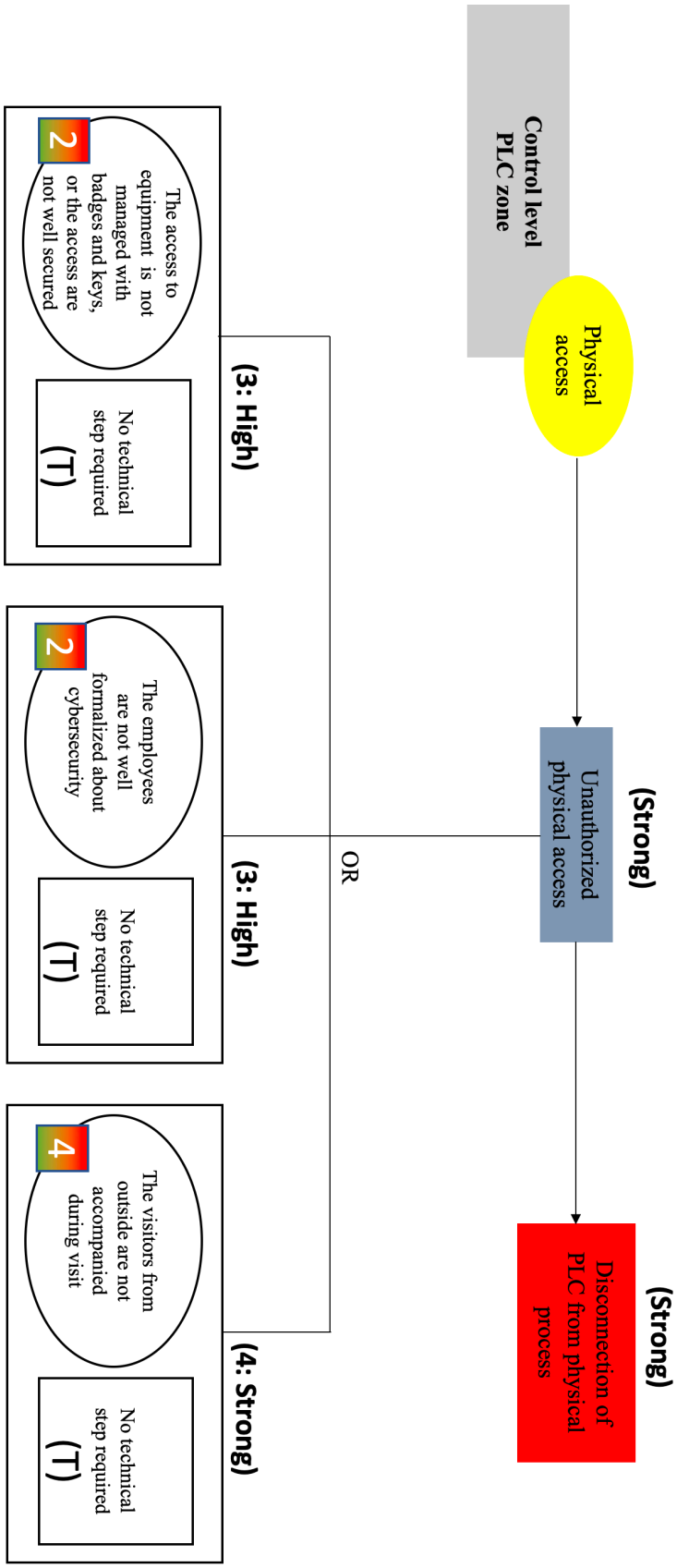

Figure 5.4 - The likelihood evaluation of the cybersecurity event AE 1

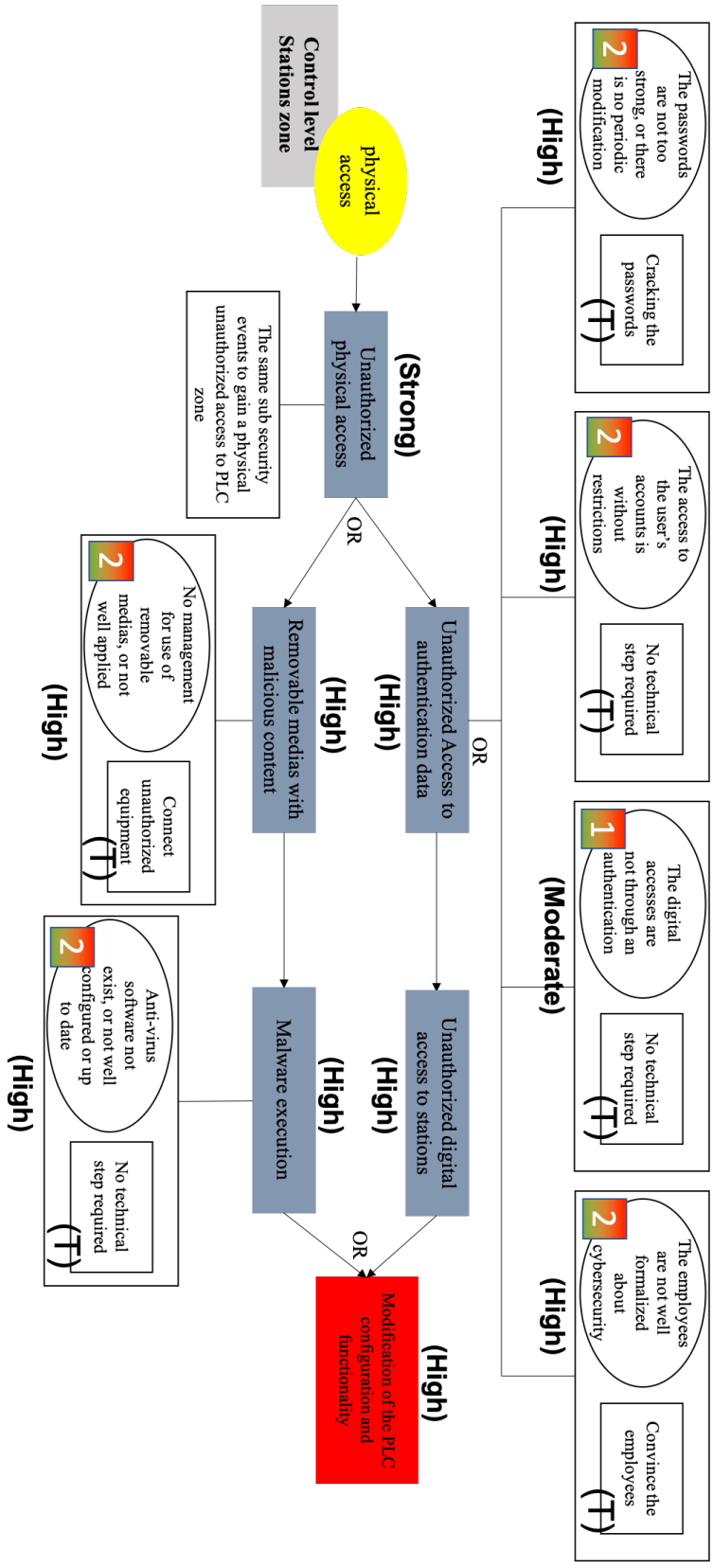

Figure 5.5 - The likelihood evaluation of Scenario 2 from AE 2

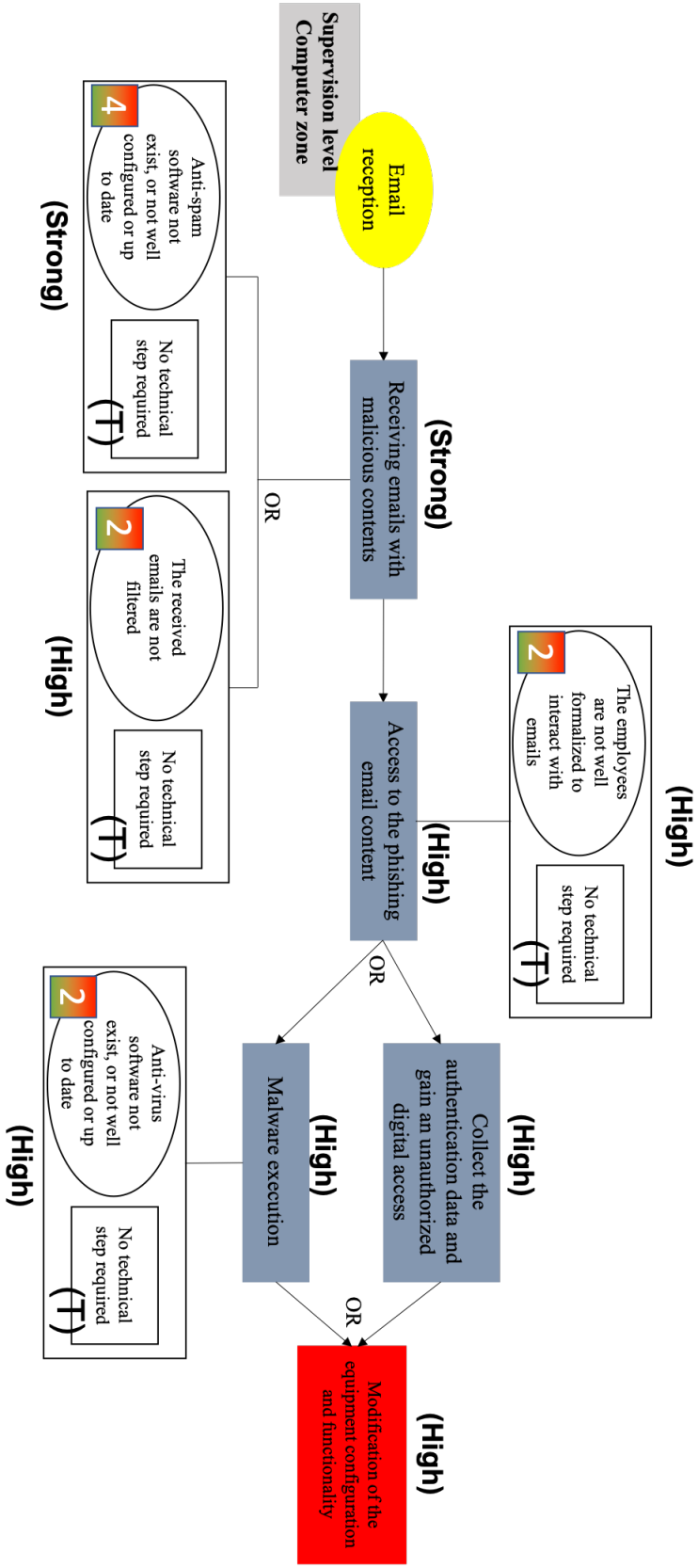

Figure 5.6 - The likelihood evaluation of the scenario through the email reception from AE 4

