École doctorale no 072 : Sciences pour l'ingenieur

Doctorat Université de Lille

THÈSE

pour obtenir le grade de docteur délivré par

l'Université de Lille

Spécialité : "Automatique et Informatique Industrielle"

présentée et soutenue publiquement par

Riad CHEMALI

le 09 Juillet 2021

Méthodologie orientée sûreté de fonctionnement pour la cybersécurité des systèmes de contrôle-commande

Directeur de thèse : **Mireille BAYART**
Co-encadrant de thèse : **Blaise CONRARD**

Jury

Jean-Marc THIRIET,	Professeur, Université de Grenoble Alpes	Président - Rapporteur
Christophe AUBRUN,	Professeur, Université de Lorraine	Rapporteur
Christophe BERENGUER,	Professeur, Université de Grenoble Alpes	Examinateur
Laurent CAUFFRIEZ,	Maître de conférences, UPHF	Examinateur
Mireille BAYART,	Professeur, Université de Lille	Superviseur
Blaise CONRARD,	Maître de conférences, Université de Lille	Superviseur

Centre de Recherche en Informatique Signal et Automatique de Lille (CRIStAL)
UMR CNRS 9189, ÉQUIPE ToSyMA

Université de Lille Sciences et Technologies
École Polytech Lille
École Doctorale Sciences pour l'Ingénieur
Centre de Recherche en Informatique Signal et Automatique de Lille
Équipe Tolérance aux fautes des Systèmes Mobiles Autonomes
Cité Scientifique
Boulevard Paul Langevin
59655 Villeneuve d'Ascq
France.

Abstract

The modern ICSs (Industrial Control Systems) are based primarily on Operational Technologies (OTs) that have been inherited from a wide variety of Information Technologies (ITs). In order to ensure the ICSs requirements, several of ITs have been designed or adapted. These technologies are sometimes badly adapted or in some cases they are used with their vulnerabilities for cost reasons (use Commercial Off-The-Shelf products). As a result, new vulnerabilities appeared, and most of them have not been considered in the design phase. Therefore, their ranking, prioritizing and mitigating risks are a crucial task for organizations and researchers that are involved with the security and safety of ICSs systems.
The focus of this thesis is to address the cyber security challenges faced by these systems. It discusses the features of the ICS threat environment and aligns safety and security risk analysis. In fact, the first problem in security risk analyzes is to determine the likelihood of the cyber-attacks. The use likelihood in security analysis is not practical and sometimes does not make sense. Therefore, this prevents the research community from using a panoply of methods that exist in the field of safety because they are based on the use of probabilities. As a consequence, we introduce a new vulnerability scoring system, called ICVSS (Industrial Control Vulnerability Scoring System). The methodology uses different approaches to score vulnerabilities in ICS, taking into account their characteristics. The ICVSS not only makes possible to assess the vulnerability or to ease the communication between the safety and security teams, but also it is a good alternative to replace the likelihood in order to be able to use these safety methods. Moreover, a new approach to co-analysis and co-assessment of safety and security is presented.

Résumé

Les ICSs (Systèmes de Contrôle Industriels) modernes sont basés principalement sur des Technologies Opérationnelles (OTs) héritées d'une grande variété de Technologies de l'information (ITs). Ils remplissent des fonctions vitales dans les systèmes critiques, telles que la distribution d'énergie électrique, la distribution de pétrole et de gaz naturel. Ils sont également au cœur des dispositifs médicaux, des systèmes d'alarmes et de la gestion des transports.
Cependant, ces technologies sont parfois mal adaptées ou, dans certains cas, elles sont utilisées avec leurs vulnérabilités pour des raisons de coûts (utilisation de produits commerciaux disponibles sur le marché (Commercial off-the-shelf COTS). En conséquence, de nouveaux risques sont apparus qui pourraient influencer la sécurité innocuité (SAF) et sécurité immunité (SEC). Parmi ces risques, la plupart n'ont pas été pris en compte lors de la phase de conception. Nous pouvons noter plusieurs similitudes entre la sécurité-innocuité (safety) et la sécurité-immunité (security) en termes d'évaluation des risques. Ce que l'on appelle dangers en matière de SAF, ce sont des menaces à la SEC. Depuis longtemps, nous nous focalisons sur la sécurité-innocuité reliée aux pannes accidentelles. Aujourd'hui, la sécurité-innocuité pourrait être menacée par la branche de sécurité-immunité et les cyberattaques. Dans ce cas, toutes les techniques utilisées dans l' étude de la SAF reliées aux dangers accidentels sont remises en question, car nous sommes en face d'un facteur humain qui est très difficile à modéliser ou d'en prédire le comportement (menace intentionnelle). Ces dernières années, l'évaluation des probabilités des cyberattaques dans les systèmes de contrôle industriel (ICSs) est la partie la plus controversée et subjective. En particulier, pour les industries hautement réglementées et les industries critiques, c'est un problème majeur, car il faut souvent faire des estimations des risques pour des paramètres subjectifs tels que la motivation de l'attaquant. Il a déjà été démontré qu'une approche probabiliste quantitative n'est pas réalisable. De plus, les menaces changent de manière continue et de nouvelles vulnérabilités sont publiées chaque jour. Cela doit être accompagné par un changement des évaluations des risques. Il est donc très important d'évaluer les niveaux de risques, en priorisant les vulnérabilités du ICS en fonction leur niveau de gravité.
L'objectif de cette thèse est de relever les défis de la cybersécurité auxquels ces systèmes industriels sont confrontés. Elle examine les caractéristiques de l'environnement des ICSs et aligne l'analyse des risques de sécurité-innocuité et de sécurité-immunité. Les systèmes de notation de la vulnérabilité comme l'ICVSS (Industrial Control Vulnerability Scoring) ou le CVSS (Common Vulnerability Scoring System) permettent non seulement d'évaluer la vulnérabilité ou de faciliter la communication entre les équipes de sécurité, mais constituent également une bonne alternative pour remplacer les probabilités afin de pouvoir utiliser les méthodes existantes pour modéliser la sécurité-innocuité. Cette thèse présente une nouvelle approche de co-évaluation de la SAF/SEC conforme aux normes utilisées dans la sûreté de fonctionnement des ICSs.