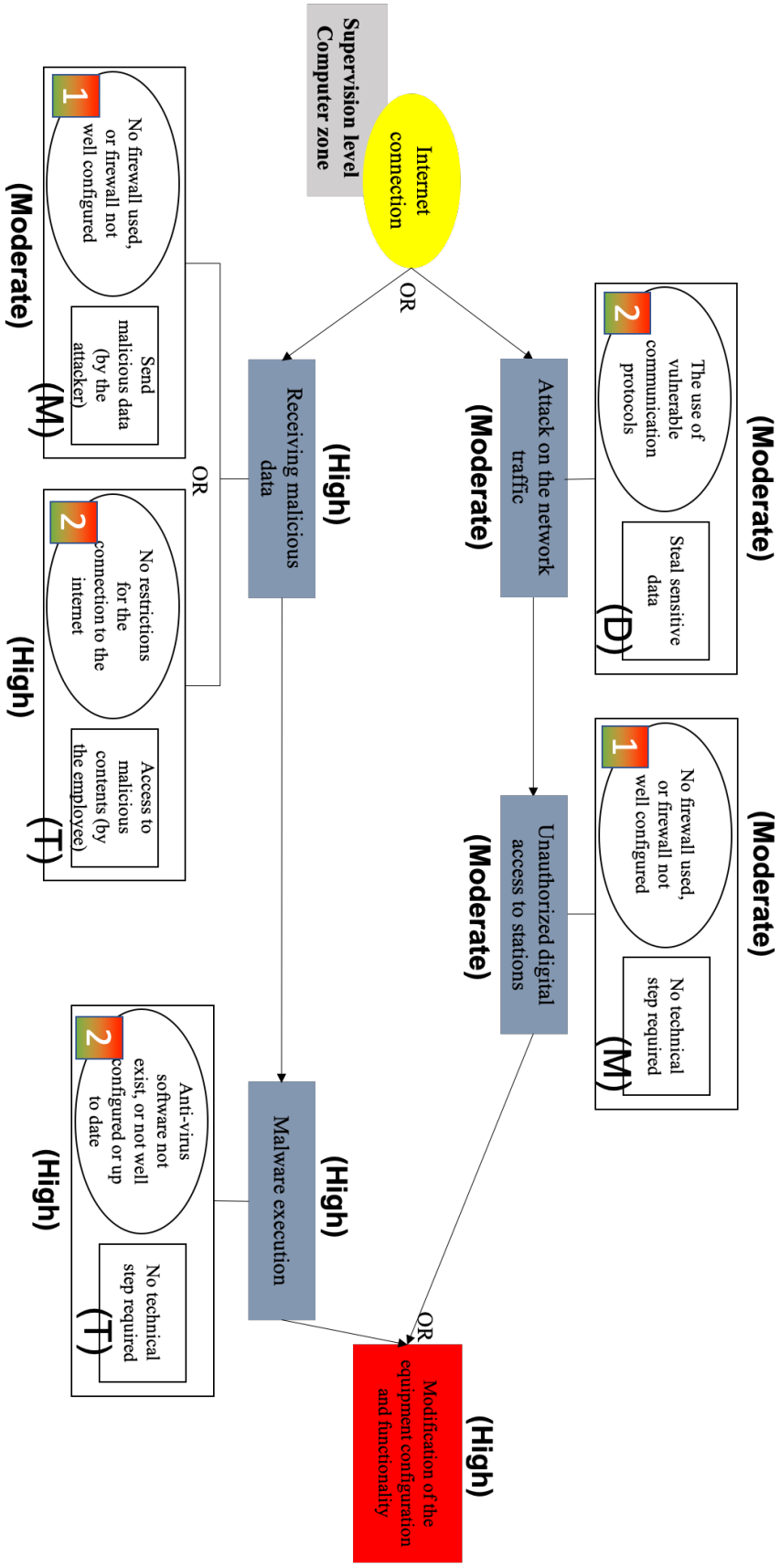

Figure 5.7 - The likelihood evaluation of the scenario through the internet connection from AE 6

MCs	Likelihood	Likelihood Level	MCs	Likelihood	Likelihood Level
SE1, SE5	(N/A, C)	M	AE2, AE5, AE7	(3, N/A)	H
SE1, SE5, SE6	(N/A, C)	M	AE2, AE5, AE8	(3, N/A)	H
SE1, SE5, AE7	(4, C)	M	AE 2, AE6	(3, N/A)	H
SE1, SE5, AE8	(3, C)	M	AE2, AE6, SE6	(3, C)	M
SE1, AE5	(3, C)	M	AE2, AE6, AE7	(3, N/A)	H
SE1, AE5, SE6	(3, C)	M	AE2, AE6, AE8	(3, N/A)	H
SE1, AE5, AE7	(3, C)	M	SE 3, SE5	(N/A, E)	VL
SE1, AE5, AE8	(3, C)	M	SE3, SE5, SE6	(N/A, E)	VL
SE1, AE6	(3, C)	M	SE3, SE5, AE7	(4, E)	VL
SE1, AE6, SE6	(3, C)	M	SE3, SE5, AE8	(3, E)	VL
SE1, AE6, AE7	(3, C)	M	SE3, AE5	(3, E)	VL
SE1, AE6, AE8	(3, C)	M	SE3, AE5, SE6	(3, E)	VL
SE2, SE5	(N/A, D)	L	SE3, AE5, AE7	(3, E)	VL
SE2, SE5, SE6	(N/A, D)	L	SE3, AE5, AE8	(3, E)	VL
SE2, SE5, AE7	(4, D)	L	SE3, AE6	(3, E)	VL
SE2, SE5, AE8	(3, D)	L	SE3, AE6, SE6	(3, E)	VL
SE2, AE5	(3, D)	L	SE3, AE6, AE7	(3, E)	VL
SE2, AE5, SE6	(3, D)	L	SE3, AE6, AE8	(3, E)	VL
SE2, AE5, AE7	(3, D)	L	SE4, SE5	(N/A, D)	L
SE2, AE5, AE8	(3, D)	L	SE4, SE5, SE6	(N/A, D)	L
SE2, AE6	(3, D)	L	SE4, SE5, AE7	(4, D)	L
SE2, AE6, SE6	(3, D)	L	SE4, SE5, AE8	(3, D)	L
SE2, AE6, AE7	(3, D)	L	SE4, AE5	(3, D)	L
SE2, AE6, AE8	(3, D)	L	SE4, AE5, SE6	(3, D)	L
AE 1, SE 5	(4, C)	M	SE4, AE5, AE7	(3, D)	L
AE1, SE5, SE6	(4, C)	M	SE4, AE5, AE8	(3, D)	L
AE1, SE5, AE7	(4, C)	M	SE4, AE6	(3, D)	L
AE1, SE5, AE8	(3, C)	M	SE4, AE6, SE6	(3, D)	L
AE1, AE5	(3, N/A)	H	SE4, AE6, AE7	(3, D)	L
AE1, AE5, SE6	(3, C)	M	SE3, AE6, AE8	(3, D)	L
AE1, AE5, AE7	(3, N/A)	H	AE4, SE5	(4, C)	M
AE1, AE5, AE8	(3, N/A)	H	AE4, SE5, SE6	(4, C)	M
AE1, AE6	(3, N/A)	H	AE4, SE5, AE7	(4, C)	M
AE1, AE6, SE6	(3, C)	M	AE4, SE5, AE8	(3, C)	M
AE1, AE6, AE7	(3, N/A)	H	AE4, AE5	(3, N/A)	H
AE1, AE6, AE8	(3, N/A)	H	AE4, AE5, SE6	(3, C)	M
AE2, SE5	(3, D)	L	AE4, AE5, AE7	(3, N/A)	H
AE2, SE5, SE6	(3, C)	M	AE4, AE5, AE8	(3, N/A)	H
AE2, SE5, AE7	(3, C)	M	AE4, AE6	(3, N/A)	H
AE2, SE5, AE8	(3, C)	M	AE4, AE6, SE6	(3, C)	M
AE2, AE5	(3, N/A)	H	AE4, AE6, AE7	(3, N/A)	H
AE2, AE5, SE6	(3, C)	M	AE4, AE6, AE8	(3, N/A)	H

Table 5.4 - The list of MCs with their likelihood's evaluation

MCs	Likelihood Level	Undesirable events UE	Criticality levels of UE	Risk scenario level
SE1, SE5 (**Scenario 1**)	M	UE 1	Disastrous	**Unacceptable**
SE1, SE5 (**Scenario 2**)	M	UE 2	Serious	**To be reduced**
SE1, SE5, SE6 (**Scenario 3**)	M	UE 3	Catastrophic	**Unacceptable**
SE1, SE5, AE7 (**Scenario 4**)	M	UE 3	Catastrophic	**Unacceptable**
SE2, SE5, AE8 (**Scenario 5**)	L	UE 3	Catastrophic	**To be reduced**
SE2, AE5 (**Scenario 6**)	L	UE 2	Serious	**Acceptable**
SE2, AE6 (**Scenario 7**)	L	UE 1	Disastrous	**Unacceptable**
AE1, AE5, AE7 (**Scenario 8**)	H	UE 3	Catastrophic	**Unacceptable**
AE2, AE5 (**Scenario 9**)	H	UE 1	Disastrous	**Unacceptable**
AE2, AE6 (**Scenario 10**)	H	UE 2	Serious	**To be reduced**
SE3, AE6 (**Scenario 11**)	VL	UE 2	Serious	**Acceptable**
SE3, AE6 (**Scenario 12**)	VL	UE 1	Disastrous	**Unacceptable**

Table 5.5 - The evaluation of some risk scenarios

Risk scenarios	Proposed measures	Status
Scenario 1	• Periodic maintenance of physical equipment (sensors, valves, PLC…). • Redundancy of critical physical equipment.	Partially applied To apply
Scenario 3	The same measures that partially applied and to be applied for Scenario 1.	
Scenario 4	The same measures of Scenario1, adding: • Protect access to the equipment with badges and keys. • Train employees to raise their awareness of security. • Accompaniment of visitors from outside the industry.	Applied almost everywhere Applied almost everywhere To apply
Scenario 7	The same measures of Scenario 1 and Scenario 4, adding: • Choose the passwords carefully with periodic modification.	Applied almost everywhere

	• Refuse the connection of third-party equipment (USB, Hard disk). • Protect the stations by an anti-virus which should be up to date. • Protect the stations that receive emails by an anti-spam up to date. • Implement a backup system for critical data. • Update the existing software and the operating systems in line with the security updates. • Redundancy of critical equipment	Applied almost everywhere Applied almost everywhere To apply To apply To apply To apply
Scenario 8	The same measures of Scenario 4 and Scenario 7.	
Scenario 9	The same measures as Scenario 7.	
Scenario 12	The same measures of Scenario 7, adding: • Alert in case of unwanted events. • Implement an effective rescue plan in case of unwanted events.	Applied Partially applied
Scenario 2	The same measures as Scenario 1.	
Scenario 5	The same measures as Scenario 4.	
Scenario 10	The same measures as Scenario 7.	

Table 5.6 - The list of some of the proposed safety and security measures

5.2.3. Discussion and improvement

The application of the proposed approach to the case study of a chemical reactor and the different risk scenarios containing safety and/or safety events demonstrate the relevance of treating safety and cybersecurity risks together in order to improve the risk analysis and decision making. The list of MCs defined

in Table 5.4 depicts the different risk scenarios for the occurrence of the undesirable event, and we should note that MCs purely related to cybersecurity are ranked High (H). Thus, it is much more vital to think about cybersecurity risks while assessing safety risks.

The modelling of the components responsible for the occurrence of undesirable events with the list of the attributes (physical access, internet connection, emails reception, implemented software, use of removable media) aids and simplifies the process of searching for the vulnerabilities from the check-list of vulnerabilities generated and the attack surfaces present on each ICS levels of this case study. Furthermore, the previous steps aid in the preparation of the data required to automatically generate the attack scenarios for this case study using an algorithm. This new process of searching the step of searching the attack scenario from the generated meta-models is made easier with this new approach. Therefore, the proposed approach provides a guided and systematic risk analysis process, as well as making the process easier to implement with a sufficient level of detail by using the generated meta-models, the generated list of vulnerabilities, and the automatic generation of attack scenarios. In the following section, a conclusion finishes this chapter.

5.3. Conclusion

The proposed approach focuses on combining safety and cybersecurity risks analysis in a single process that is easy to use and incorporates as many attack scenarios as possible. Finally, we demonstrated in this chapter the proposed risk analysis approach using a case study of a polymerization system from INERIS. For this case study, the classical hazard study “Bow-Tie” exists, which aids in determining the sequences of the occurrence of three physical undesirable events that are examined in the proposed process. These events can occur from cyberattacks, safety events, or a mix of the two. The system architecture was modelled by creating tables that listed the components responsible for the occurrence of UE and their attributes. From the generated list of vulnerabilities, the existing ones were validated, and the applicability levels of the policies linked to the vulnerabilities were defined. On each ICS level and zone, the current attack surfaces have been established. At this level, the data required to execute the algorithm for generating the attack scenarios was available, allowing for the

generation of a list of possible attack scenarios. The outcomes of these steps provide a new and simple way for determining the attack scenarios.

In the same graph, the cyber Bow-tie, these attack scenarios have been coupled with the appropriate safety events. The outputs of the approach reveal significant improvements in both the representation of the risk scenario and the likelihood evaluation step. The lists of MCs, as well as the separation between those MCs that are purely related to safety, cybersecurity, or both, aid in understanding the origin of risk and determining the right decision of applying control and security measures. The results of the application are discussed in this chapter in order to improve the proposed approach and its benefits. The proposed approach respects the main steps of risk analysis of the standard ISO 31000 (risk identification, risk analysis, risk treatment), it is applicable and adapted with industrial processes and aims to analyse the potential risks. We give at the end of this thesis a global conclusion on the objective and the contributions of this work, along with some perspectives that should addressed for future research.

Global conclusion and perspectives

Risk analysis is an important manner for regulators to use when making decisions about critical industrial systems that are high-risk level. These industries are required to do a risk analysis on their installations in order to protect them and avoid the unintentional risk that can cause harm to people and the environment. A large number of hazardous risk analysis approaches have been offered for this purpose. The INERIS uses the Bow-Tie analysis to identify and analyze the risk scenarios associated to the accidental situations. The industrial systems throughout the world have recently integrated digital and communicating technologies into their control systems, exposing their infrastructures to new types of threats known as “cyberattacks” and posing new cybersecurity challenges and issues that must be addressed. For these reasons, the INERIS needs to incorporate the cybersecurity concerns into the safety risk analysis process. The goal of this thesis is to propose and develop a risk analysis approach that considers both safety and cybersecurity risks in the same process.

Chapter 1 discusses the terms safety and cybersecurity, as well as their differences, similarities, and the different types of interdependencies between them. The remainder of Chapter 1 describes the structure of an industrial control systems, as well as the new cybersecurity issues that have arisen as result of the digitization and the integration of new technologies into the control systems. This section is followed by a list of the most serious cybersecurity incidents that have occurred around the world. Therefore, the problem and the goal of this work are to propose a new risk analysis approach that combine the cybersecurity and safety risks, despite the fact that most of the existing risk analysis approaches are only designed to deal with safety risks, despite the common consequences and the interdependencies between the two.

After presenting the context of the study and the research problems, Chapter 3 provides the state-of-the-art of the thesis work, which seeks to describe, compare, and classify about twenty existing risk analysis approaches with different processes that combine the safety and cybersecurity in various ways. As a result of this review, the advantages and the limits of the presented approaches were determined, which assisted us in deciding how to design our proposed approach,

which can answer to the requirement for risk analysis while simplifying the analysis steps.

Chapters 3 and 4 present the contributions to the objective and the different steps of the proposed risk analysis approach. It is divided into three big parts:

- Data collection which aims to collect the data needed from the industrial installation for the rest of the approach process: the physical undesirable events from a classical hazardous study with their initiating events, which can be from source safety, cybersecurity, or both; the system modeling which aims to define and model the list of the components responsible for the occurrence with a list of attributes; the searching for vulnerabilities from a generated checklist of generic organizational policies that can be encountered on an industrial site.

- Searching for possible attacks: new meta-models are generated that reflect the different possible attack scenarios through different attack surface on the different ICS levels of any industrial site. To make searching for the attack scenarios on a case study easier, a computerized code was developed in order to search and generate the existing attack scenarios on a case study automatically.

- Risk combination: the safety and cybersecurity risks (related to cyberattacks) are combined in the same Bow-Tie, with an evaluation of the likelihood of the combined risks, as well as an evaluation of the level of criticality for each combined risk scenario. Finally, the unacceptable high risks are treated by proposing effective safety and cybersecurity measures.

The proposed approach is demonstrated in Chapter 5 using a case study of a polymerization system developed by INERIS. A discussion and an improvement for the proposed risk analysis approach are presented at the end of this chapter.

Perspectives

As perspectives that can be envisaged for future work, the most important are mentioned as follows:

- The application of the proposed risk analysis approach to a real case study of a polymerization system by visiting the site of INERIS, in order to show

its ability to assess the safety and cybersecurity risks on an industrial system from different natures of domains.

- We proposed the automatic generation of attack scenarios for a case study in order to make the application of the proposed process easier. However, in order to evaluate the likelihood of each attack scenario, the user must do so using the generated meta-models. This results a difficult step for non-expert users to evaluate the likelihood of attack scenarios users, but it will aid future research into integrating the likelihood evaluation of each attack scenario into the same algorithm of generation for attack scenarios to be evaluated automatically.

- The integration of classical failures into the generic meta-models of attack scenarios. At each zone of ICS level, there are different traditional failures, such as the failure and malfunction of an essential physical equipment (sensors, valves, etc.), or the dysfunction of the PLC, etc. This integration intends to generate the possible failure modes at each level of ICS automatically using the same attack scenario algorithm.

Annex

Annex A

Field level: Physical components zone

1- Physical access

At the filed level, an attack can usually limited to the surface of physical access. Employees (operators, technicians, etc.), visitors, service companies, and others may have access to this level, depending on the case study. Figure 1 illustrates the attack scenarios that can occur on the filed level through the physical access that allows an attacker to disconnect an equipment (sensors, valves, etc.) from the physical process, cuasing the system to malfunction and causing damage (attack on hardware), or if there are intelligent sensors, the attacker can change their configurations and functioning to cause damage to the system.

To carry out this attack, the attacker needs as a first security event an unauthorized physical access. This unauthorized physical access can be achieved [99] by one of these combinations of vulnerabilities and technical steps listed below:

- The attacker takes advantages of a vulnerability in the access to the physical equipment locals, this access could be without badges or keys, or it could be controlled without badges or keys. This vulnerability can be exploited without requiring any technical step (the lowest level of difficulty from the scale in Table 4.5)

- The attacker can exploit the vulnerability during an unsupervised visit by someone from outside the industry, and get an unauthorized physical access. This vulnerability can be exploited without the attacker's expertise or technical skills.

- If the employees in an industry are not well formalized about the cybersecurity and its risks, they might be an important source of vulnerability, executing an unintentional attack without any technical step required (internal attacker and threat).

Control level: PLC zone

In this zone, the attack scenarios through the current attack surfaces on a PLC, which are the physical access and the remote access, are generated.

1- Physical access

At the control level, on the PLC zone, using the physical access, an attack scenario can occur in order to disconnect the PLC control from the physical process and cause damage to the operation of the equipment controlled by the attacked PLC. The same process of the physical access on the field level was used to execute this attack, which was linked to the security event of getting an unauthorized physical access, and the different security sub events that could occur. Figure 2 illustrates the attack scenario against the PLC zone via the physical access.

2- Remote access

A PLC can be accessed remotely from outside the industry in some circumstances of industrial systems. Therefore, an attack scenario through the attack surface of remote access exists. The objective of the attacker is to change the configuration and the functionality of the PLC, causing damage to the physical process and industrial infrastructure (send false instructions to valves, etc.). To carry out this attack, the attacker requires as a first security event an unauthorized remote access.

This security event can occur because a vulnerability exists on the option of the remote access on the PLC, which is not adequately controlled, such as the remote access is always in active mode, or there is no management on the employee's accounts that can access the system remotely. The attacker takes advantage of this vulnerability by establishing a remote session and gaining an access to the PLC. Figure 3 shows the attack scenarios on the PLC via the remote access.