Praise and biggest set of thanks to God first who is the only guide in the right direction during this life.
I dedicate this work to my mother Zakia and my father Abdelmalek, To my brothers, my sisters and my wife who supported and encouraged me throughout the writing of this thesis.

Remerciement

Je tiens à exprimer ma sincère gratitude aux membres du jury : M. Jean-Marc THIRIET et M. Christophe AUBRUN pour avoir accepté d'examiner cette thèse et pour leurs précieux commentaires sur mon travail. Je remercie également chaleureusement les examinateurs : M. Laurent CAUFFRIEZ, M. Christophe BERENGUER pour l'intérêt qu'ils ont porté à mon travail et pour leurs commentaires pertinents. Je suis heureux et honoré d'avoir présenté mon travail devant un jury aussi qualifié.

⋆ ⋆ ⋆ ⋆ ⋆

Je tiens en préambule de ce rapport à remercier tous ceux qui ont participé, de près ou de loin, à son élaboration, ainsi qu'à tous ceux qui m'ont apporté leur aide tout au long de ce projet de fin d'études.
Je souhaite, tout d'abord, exprimer ma profonde reconnaissance à ma promotrice de thèse : Mireille Bayart, et mon co-encadrant Blaise Conrard qui ont su encadrer mon travail avec justesse et application. Leur relecture méticuleuse de ce rapport a assurément contribué à la précision de mon propos.
J'adresse aussi mes remerciements à la direction de laboratoire CRIsAL, pour avoir accepté de m'accueillir au sein de son établissement. Je remercie bien entendu les membres de l'équipe ToSyMA et SoftE : Abdelkader, Othman. Leur aide a été précieuse sur de nombreux problèmes, et leurs conseils toujours avisés et tous les doctorants : Houria, Adel, Mahdi, Imène ... qui ont rendu mon séjour au labo, tellement agréable et convivial.
Je tiens à exprimer toute ma gratitude à mes frères, mes soeurs, mes cousins qui m'ont toujours soutenu, avec leurs encouragements, pour aller jusqu'au bout de mes rêves. J'adresse mes profonds remerciements à mes parents: Zakia et Abdelmalek qui m'ont encouragé à faire cette thèse. Merci d'être toujours présent à mes côtés pour me soutenir, m'encourager, me conseiller, et m'aimer... Je leur dédie cette thèse, qui est aussi la leur, car c'est grâce à eux que j'en suis là aujourd'hui.
Je remercie également mes camarades: Deborah, Yacine et Ahmed pour leur aide, et de m'avoir toujours encouragé et donner de l'énergie positive.

Tables des matières

Liste des figures

Liste des Tableaux

Introduction générale

Les ICSs (Systèmes de Contrôle Industriels) modernes sont basés principalement sur des Technologies Opérationnelles (OT) héritées d'une grande variété de Technologies de l'information (IT) (Amin, 2011). Ils remplissent des fonctions vitales dans les systèmes critiques, tels que la distribution d'énergie électrique, la distribution de pétrole et de gaz naturel, le traitement de l'eau et des eaux usées. Ils sont également au cœur des dispositifs médicaux, des systèmes d'alarmes et de la gestion des transports.