Control level: Configuration and programming stations zone

1- Physical access

The first attack surface that generates the attacks scenarios at the control level for the configuration and programming stations zone is the physical access. As previously stated, the first step in an attack through the physical access is to gain an unauthorized physical access to the local where the equipment being attacked is located. For this zone, to acquire an unauthorized physical access to the local of stations, the identical security sub events as the preceding zone can occur. Once an attacker gains a physical access to the stations, he has a variety of alternatives and sequences of security events to carry out his attack and modify the configuration or the code source (automate) of PLC (Figure 4):

- The attacker can attempt to get an unauthorized access to authentication data (username, password) in order to gain a digital access to the stations and execute its attack. One of the following combinations of vulnerabilities and technical steps is used to gather authentication data:

    a) The attacker can crack the passwords of a user by exploiting the vulnerability in the policies used to generate and protect the passwords (forced password expiration, strong passwords, forbidding password sharing).

    b) The attacker can exploit the vulnerability that exists on the user accounts that is unrestricted (no access controls are enforced, and administrative access in unrestricted), and gain the authentication without requiring any technical steps.

    c) The stations can be accessed digitally without required authentication. Therefore, the attacker can take advantage of this vulnerability without having to take any technical steps.

    d) Using the fact that the employees are not well formalized about the cybersecurity, the attacker can persuade the employees to pass over credentials or sensitive data, including the authentication data.

- Alternatively, the attacker can insert an unauthorized removable media containing a malicious content into a station to execute a malware (types of

malware that can be executed are listed in Annex B) and subsequently modify the configuration or the code source of the PLC. To connect the removable media, the attacker exploits the vulnerability that there is no or ineffective management for the usage of removable medias on the configuration ad programming stations. The attacker can then use the fact that there is no anti-virus software to detect the malware, or that the anti-virus software is improperly set or out to date to successfully execute the malware. Through these many scenarios, the attacker can change the PLC configuration or functionality (shutdown mode, code source modification), or erase crucial data from the stations that control the functionality of the PLC.

2- Email reception

If these two stations receive emails from outside the industry, an attack on the PLC configuration, its functionality, or its code source can also happen through the surface of email receiving. The possible attack scenarios resulting from this attack surface of receiving email are depicted in Figure 5. As a first step in executing the attack, and without any technical step, the attacker sends email with harmful contents (phishing email, spam) to the user's emails on the configuration and programming stations, by exploiting these two probable vulnerabilities on these stations:

- There is no anti-spam software implemented to prevent these kinds of emails from being received, or it is implemented but not effectively configured or up to date.

- The received emails on these stations are not filtered, therefore a station can receive any form of emails from outside the industry without restrictions.

When a station receives a phishing email, an employee can access to the content of the email (virus, malicious website, malicious applications, and so on), exploiting the vulnerability that the employees may not well-trained to deal with such emails. After gaining access to the content, the attacker can obtain the authentication data and use it to acquire an unauthorized digital access to this station, or the attacker can use this station to execute a malware (a possibility to have a vulnerability on the anti-virus software). Using these two scenarios, the

attacker can change the configuration of the PLC, its functionality, or its code source.

3- Remote access

If these two stations can be accessible remotely from outside the industry, an attack on the PLC configuration, its functionality or its code source can also happen through the surface of remote access. The possible attacks scenarios for this attack surface are depicted in Figure 6. The attacker attempts to start an unauthorized remote session on the station first, exploiting the vulnerability that the remote access on this station is not adequately managed, such as the remote access is always in active mode or there is no management on employee accounts that can access the system remotely. After successfully opening a remote session, the attacker can acquire an unauthorized digital access to the station, and:

- He can direct modify the configuration of the PLC, its functionality, or its code source.

- Or he can use a malware to cause damage to the PLC functionality or configuration by exploiting the possible vulnerability that there is no anti-virus software, or that it is not properly configured.

4- Internet connection

The stations at the control level can be connected to the internet, allowing the user to access websites and applications. Therefore, an attacker can exploit the vulnerabilities in the internet connection and get access to stations and manipulate the configuration of the PLC, its functionality, or its code source. Figure 7 depicts the different possible attack scenarios that could occur over the internet connection.

- An attacker can attack the network traffic to steal sensitive data (authentication data, configuration data, etc.) by exploiting the use of insecure communication protocols in the industrial system (lack of data encryption, etc.). After that, if he exploits the vulnerability that there is no firewall to protect and manage the input and output traffic to stations, or it is not effectively set, he can successfully acquire an unauthorized digital access to stations. This unauthorized access allows the attacker

to do direct or indirect harm to the stations and the PLC by executing a malware.

- The stations can receive malicious data via the internet connection if one of the following conditions exists: there is no firewall to filter the input and output data to the system, or it poorly configured, allowing the attacker to send malicious data; or there are no restrictions for the internet connection, allowing users to access to all websites and applications that may contain malicious data. The attacker can use these two options to execute a malware and cause damage to stations and PLCs.

5- Software

By performing an attack through the attack surface of software, an attacker can cause damage to the stations at the control level. The station can be implemented using software that contains security flaws or a vulnerable operation system. The attacker can take advantage of one of these two vulnerabilities to gain unauthorized access to stations either, through the vulnerable software or the vulnerable operating system, and then execute a malware to inflict damage to the stations.

Supervision level: Supervision stations and computers zone

Servers, computer stations, and supervision stations (HMI) are examples of components at this level, and they can be accessed physically, receive emails from outside the industry, be accessed remotely from outside the industry, be connected to the internet, and be implemented by software. Like the stations at the control level, the components, at this level, can be attacked from all the five attack surfaces and with the same attack scenarios as the stations at the control level, but with different attack objectives. At this level, the attacker attempts to alter the configurations of physical equipment at the field level (sensors, valve, and so on), or to install a malware on station to disrupt all the physical process or change sensitive data, among other things. At this level, as described in the steps of the approach, there are two zones, because the organizational policies can be applied in different way at each zone with different levels of vulnerability, and for each zone, there can be different possible attack scenarios.

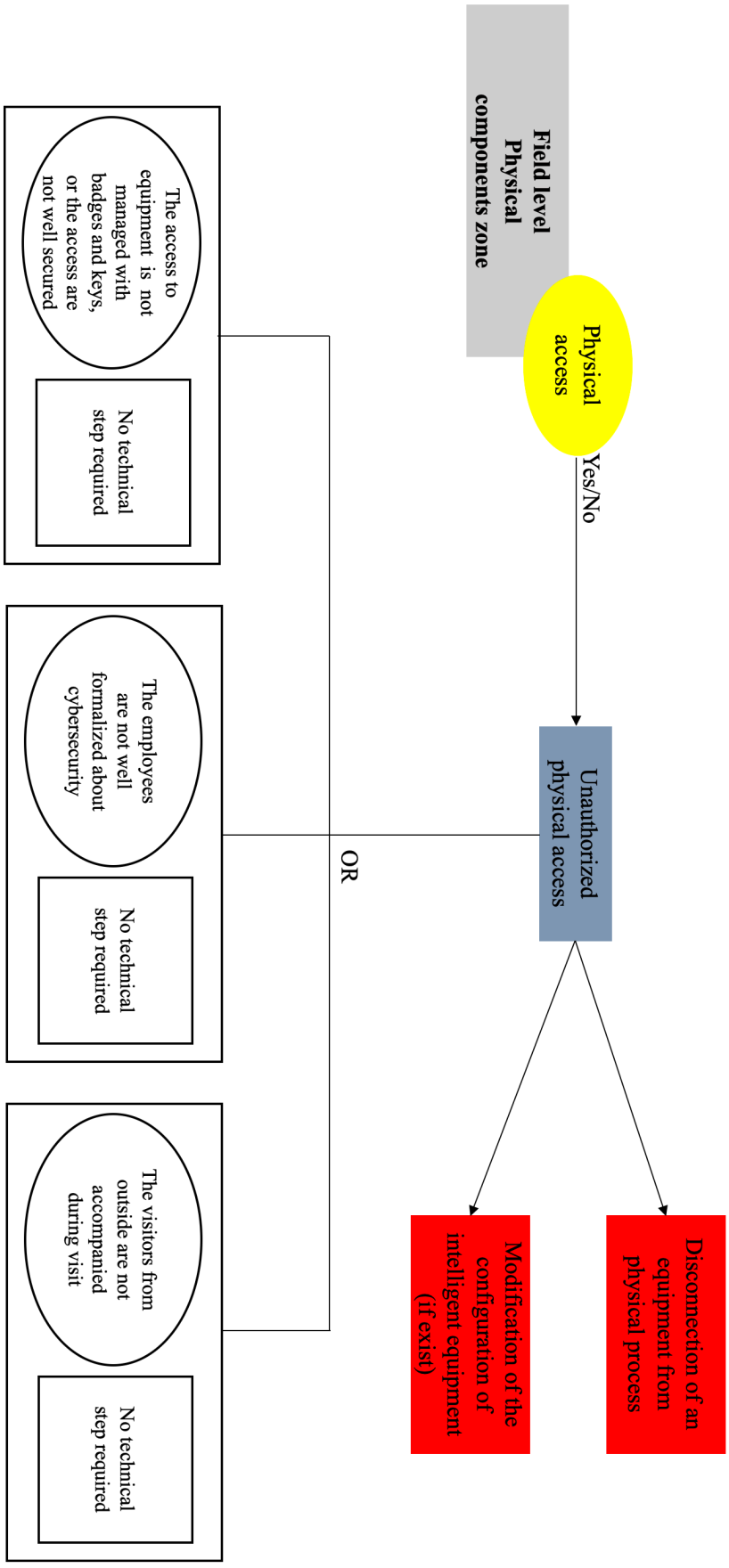

Figure 1 – The attack scenarios on the field level through a physical access

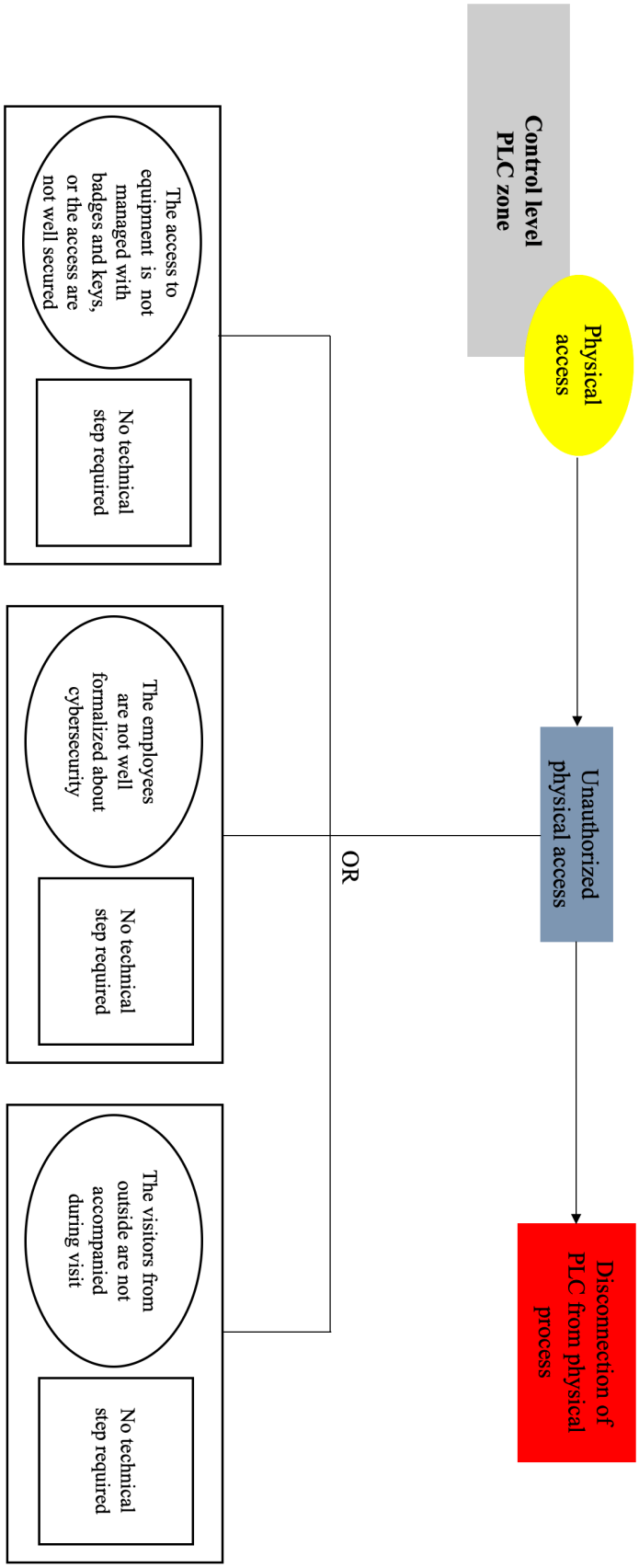

Figure 2 – The attack scenarios on the PLC zone through a physical access

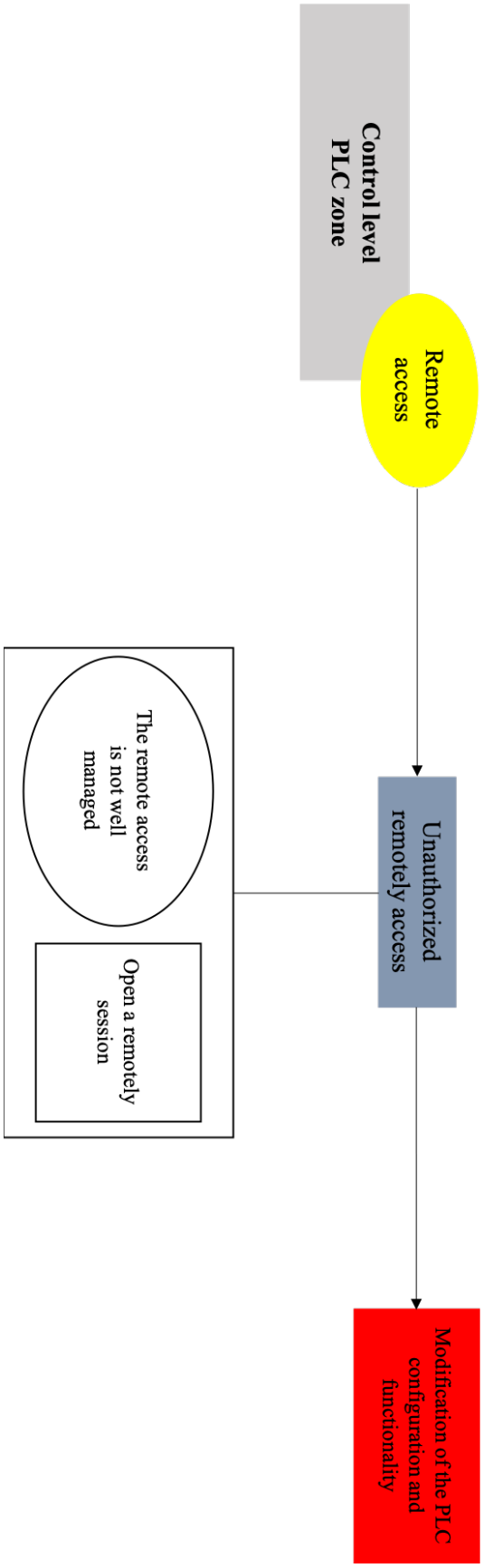

Figure 3 – The attack scenarios on the PLC zone through a remote access

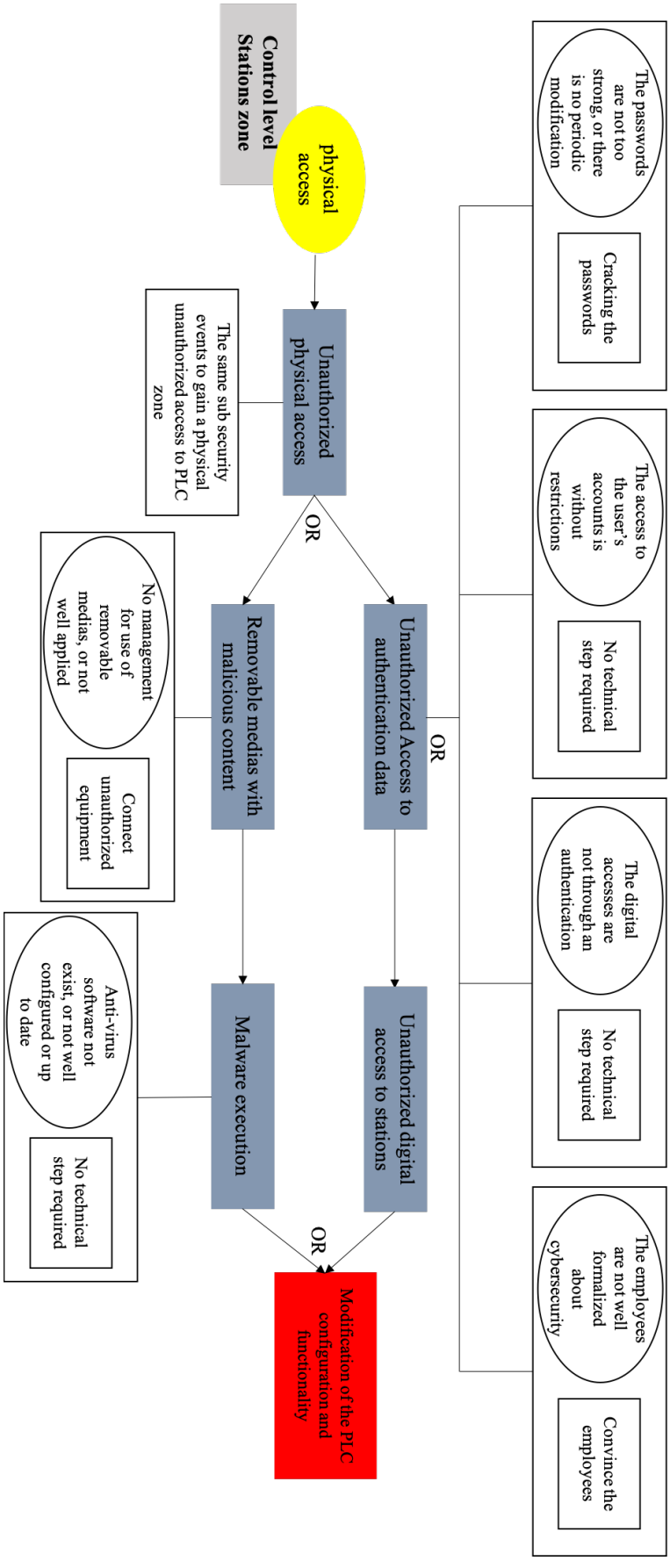

Figure 4 – The attack scenarios on the configuration and programming stations zone through a physical access

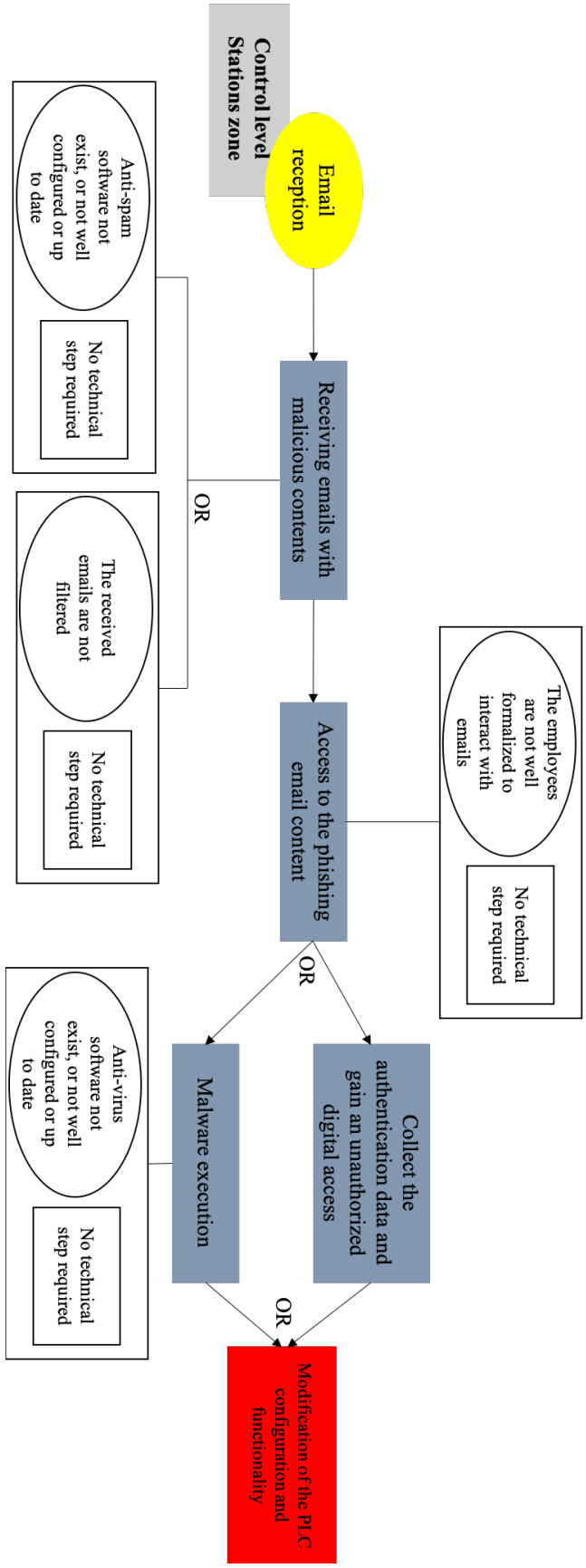

Figure 5 – The attack scenarios on the configuration and programming stations zone through the email reception