Les systèmes de Contrôle et Commande industriels (Industrial Control Systems-ICSs) traditionnels étaient basés principalement sur des équipements mécaniques ou électro-mécaniques et leurs standards étaient bien maîtrisés. Cependant, ces systèmes sont trop coûteux pour les installer ou pour les maintenir. Pour surmonter ce défi, les ICSs ont bénéficié des innovations technologiques dans les domaines des nouvelles technologies de la communication et de l'informatique comme les services basés sur les technologies radio, les systèmes d'exploitation (e.g., Windows), les communications basées sur protocole TCP/IP... etc. En effet, les ICSs contiennent un nombre important des fournisseurs de technologies (e.g. Les systèmes SCADA - Supervisory Control and Data Acquisition) qui sont déployés sur plusieurs industries. Leurs difficultés d'intégration expliquent l'utilisation des technologies d'information et de la communication standards et open source. Non seulement celles-ci sont faciles à installer ou intégrer, mais aussi leurs coûts de développement sont très réduits (Low Cost).

Cependant, ces technologies sont parfois mal adaptées ou, dans certains cas, elles sont utilisées avec leurs vulnérabilités pour des raisons de coûts (utilisation de produits commerciaux disponibles sur le marché -Commercial off-the-shelf- COTS). Ce sont des vulnérabilités ouvertes aux cyberattaques dont le nombre et les compétences augmentent chaque jour (Abdo et al., 2017). En conséquence, de nouveaux risques sont apparus qui pourraient nuire la sécurité innocuité (Safety SAF) et sécurité immunité (Sécurity SEC). La plupart de ces risques n'ont pas été pris en compte lors de la phase de conception. Ces dernières années, les évaluations des risques de cyberattaques dans les systèmes de contrôle industriel (ICSs) sont la partie la plus controversée et subjective. Cela est bien confirmé par des organismes de normalisation tels que l'ISO/IEC (International Organization for Standardization) / International Electrotechnical Commission) ou le NIST(National Institute of Standards and Technology). On peut noter plusieurs similitudes entre la sécurité-innocuité (SAF) et la sécurité-immunité (SEC) en ce qui concerne l'évaluation des risques. Ce que l'on appelle des dangers en SAF, ce sont des menaces à la SEC.

Depuis longtemps, nous nous focalisons sur la SAF, qui est reliée aux pannes accidentelles. Aujourd'hui, la SAF pourrait être menacée par la branche de la SEC par des attaques informatiques. Dans ce cas, toutes les techniques utilisées dans l'étude de la SAF (reliée aux menaces accidentelles) sont remises en question, car nous sommes en face du facteur

humain qui est difficile à modéliser (une menace intentionnelle).
Bien que les deux communautés de SAF et de SEC traitent des risques et partagent le même objectif de protection des infrastructures industrielles, elles travaillent toujours séparément. Pourtant, dans les infrastructures industrielles les exigences et les risques de la SAF et de la SEC convergent et peuvent avoir des interactions mutuelles (Piètre-Cambacèdès, 2010). En effet, les exigences et les risques liés à la SEC peuvent influencer la SAF du système et inversement les exigences et les risques liés à la SAF peuvent influencer la SEC du système. Pour relever ces défis, un cadre commun d'analyse des risques prenant en compte à la fois les aspects de SAF et de SEC est devenu crucial. Il permet de couvrir exhaustivement les risques liés à la SEC et à la SAF et d'identifier leurs interdépendances potentielles.

L'objectif de cette thèse est d'aller dans ce sens et de comprendre l'influence des cyberattaques sur la SAF particulièrement et sur la sûreté de fonctionnement d'une façon générale. Ensuite, de proposer un cadre de travail qui permet d'avoir une gestion efficace et une évaluation optimale des risques ainsi qu'une optimisation des coûts et des ressources. En effet, des modèles plus ou moins complexes sont utilisés pour l'évaluation et la gestion des risques. Ces modèles sont basés surtout sur la théorie de la probabilité (théorie du jeu (Orojloo and Azgomi, 2017a) , chaînes de Markov). Cependant, les risques liés à la cyberattaque ne peuvent pas être uniquement analysés à l'aide de modèles de probabilité classiques. Ceci est dû à deux facteurs :