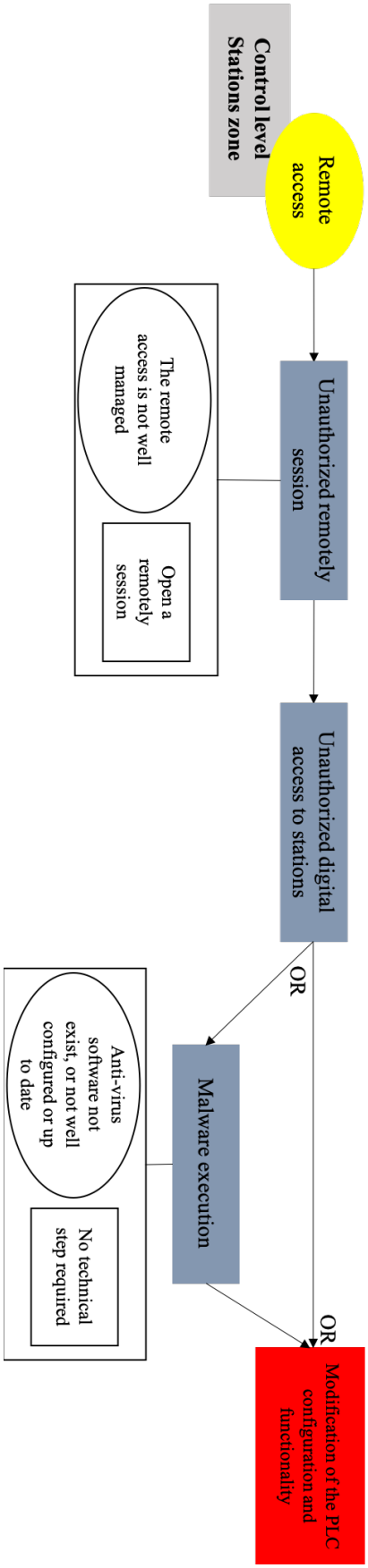

Figure 6 – The attack scenarios on the configuration and programming stations zone through a remote access

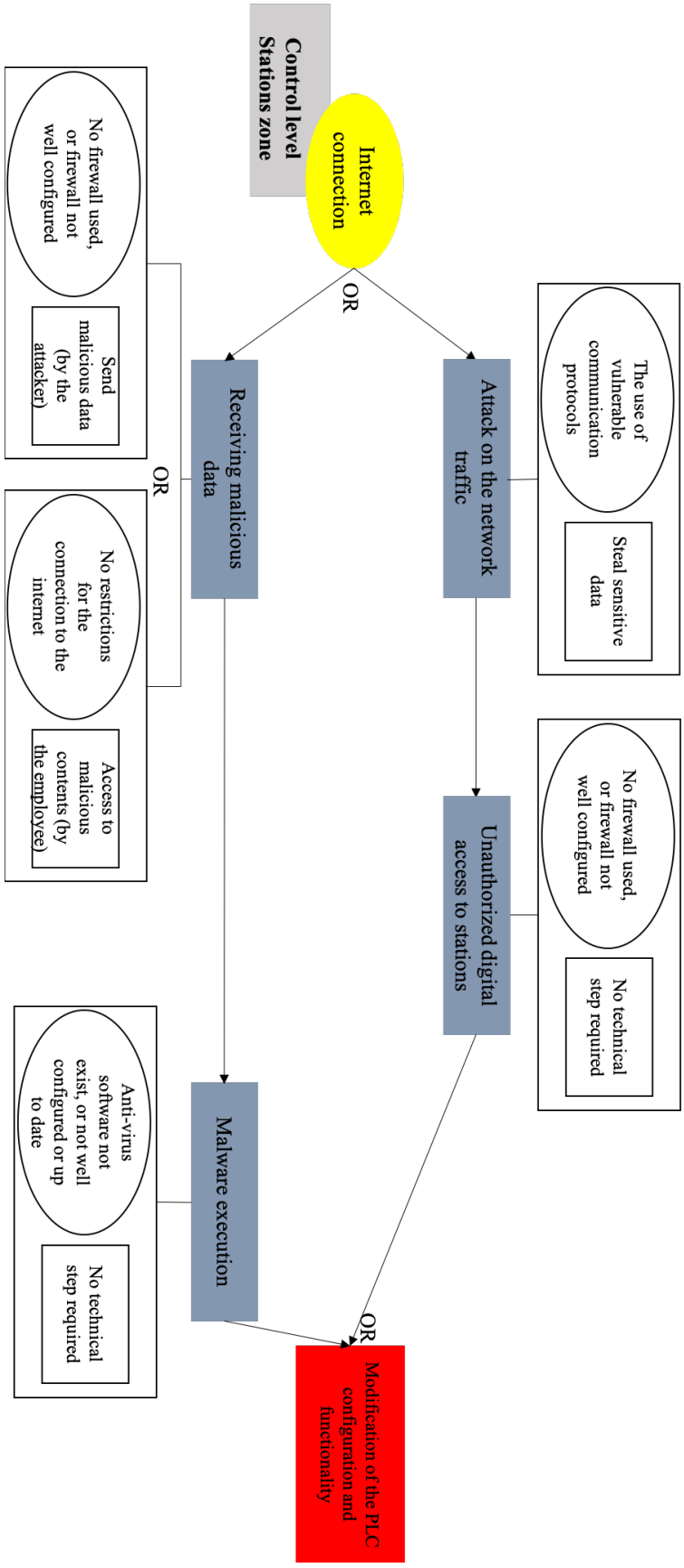

Figure 7 – The attack scenarios on the configuration and programming stations zone through an internet connection

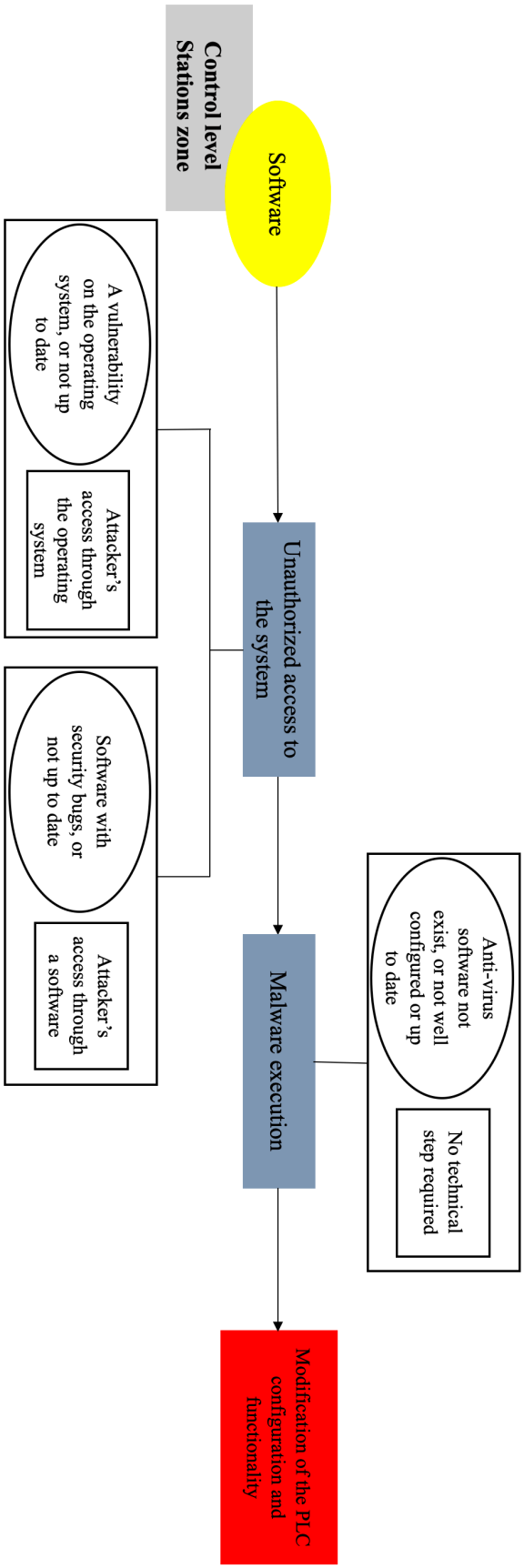

Figure 8 – The attack scenarios on the configuration and programming stations zone through a software

Annex B:

A malware is a malicious software developed by cybercriminals in order to obtain unauthorized access or cause damage to a computer or system in order to steal data, sensitive information, or degrade the functionality of the system, among other things. Thus, a malware comes in different forms, depending on the level of harm it causes, therefore knowing the different forms of possible malware is all that is required. The most prevalent and widespread types of malware that can be executed through the generated scenarios are listed below [100] [101] [1].

- Virus: A virus is a piece of harmful software that hides itself on a computer or a component and can replicate itself from one computer to another. A worm is a sort of virus that spreads through the network. A computer virus is more harmful than a computer worm because it changes or deletes the files on a computer, whereas a worm just copies itself without changing the files or data.

- Ransomware: This is a sort of malicious software that blocks or limits the access of users to their system by locking the screens of the system or locking the files of the users. To regain the access, a ransom should be paid to the attacker.

- Trojan horse: A Trojan horse is a destructive malware disguised as a legitimate application. A trojan horse is damaging and also opens an entry port on the computer, allowing malicious users or applications to get access to the confidential and personal information.

- Rootkit: A Rootkit is a malicious software that installs invisibly, and whose purpose is to provide an attacker access to a system or computer as a privileged user, giving him or her practically a complete control over the system or computer.

- SQL injection: This is a malicious code that is injected into sequences and then provided to a SQL server to be examined and executed in order to access and change information that was not intended to be displayed.

- Cross-Site Scripting XSS: This is a sort of attack in which the attacker injects data, such a malicious script, into the content of trusted websites, in order to bypass access controls to a computer and overflow the data and information.

References

[1] J.-M. Flaus, *Cybersécurité des systèmes industriels*. ISTE Editions, 2019.

[2] A. Burns, J. McDermid, and J. Dobson, "On the meaning of safety and security," *The Computer Journal*, vol. 35, no. 1, pp. 3–15, 1992.

[3] L. Piètre-Cambacédès and C. Chaudet, "The SEMA referential framework: Avoiding ambiguities in the terms 'security' and 'safety,'" *International Journal of Critical Infrastructure Protection*, vol. 3, no. 2, pp. 55–66, 2010.

[4] C. Schmittner, T. Gruber, P. Puschner, and E. Schoitsch, "Security application of failure mode and effect analysis (FMEA)," in *International Conference on Computer Safety, Reliability, and Security*, 2014, pp. 310–325.

[5] R. Mohr, "Preliminary hazard analysis," *Jacobs Sverdrup. February*, 2002.

[6] R. Ferdous, F. Khan, R. Sadiq, P. Amyotte, and B. Veitch, "Handling and updating uncertain information in bow-tie analysis," *Journal of Loss Prevention in the Process Industries*, vol. 25, no. 1, pp. 8–19, 2012.

[7] J. Wei, Y. Matsubara, and H. Takada, "HAZOP-Based Security Analysis for Embedded Systems: Case Study of Open Source Immobilizer Protocol Stack," in *Recent Advances in Systems Safety and Security*, Springer, 2016, pp. 79–96.

[8] M. S. Lund, B. Solhaug, and K. Stølen, *Model-driven risk analysis: the CORAS approach*. Springer Science & Business Media, 2010.

[9] I. N. Fovino and M. Masera, "Through the description of attacks: A multidimensional view," in *International Conference on Computer Safety, Reliability, and Security*, 2006, pp. 15–28.

[10] S. Lautieri, D. Cooper, and D. Jackson, "SafSec: Commonalities between safety and security assurance," in *Constituents of Modern System-safety Thinking*, Springer, 2005, pp. 65–75.

[11] S. Kriaa, L. Pietre-Cambacedes, M. Bouissou, and Y. Halgand, "A survey of approaches combining safety and security for industrial control systems," *Reliability engineering & system safety*, vol. 139, pp. 156–178, 2015.

[12] L. Piètre-Cambacédès, “Des relations entre sûreté et sécurité,” PhD Thesis, Télécom ParisTech, 2010.

[13] S. Kriaa, “Joint safety and security modeling for risk assessment in cyber physical systems,” PhD Thesis, 2016.

[14] A. Almalawi, X. Yu, Z. Tari, A. Fahad, and I. Khalil, “An unsupervised anomaly-based detection approach for integrity attacks on SCADA systems,” *Computers & Security*, vol. 46, pp. 94–110, 2014.

[15] T. Aven, “On the need for restricting the probabilistic analysis in risk assessments to variability,” *Risk Analysis: An International Journal*, vol. 30, no. 3, pp. 354–360, 2010.

[16] ISA, “ISA-62443-3-3 Security for industrial automation and control systems - Security risk assessment for system design.” 2020.

[17] A. Biswas and S. Karunakaran, “Cybernetic modeling of Industrial Control Systems: Towards threat analysis of critical infrastructure,” *arXiv preprint arXiv:1510.01861*, 2015.

[18] L. Pietre-Cambacedes, E. L. Quinn, and L. Hardin, “Cyber security of nuclear instrumentation & control systems: overview of the IEC standardization activities,” *IFAC Proceedings Volumes*, vol. 46, no. 9, pp. 2156–2160, 2013.

[19] S. Schweizerische, “Information technology-Security techniques-Information security management systems-Requirements,” *ISO/IEC International Standards Organization*, 2013.

[20] K. E. Hemsley, E. Fisher, and others, “History of industrial control system cyber incidents,” Idaho National Lab.(INL), Idaho Falls, ID (United States), 2018.

[21] A. Hobbs, *The colonial pipeline hack: Exposing vulnerabilities in us cybersecurity*. SAGE Publications: SAGE Business Cases Originals, 2021.

[22] S. Chen, X. Zhao, X. Baoqiang, X. Yuanhao, and X. Junpeng, “Evaluation Method Of Important Nodes Of Water Supply Network Under Terrorist Attack,” in *IOP Conference Series. Earth and Environmental Science*, 2020, vol. 571, no. 1.

[23] A. Di Pinto, Y. Dragoni, and A. Carcano, “TRITON: The first ICS cyber attack on safety instrument systems,” in *Proc. Black Hat USA*, 2018, vol. 2018, pp. 1–26.

[24] S. Mohurle and M. Patil, “A brief study of wannacry threat: Ransomware attack 2017,” *International Journal of Advanced Research in Computer Science*, vol. 8, no. 5, pp. 1938–1940, 2017.

[25] S. Y. A. Fayi, “What Petya/NotPetya ransomware is and what its remidiations are,” in *Information Technology-New Generations*, Springer, 2018, pp. 93–100.

[26] J. E. Sullivan and D. Kamensky, “How cyber-attacks in Ukraine show the vulnerability of the US power grid,” *The Electricity Journal*, vol. 30, no. 3, pp. 30–35, 2017.

[27] J. T. Langill, “Defending against the dragonfly cyber security attacks,” *Retrieved*, vol. 11, p. 2015, 2014.

[28] P. K. Kerr, J. Rollins, and C. A. Theohary, *The stuxnet computer worm: Harbinger of an emerging warfare capability*. Congressional Research Service Washington, DC, 2010.

[29] T. Oueidat, J.-M. Flaus, and F. Massé, “A review of combined safety and security risk analysis approaches: Application and Classification,” in *2020 International Conference on Control, Automation and Diagnosis (ICCAD)*, 2020, pp. 1–7.

[30] T. Oueidat, J.-M. Flaus, and F. Massé, “Classification des principales méthodes d’analyse des risques combinant la sécurité et la sûreté,” 2020.

[31] E. Lisova, I. Šljivo, and A. Čaušević, “Safety and security co-analyses: A systematic literature review,” *IEEE Systems Journal*, vol. 13, no. 3, pp. 2189–2200, 2018.

[32] S. Chockalingam, D. Hadžiosmanović, W. Pieters, A. Teixeira, and P. van Gelder, “Integrated safety and security risk assessment methods: a survey of key characteristics and applications,” in *International Conference on Critical Information Infrastructures Security*, 2016, pp. 50–62.

[33] Y. Cherdantseva *et al.*, “A review of cyber security risk assessment methods for SCADA systems,” *Computers & security*, vol. 56, pp. 1–27, 2016.

[34] T. Novak, A. Treytl, and P. Palensky, “Common approach to functional safety and system security in building automation and control systems,” in *2007 IEEE Conference on Emerging Technologies and Factory Automation (EFTA 2007)*, 2007, pp. 1141–1148.

[35] J. Dürrwang, K. Beckers, and R. Kriesten, “A lightweight threat analysis approach intertwining safety and security for the automotive domain,” in

International Conference on Computer Safety, Reliability, and Security, 2017, pp. 305–319.

[36] C. Schmittner, Z. Ma, and P. Smith, "FMVEA for safety and security analysis of intelligent and cooperative vehicles," in *International Conference on Computer Safety, Reliability, and Security*, 2014, pp. 282–288.

[37] R. Scandariato, K. Wuyts, and W. Joosen, "A descriptive study of Microsoft's threat modeling technique," *Requirements Engineering*, vol. 20, no. 2, pp. 163–180, 2015.

[38] M. Howard and S. Lipner, *The security development lifecycle*, vol. 8. Microsoft Press Redmond, 2006.

[39] S. Christey, J. Kenderdine, J. Mazella, and B. Miles, "Common weakness enumeration," *Mitre Corporation*, 2013.

[40] M. Steiner and P. Liggesmeyer, "Qualitative and quantitative analysis of CFTs taking security causes into account," in *International Conference on Computer Safety, Reliability, and Security*, 2014, pp. 109–120.

[41] M. Steiner and P. Liggesmeyer, "Combination of safety and security analysis-finding security problems that threaten the safety of a system," 2013.

[42] S. Bezzateev, N. Voloshina, and P. Sankin, "Joint safety and security analysis for complex systems," in *2013 13th Conference of Open Innovations Association (FRUCT)*, 2013, pp. 3–13.

[43] F. Reichenbach, J. Endresen, M. M. Chowdhury, and J. Rossebø, "A pragmatic approach on combined safety and security risk analysis," in *2012 IEEE 23rd International Symposium on Software Reliability Engineering Workshops*, 2012, pp. 239–244.

[44] S. Plósz, C. Schmittner, and P. Varga, "Combining safety and security analysis for industrial collaborative automation systems," in *International Conference on Computer Safety, Reliability, and Security*, 2017, pp. 187–198.

[45] G. Macher, H. Sporer, R. Berlach, E. Armengaud, and C. Kreiner, "SAHARA: a security-aware hazard and risk analysis method," in *Proceedings of the 2015 Design, Automation & Test in Europe Conference & Exhibition*, 2015, pp. 621–624.

[46] H. Abdo, M. Kaouk, J.-M. Flaus, and F. Masse, "A new approach that considers cyber security within industrial risk analysis using a cyber bow-tie analysis," 2017.

[47] G. Sabaliauskaite and A. P. Mathur, “Aligning cyber-physical system safety and security,” in *Complex Systems Design & Management Asia*, Springer, 2015, pp. 41–53.

[48] I. N. Fovino, M. Masera, and A. De Cian, “Integrating cyber attacks within fault trees,” *Reliability Engineering & System Safety*, vol. 94, no. 9, pp. 1394–1402, 2009.

[49] S. Kriaa, M. Bouissou, and Y. Laarouchi, “A model based approach for SCADA safety and security joint modelling: S-Cube,” 2015.

[50] M. Bouissou, N. Villatte, H. Bouhadana, and M. Bannelier, “Knowledge modelling and reliability processing: presentation of the FIGARO language and associated tools,” Electricite de France (EDF), 1991.

[51] J. Brunel, D. Chemouil, L. Rioux, M. Bakkali, and F. Vallée, “A viewpoint-based approach for formal safety & security assessment of system architectures,” in *11th Workshop on Model-Driven Engineering, Verification and Validation*, 2014, vol. 1235, pp. 39–48.

[52] J. Voirin, “Method and tools to secure and support collaborative architecting of constrained systems,” in *27th Congress of the International Council of the Aeronautical Science (ICAS 2010), Nice, France*, 2010, pp. 19–24.

[53] C. Schmittner, Z. Ma, E. Schoitsch, and T. Gruber, “A case study of fmvea and chassis as safety and security co-analysis method for automotive cyber-physical systems,” in *Proceedings of the 1st ACM Workshop on Cyber-Physical System Security*, 2015, pp. 69–80.

[54] A. J. Kornecki, N. Subramanian, and J. Zalewski, “Studying interrelationships of safety and security for software assurance in cyber-physical systems: Approach based on bayesian belief networks,” in *2013 Federated Conference on Computer Science and Information Systems*, 2013, pp. 1393–1399.