- D'un côté, le manque de données expérimentales et la difficulté de modéliser les facteurs humains. En conséquence, l'analyse des risques avec des connaissances insuffisantes ou des données imprécises en utilisant des modèles probabilistes génère des modèles ayant de grandes incertitudes. De plus, l'approche de l'analyse des risques est très différente de celle de la SAF, car l'évaluation des risques en matière de SEC comporte plusieurs paramètres subjectifs, par exemple, les motivations de l'attaquant, cela limite l'utilisation de méthodes probabilistes quantitatives (Braband and Schäbe, 2019).
De l'autre côté, les types menaces évoluent d'une manière permanente et rapide et de nouvelles vulnérabilités sont publiées chaque jour, cela doit être accompagné par une évaluation régulière de la cybersécurité. Il est donc très important d'évaluer les niveaux de risque à travers une politique de priorisation des vulnérabilités du ICS en fonction de leur niveau de criticité. Plusieurs travaux ont été publiés dans l'évaluation des risques dans ce sens, qui prennent en compte les risques de vulnérabilité et leurs criticités. À ce propos, le système de notation de la vulnérabilité CVSS (Commun Vulnerabilty Scoring System) (FIR, b) est le plus connu et le plus utilisé.

Dans cette thèse, nous proposons une nouvelle approche orientée processus que nous avons appelé AMDVEC & ER (Analyse des Modes de Défaillance et de Vulnérabilité et de leurs effets et de leur criticité & Évaluation de Risque) , pour une démarche conjointe de la SAF et la SEC des ICSs. La méthodologie AMDVEC & ER offre un cadre de travail qui couvre les aspects de la SEC et de la SAF associés et évalue les scénarios de risque qui conduisent à un événement indésirable avec des problèmes liés à la SAF. Elle peut être appliquée soit dans la conception de nouveaux systèmes sûrs et sécurisés ou dans la phase opérationnelle des systèmes existants pour optimiser et maîtriser leur SAF et leur SEC.

En plus de cette contribution principale, cette thèse intègre d'autres contributions que nous résumons comme suit :

- Un premier système de notation (ICVSS Industrial Control Vulnerability Scoring System) destiné spécialement aux systèmes de contrôles industriels (ICSs) hérité du système de notation classique (CVSS) qui permet d'éviter toutes les ambiguïtés et les limitations du CVSS dans le cas des systèmes industriels. De plus, la caractéristique qualitative et quantitative du nouveau système de notation crée une voie de communication entre les ingénieurs de la SAF et ceux de la SEC, à travers un langage commun.

- Une modélisation qui inclut à fois l'aspect humain et les incertitudes liées à l'analyse des risques des cyberattaques. La théorie des ensembles flous et la logique floue fournit un cadre mathématique plus convenable (Zadeh, 1965a). En fait, l'utilisation des variables linguistiques rend les modèles de logique floue plus similaires au raisonnement humain. Ils permettent d'introduire le facteur humain en incorporant l'opinion des experts dans le modèle via les règles floues. Nous montrons que les modèles logiques flous peuvent être appliqués pour améliorer l'évaluation des vulnérabilités et la prise de décisions en l'intégrant aux métriques de système populaire d'évaluation ou de notation des vulnérabilités CVSS, et afin que les experts ou les ingénieurs puissent établir l'ordre de priorité des risques en fonction de la criticité des vulnérabilités du système.

Cette thèse est organisée comme suit : le chapitre 1 donne les définitions principales, les bases et les standards liés la cybersécurité et les terminologies de la sûreté de fonctionnement. Le chapitre 2 résume l'état de l'art concernant les méthodes d'évaluation des risques dans les ICSs. Le chapitre 3 présente en détail le système de notation de la vulnérabilité le plus populaire (CVSS) et ensuite, le système de notation destiné aux systèmes industriels ICVSS (Industrial Control Vulnerability Scoring System) que nous avons développé. Dans le chapitre 4, la logique floue du Takagi Seguno (TS) est utilisée pour améliorer le système de notation ICVSS pour modéliser les incertitudes liées à décision. Nous présentons aussi dans le même chapitre les résultats comparatifs des deux méthodologies CVSS et ICVSS avec utilisation de la logique floue dans le cas des centrales électriques à eau bouillante (Boiling Water Power Plant BWPP). Dans chapitre 5, la méthodologie AMDVEC & ER qui harmonise l'évaluation SAF/SEC est présentée sur un cas d'utilisation d'un réseau de communication entre mobiles. Dans le dernier chapitre, la conclusion et les futurs travaux sont présentés.

Chapitre 1

Cybersécurité des ICSs : spécificités, enjeux et défis associés

Contents

Ce premier chapitre aborde les nouveaux risques de la cybersécurité liés aux systèmes de contrôle industriels (ICSs) modernes dans différents domaines industriels. Il offre également les principales définitions de la sûreté de fonctionnement, de la sécurité-innocuité et de la sécurité-immunité, leurs similitudes et leurs différences. Ensuite, les spécificités et les exigences des systèmes de contrôle industriels sont précisées. Finalement, nous présentons quelques standards émergents qui traitent la problématique des cyberattaques dans les ICSs.