[55] L. Apvrille and Y. Roudier, “Designing safe and secure embedded and cyber-physical systems with SysML-Sec,” in *International Conference on Model-Driven Engineering and Software Development*, 2015, pp. 293–308.

[56] Y.-R. Chen, S.-J. Chen, P.-A. Hsiung, and I.-H. Chou, “Unified security and safety risk assessment-a case study on nuclear power plant,” in *2014 International Conference on Trustworthy Systems and Their Applications*, 2014, pp. 22–28.

[57] A. Kornecki and M. Liu, “Fault tree analysis for safety/security verification in aviation software,” *Electronics*, vol. 2, no. 1, pp. 41–56, 2013.

[58] L. Piètre-Cambacédès and M. Bouissou, “Modeling safety and security interdependencies with BDMP (Boolean logic Driven Markov Processes),” in *2010 IEEE International Conference on Systems, Man and Cybernetics*, 2010, pp. 2852–2861.

[59] J. Thomas, “Introduction to Systems Theoretic Process Analysis (STPA).” 2016. [Online]. Available: http://psas.scripts.mit.edu/home/wp-content/uploads/2016/01/Systems-Theoretic-Process-Analysis-STPA-John-Thomas.pdf

[60] D. Pereira, C. Hirata, R. Pagliares, and S. Nadjm-Tehrani, “Towards combined safety and security constraints analysis,” in *International Conference on Computer Safety, Reliability, and Security*, 2017, pp. 70–80.

[61] N. G. Leveson, *Engineering a safer world: Systems thinking applied to safety*. The MIT Press, 2016.

[62] W. Young and N. Leveson, “Systems thinking for safety and security,” in *Proceedings of the 29th Annual Computer Security Applications Conference*, 2013, pp. 1–8.

[63] W. Young, “System-Theoretic Process Analysis for Security (STPA-SEC): Cyber Security and STPA.” STAMP Conference, 2017. [Online]. Available: https://psas.scripts.mit.edu/home/wp-content/uploads/2017/04/STAMP_2017_STPA_SEC_TUTORIAL_as-presented.pdf

[64] I. Friedberg, K. McLaughlin, P. Smith, D. Laverty, and S. Sezer, “STPA-SafeSec: Safety and security analysis for cyber-physical systems,” *Journal of Information Security and Applications*, vol. 34, pp. 183–196, 2017.

[65] W. G. Temple, Y. Wu, B. Chen, and Z. Kalbarczyk, “Systems-theoretic likelihood and severity analysis for safety and security co-engineering,” in *International Conference on Reliability, Safety and Security of Railway Systems*, 2017, pp. 51–67.

[66] N. P. de Souza, C. de A. C. César, J. de Melo Bezerra, and C. M. Hirata, “Extending STPA with STRIDE to identify cybersecurity loss scenarios,” *Journal of Information Security and Applications*, vol. 55, p. 102620, 2020.

[67] M. M. Islam, A. Lautenbach, C. Sandberg, and T. Olovsson, “A risk assessment framework for automotive embedded systems,” in *Proceedings of the 2nd ACM International Workshop on Cyber-Physical System Security*, 2016, pp. 3–14.

[68] G. Sabaliauskaite and S. Adepu, “Integrating six-step model with information flow diagrams for comprehensive analysis of cyber-physical system safety and security,” in *2017 IEEE 18th International Symposium on High Assurance Systems Engineering (HASE)*, 2017, pp. 41–48.

[69] S. Procter, E. Y. Vasserman, and J. Hatcliff, “SAFE and secure: Deeply integrating security in a new hazard analysis,” in *Proceedings of the 12th International Conference on Availability, Reliability and Security*, 2017, pp. 1–10.

[70] M. Ito, “Finding threats with hazards in the concept phase of product development,” in *European Conference on Software Process Improvement*, 2014, pp. 277–284.

[71] J. Delange, L. Pautet, and P. Feiler, “Validating safety and security requirements for partitioned architectures,” in *International Conference on Reliable Software Technologies*, 2009, pp. 30–43.

[72] M. Gallab, M. Tkiouat, H. Bouloiz, and E. Garbolino, “Model for developing a database for risk analysis,” in *2015 International Conference on Industrial Engineering and Systems Management (IESM)*, 2015, pp. 833–841.

[73] S. Kaplan, “The words of risk analysis,” *Risk analysis*, vol. 17, no. 4, pp. 407–417, 1997.

[74] ANSSI, “Classification Method and Key Measures.” [Online]. Available: https://www.ssi.gouv.fr/uploads/2014/01/industrial_security_WG_Classification_Method.pdf

[75] S. Beer, “The viable system model: Its provenance, development, methodology and pathology,” *Journal of the operational research society*, vol. 35, no. 1, pp. 7–25, 1984.

[76] Varonis, “134 Cybersecurity Statistics and Trends for 2021.” 2021. [Online]. Available: https://www.varonis.com/blog/cybersecurity-statistics

[77] Y. Kwak, S. Lee, A. Damiano, and A. Vishwanath, “Why do users not report spear phishing emails?,” *Telematics and Informatics*, vol. 48, p. 101343, 2020.

[78] H. G. Brauch, “Concepts of security threats, challenges, vulnerabilities and risks,” in *Coping with global environmental change, disasters and security*, Springer, 2011, pp. 61–106.

[79] M. A. McQueen, W. F. Boyer, S. M. McBride, and T. A. McQueen, “Empirical estimates of 0day vulnerabilities in control systems,” Idaho National Lab.(INL), Idaho Falls, ID (United States), 2009.

[80] ANSSI, “LA CYBERSÉCURITÉ DES SYSTÈMES INDUSTRIELS.” [Online]. Available: https://www.ssi.gouv.fr/guide/la-cybersecurite-des-systemes-industriels/

[81] M.-E. Paté-Cornell, M. Kuypers, M. Smith, and P. Keller, “Cyber risk management for critical infrastructure: a risk analysis model and three case studies,” *Risk Analysis*, vol. 38, no. 2, pp. 226–241, 2018.

[82] Avast Business, “What is attack surface?” [Online]. Available: https://www.avast.com/fr-fr/business/resources/what-is-attack-surface#mac

[83] E. Irmak and İ. Erkek, “An overview of cyber-attack vectors on SCADA systems,” in *2018 6th international symposium on digital forensic and security (ISDFS)*, 2018, pp. 1–5.

[84] E. J. Byres, M. Franz, and D. Miller, “The use of attack trees in assessing vulnerabilities in SCADA systems,” in *Proceedings of the international infrastructure survivability workshop*, 2004, pp. 3–10.

[85] M. ATT&CK, “Mitre att&ck,” *URL: https://attack. mitre. org*, 2020.

[86] W. Yuanhui, “Safety system engineering,” *Tianjin: Tianjin University Publishing House*, 1999.

[87] S. S. Grossel, “Guidelines for Chemical Process Quantitative Risk Analysis-; By Center for Chemical Process Safety; American Institute of Chemical Engineers, New York, NY, 2000, pp. 750.,” *Journal of Loss Prevention in the Process Industries*, vol. 5, no. 14, pp. 438–439, 2001.

[88] INERIS, “Agrégation semi-quantitative des probabilits dans les études de dangers des installations classées - omega probabilités.” 2015.

[89] INERIS, “Agrégation semi-quantitative des probabilités dans les études de danger des installations classées - omega probabilités.” 2018. [Online]. Available: https://www.ineris.fr/sites/ineris.fr/files/contribution/Documents/DRA-18-171229-00918A_Proba_semi-quanti_Oméga%2025_final_2.pdf

[90] ISO/IEC, “Information Technology - Security techniques - Code of practice for information security management. Manuel de pratiques.” 2013.

[91] ANSSI, “Recommandations relatives à l’authentification multifacteur et aux mots de passe.” 2021. [Online]. Available: https://www.ssi.gouv.fr/uploads/2021/10/anssi-guide-authentification_multifacteur_et_mots_de_passe.pdf

[92] ANSSI, “Cybersécurité pour les systèmes industriels: Mesures détaillées.” 2013. [Online]. Available: https://www.ssi.gouv.fr/uploads/2014/01/securite_industrielle_GT_details_principales_mesures.pdf

[93] ANSSI, “Cybersécurité pour les systèmes industriels: Classification et mesures principales.” 2013. [Online]. Available: https://www.ssi.gouv.fr/uploads/2014/01/industrial_security_WG_Classification_Method.pdf

[94] NIST, “Security and Privacy Controls for Federal Information Systems and Organizations.” 2013. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-53r4.pdf

[95] ISA, “The 62443 Series of Standards, Industrial Automation and Control Systems Security. Collection des normes.” 2018.

[96] K. Stouffer, J. Falco, K. Scarfone, and others, “Guide to industrial control systems (ICS) security,” *NIST special publication*, vol. 800, no. 82, pp. 16–16, 2011.

[97] D. P. Eames and J. Moffett, “The integration of safety and security requirements,” in *International Conference on Computer Safety, Reliability, and Security*, 1999, pp. 468–480.

[98] M. Sun, S. Mohan, L. Sha, and C. Gunter, “Addressing safety and security contradictions in cyber-physical systems,” 2009.

[99] “Ultimate guide to hysical security.” [Online]. Available: https://pages.getkisi.com/physical-security-guide

[100] R. Tahir, “A study on malware and malware detection techniques,” *International Journal of Education and Management Engineering*, vol. 8, no. 2, p. 20, 2018.

[101] Norton, “10 types of malware and how to prevent malware from the start.” 2021. [Online]. Available: https://us.norton.com/internetsecurity-malware-types-of-malware.html

List of publications

International Conferences

- T. OUEIDAT, J-M. FLAUS, F. MASSE. *A new model-based risk analysis approach that generate cyberattacks scenarios and combine them with safety risks.* ESREL*,* Angers, France (2021).

- T. OUEIDAT, J-M. FLAUS, F. MASSE. *A Review of combined safety and security risk analysis approaches: Application and classification.* ICCAD*,* video conference, Paris, France (2020).

National Conferences

- T. OUEIDAT, J-M. FLAUS, F. MASSE. *Classification des principales méthodes d'analyse des risques combinant la sécurité et la sûreté.* Congrès Lambda Mu 22 - ImDR*,* Video conference, Le Havre, France (2020).

Under submission

- T. OUEIDAT, J-M. FLAUS, F. MASSE. *A new way to generate automatically the attack scenarios and combine them with safety risks.* ESREL*,* Ireland (2022).

- T. OUEIDAT, J-M. FLAUS, F. MASSE. *Un nouveau modèle pour générer les scénarios des attaques dans un système industriel pour une analyse des risques.* Congrès Lambda Mu 23 - ImDR, Paris, France (2022).