1.1 Systèmes de contrôle industriels et cyberattaques

1.1.1 Introduction

La cybersécurité des installations industrielles est une préoccupation très importante dans la dernière décennie (Schwab and Poujol, 2018). La fréquence et la gravité des cyberattaques qui visent les infrastructures critiques sont largement augmentées, (par exemple les attaques de Stuxnet en 2010 et de Flame en 2012 (Flaus, 2018)). De plus, de nombreux systèmes informatiques de traitement de l'information (IT) sont victimes d'attaques qui peuvent se propager rapidement et avoir un impact important, comme le Wanacry (Flaus, 2018).

En outre, les experts en sécurité démontrent régulièrement l'existence des vulnérabilités dans les systèmes de contrôle lors de conférences telles que Black Hat ou DefCon (Kriaa, 2016).

Dès les années soixante, les systèmes informatiques ont été employés pour commander des systèmes physiques. Cependant, ces systèmes étaient difficiles à mettre en place et à programmer. Pour cette cause, un nouvel appareil appelé "PLC" a été conçu par Modicon en 1968 (Flaus, 2018). Il rend l'installation du matériel plus facile et permet d'utiliser un langage de programmation plus simple.

Ces systèmes étaient utilisés dans un premier temps pour contrôler les grandes installations. Par la suite, avec la miniaturisation, ces systèmes ont été incorporés dans des systèmes physiques et ont enfin donné naissance à des dispositifs de dimensions compactes ayant une certaine aptitude de traitement et de communication, les systèmes cyberphysiques. Dans de nombreux cas, ces systèmes peuvent se connecter directement sur l'Internet en utilisant les protocoles de communication du monde informatique, ce qui a donné lieu à l'émergence de l'Internet des objets. Les problématiques de sécurité informatique ont donc commencé à se manifester avec une grande acuité. Ce bref rappel historique est essentiel pour expliquer la différence de philosophie entre les mondes de l'informatique et de l'OT (Operational Technology), et pour comprendre la raison pour laquelle le monde de l'OT, qui, au départ, était moins intéressé par les problématiques de sécurité informatique, a finalement été touché par ces problèmes et la raison pour laquelle la menace, qui est désormais bien réelle, ne fait qu'augmenter.

De nombreux industriels ont été touchés par la modernisation et la numérisation de leurs systèmes de contrôle et commande. Ces industries regroupent des fabricants qui produisent des systèmes critiques impactant directement leurs utilisateurs tels que les voitures, les avions, les trains, les implants médicaux, etc. On trouve aussi des industriels qui possèdent de grandes infrastructures telles que des centrales de production d'électricité, des raffineries de pétrole.. etc. Même si elles sont différentes, toutes ces industries partagent aujourd'hui le même défi de protéger leurs systèmes critiques des risques de

cybersécurité qui peuvent engendrer des impacts sur la sûreté de fonctionnement.

1.1.2 Systèmes de contrôle industriels (ICSs)

"Système de contrôle industriel (Industriel Control System - ICS)" est un terme général ou une appellation qui inclut plusieurs systèmes comme :
- les **systèmes de contrôle et d'acquisition de données** SCADA (Supervisory Control and Data Acquisition), généralement utilisés pour des systèmes ayant une large couverture géographique. Ils sont composés de matériel et de logiciels de différents fournisseurs assemblés en système par un intégrateur.
- les **systèmes de contrôle distribués** (Distributed Control System - DCS), ils relèvent en général, d'un seul fournisseur. Les ICSs consistent alors en plusieurs systèmes physiques (e.g., électrique, mécanique, hydraulique, pneumatique) qui doivent ensemble accomplir des tâches et des fonctions industrielles (e.g. chaîne de productions, système de transports, productions d'énergie). Ces ICSs sont utilisés pour contrôler et surveiller les infrastructures critiques telles que les centrales nucléaires, les systèmes de production de pétrole et du gaz.

Généralement, les systèmes de contrôle industriels sont composés d'équipements et systèmes spécialisés ou conventionnels que nous pouvons classer comme suit (Flaus, 2018) :
- Premièrement, un système informatique, proche d'un système conventionnel, (des ordinateurs bureautiques, des serveurs et réseaux classiques, d'imprimantes, des systèmes de stockage) ;
- Deuxièmement, un jeu d'équipements spécialisés qui leur permet de recueillir des mesures, de réagir sur le système physique et de communiquer avec les manipulateurs ; on trouve notamment dans cette catégorie les automates programmables (PLC - Programmable Logic Controller), les systèmes de supervision (e.g. IHM - Interface Homme-Machine, SCADA), des systèmes de diagnostic de maintenances industrielles à distance, les capteurs et les actionneurs.

Le terme "IACS - Industrial Automation Control System" a été suggéré par l'ISA dans les années 2000 et a été adapté sous une forme simplifiée, "ICS", dans le guide 800-82 du NIST (National Institute of Standards and Technology) en 2008. Cette nouvelle appellation rend les termes "DCS" et "SCADA" progressivement obsolètes (Flaus, 2018).

Toutefois, la définition ICS dans la norme CEI 62443 est plus étendue et englobe également les éléments logiciels et matériels qui assurent la bonne fonctionnement du processus industriel comme : SCADA, DCS, HMI, PLC, RTU (Remote Terminal Unit), des appareils électroniques intelligents (IED), des systèmes instrumentés de sécurité (SIS), et les systèmes d'information associés,..., etc. Avec l'augmentation de la connectivité au monde Internet pour des raisons professionnelles, l'ICS a adopté des technologies basées sur Internet et la plupart des protocoles de communication ont été repensés pour fonctionner sur protocole IP. Cette ouverture exposait les composants des ICS ainsi que les protocoles de communication aux cyberattaques présentant un risque plus élevé que les attaques sur les systèmes informatiques traditionnels. PERA (Purdue Enterprise Reference Architecture) (figure 1.1 propose un modèle de référence pour la fabrication intégrée par ordinateur (CIM - Computer-Integrated Manufacturing) (Williams, 1989) qui divise l'architecture d'entreprise en différentes couches basées sur la hiérarchie organisationnelle. Inspirée de PERA, la norme CEI 62264-1 (Commission et al., 2003) propose un modèle pour l'entreprise qui organise l'architecture en cinq niveaux clés, basés sur la hiérarchie

fonctionnelle (Kriaa, 2016)(Brun et al., 2013)(Flaus, 2018) :

- Niveau 0 (Processus physique) : le niveau du bus de terrain est consacré au contrôle (mesure avec les capteurs) et à la commande (avec les actionneurs) du système physique ;

- Niveau 1 (Contrôle local) : le niveau du procédé est dédié à la supervision et à la prise de décision, il permet donc de piloter les équipements de niveau 0. Ce niveau contient des dispositifs qui interviennent directement dans le processus de contrôle industriel comme le PLC et RTU, etc. Ces appareils permettent de lire les mesures des capteurs, exécuter des algorithmes, commander les actionneurs et enregistrer l'état du système physique ;

- Niveau 2 (Supervision) : il comprend les interfaces homme-machine (IHM), les systèmes de contrôle et d'acquisition de données (SCADA) et les systèmes distribués (DCS) ;

- Niveau 3 (Gestion des opérations) : le niveau usine est destiné à la gestion de la production en fonction de la demande d'ateliers (le plus souvent, par le biais d'un système MES - Manufacturing Execution System). Une partie du système de supervision peut aussi se situer à ce niveau (Flaus, 2018).

- Niveau 4 (Entreprise) : le niveau entreprise concerne les fonctions impliquées dans les activités liées à l'entreprise nécessaires afin de gérer l'organisation de la fabrication.

Les dispositifs qui sont directement impliqués dans le processus de contrôle industriel sont particulièrement situés aux niveaux 0, 1 et 2.

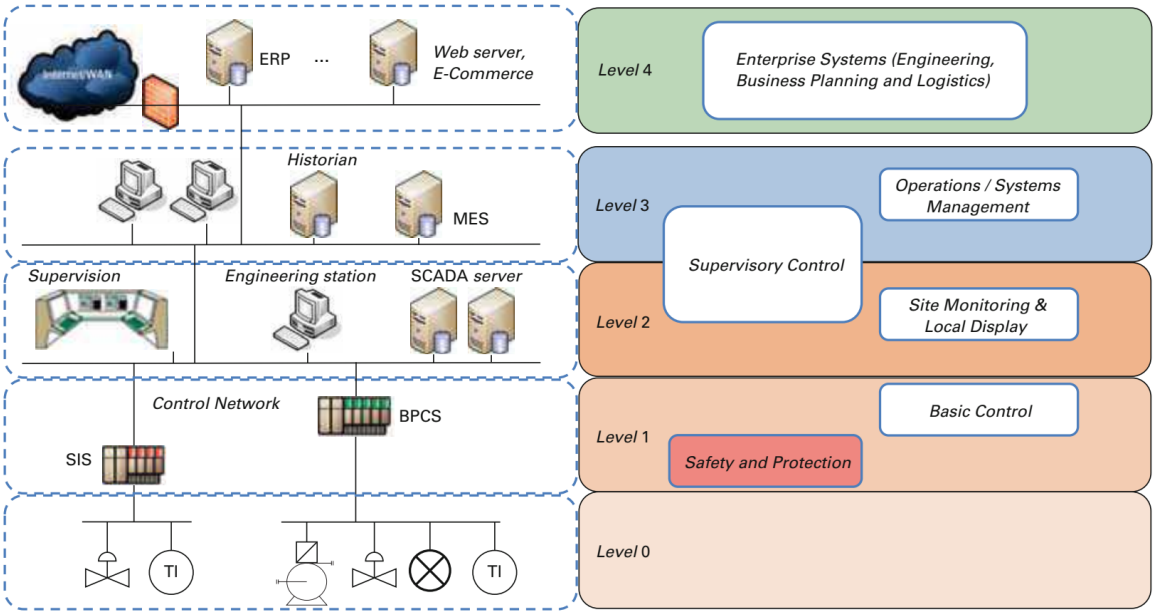


FIGURE 1.1 – Modèle de Purdue de l'architecture d'un ICS (Flaus, 2018).

1.1.3 Comparaison entre les ICSs et les systèmes informatiques classiques (IT- Information Technologies)

Les systèmes de contrôle industriels interagissent avec les systèmes physiques, ce qui crée des limites particulières. Tout d'abord, le système informatique commandant et contrôlant un système physique, il n'est pas tolérable d'arrêter brutalement l'exécution d'un programme sans prendre en considération le processus de production ou l'équipement. Il faut tout d'abord remettre le système dans un état sûr.

Par ailleurs, les mises à jour logicielles sur ICS ne peuvent pas toujours être effectuées d'une façon continue. Ces mises à jour doivent être soigneusement testées par le fournisseur de l'application de contrôle industriel et l'utilisateur final de l'application avant d'être installées. De plus, le propriétaire de l'ICS doit planifier les interruptions d'ICS plusieurs jours / semaines à l'avance. Également, les systèmes de contrôle industriels ont une durée de vie de plus ou moins 20 ans (Fabro et al., 2009), car le temps et les ressources nécessaires pour un changement sont assez importants. Enfin, la plupart des fournisseurs industriels ont développé leurs technologies avant que les cyberattaques apparaissent. Le tableau 1.1 présente une synthèse plus détaillée de ces différences.

1.1.4 Environnement d'un ICS

Dans cette section, nous présentons l'environnement et, par voie de conséquence, les menaces qui peuvent affecter un système pendant toute sa durée de vie. Le cycle de vie d'un système comprend deux grandes phases : le *développement* et l'*utilisation*. La phase de développement comporte toutes les activités, depuis la présentation du concept initial pour l'utilisateur jusqu'à la décision envers le système. Celui-ci ayant passé une série de tests de vérification et de validation est prêt à fournir le service dans l'environnement de l'utilisateur. Pendant la phase de développement, le système interagit avec l'environnement de développement. Des fautes de développement peuvent être introduites dans le système par l'environnement. L'environnement de développement d'un système est constitué :

1. d'un monde physique avec ses phénomènes naturels,

2. de développeurs humains, dont certains manquent peut-être de compétences ou ont des objectifs malveillants,

3. d'outils de développement : logiciels et matériels utilisés par les développeurs afin de les aider dans *le processus de développement*,

4. d'installations de production et de tests.

La phase d'utilisation d'un système commence lorsque le système est accepté pour une utilisation et commence la prestation de ses services aux utilisateurs. L'utilisation consiste en une alternance de périodes de prestation de services corrects, de pannes de service et d'arrêt de service.

Une *panne de service* est causée par une défaillance du service. C'est la période pendant laquelle un service incorrect (y compris aucun service du tout) est fourni à l'interface de service. Un arrêt de service est un arrêt intentionnel de service par une entité autorisée. Les actions de **Maintenance** peuvent avoir lieu durant la phase d'utilisation. Pendant cette phase, le système interagit avec son environnement d'utilisation et peut être affecté négativement par les défauts qui en proviennent. L'*environnement d'utilisation* est composé des éléments suivants :

1. le monde physique avec ses phénomènes naturels ;

2. les administrateurs (y compris les mainteneurs) : entités (humains ou autres systèmes) qui ont le pouvoir de gérer, modifier, réparer et utiliser le système ; certains intervenants autorisés peuvent manquer de compétences ou avoir des objectifs malveillants ;

3. les utilisateurs : entités (humains ou autres systèmes) qui reçoivent le service du système à leurs interfaces d'utilisation ;

4. les fournisseurs : entités (humaines ou autres systèmes) qui fournissent des services au système au niveau de ses interfaces d'utilisation ;

5. l'infrastructure : les entités qui fournissent des services spécialisés au système, comme les sources d'information , les liens de communication, les sources d'énergie, la circulation de l'air de refroidissement, etc.

6. les intrus : entités malveillantes (humains et autres systèmes) qui tentent de surpasser toute autorité à laquelle elles pourraient être assujettis; de modifier le service ou l'arrêter; de modifier la fonctionnalité ou la performance du système ou accéder à des informations confidentielles. Les exemples comprennent les pirates informatiques, les vandales, les initiés corrompus, les agents de gouvernements ou d'organisations hostiles et les logiciels malveillants.

1.1.5 Exemples d'incidents et d'attaques sur les ICSs

En 2007, l'Idaho National Laboratory a effectué le test de l'attaque Aurora afin de démontrer comment une cyberattaque peut détruire les composants physiques d'un réseau électrique. L'expérience a utilisé un programme informatique pour ouvrir et fermer rapidement les disjoncteurs d'un générateur diesel déphasé par rapport au reste du réseau et le faire exploser. Cette vulnérabilité est appelée "vulnérabilité Aurora".

Cette vulnérabilité est particulièrement préoccupante car la plupart des équipements du réseau électrique supportent l'utilisation de Modbus et d'autres protocoles de communication hérités qui ont été conçus sans tenir compte de la sécurité. En tant que tels, ils ne prennent pas en charge l'authentification, la confidentialité ou la protection contre les rediffusions, ce qui signifie que tout attaquant qui peut communiquer avec l'appareil peut le contrôler et utiliser la vulnérabilité Aurora pour le détruire. Cette expérience révèle une vulnérabilité qui est particulièrement préoccupante. Une deuxième attaque très réputée est le virus Stuxnet, découvert pour la première fois en 2010, qui pourrait être en cours de développement depuis au moins 2005. Stuxnet vise les systèmes SCADA (Supervisory Control and Data Acquisition) et est soupçonné d'être responsable des dommages importants causés au programme nucléaire iranien. Bien qu'aucun pays ne reconnaisse ouvertement sa responsabilité, le vers est considéré comme une cyber-arme construite en collaboration par les États-Unis et Israël (Nakashima and Warrick, 2012)(Technica, 2012).

Stuxnet visait spécifiquement les automates programmables (PLC), qui permettent l'automatisation de processus électromécaniques tels que ceux utilisés pour contrôler les machines et les processus industriels, notamment les centrifugeuses à gaz pour la séparation des matières nucléaires. Plus précisément, Stuxnet a été introduit dans l'environnement cible via un lecteur connecté à une prise USB. Le ver s'est propagé alors dans le réseau informatique en exploitant plusieurs vulnérabilités de Windows (Naraine et al., 2010), puis à rechercher le logiciel Step7 de Siemens utilisé pour programmer les PLC. Stuxnet a modifié la bibliothèque du logiciel Step7 qui établit la communication avec le PLC pour introduire du code malveillant dans le programme transmis (Gross, 2011)(Falliere, 2010). En 2017, une toute dernière attaque qui mérite d'être mentionnée est l'attaque connue sous le nom "Triton" qui a ciblé les automates de type Triconex fabriqués par Schneider Electric. Le malware Triton a ciblé les systèmes de protection SIS (Safety Instrumented System) d'une des unités industrielles pétrolières en Arabie Saoudite. Dans cette situation et en cas de faute de contrôle survenant par accident, ou provoquée par une autre attaque, les conséquences pourraient être dramatiques. Un bogue a permis de découvrir l'attaque. La société de sécurité informatique Symantec a affirmé que le malware, exploitait une vulnérabilité des ordinateurs fonctionnant sous le système d'exploitation Microsoft Windows. Plusieurs autres attaques ont été menées dans la dernière décennie. Le tableau 1.2 montre les plus célèbres.

Catégorie	Système Informatique (IT)	Système de contrôle industriel (ICS)
Exigences en performance	-Non temps réel. -Débit élevé est exigé. -Délai et une gigue élevée peuvent être acceptables. -Interaction d'urgence moins critique.	-Temps réel. -Débit modeste est acceptable. -Retard élevé et / ou la gigue n'est pas acceptable. -Réponse à l'urgence humaine et autre l'interaction est critique.
Exigences en Disponibilité (Fiabilité)	-Les réponses telles que le redémarrage sont acceptables. -Le manque de la disponibilité peut souvent être toléré en fonction des besoins opérationnels du système.	-Les réponses telles que le redémarrage peuvent ne pas être acceptables en raison des exigences de disponibilité du processus. Les exigences de disponibilité peuvent nécessiter des systèmes redondants Les arrêts doivent être planifiés des jours et des semaines en avance.
Exigences en gestion des risques	-Gérer les données. -La confidentialité et l'intégrité des données sont primordiales. -La tolérance aux pannes est moins importante - les temps d'arrêt momentanés ne constituent pas un risque majeur. -L'impact majeur du risque est le retard des opérations commerciales.	-Contrôler le processus physique, -La sécurité humaine est primordiale, suivie par la protection des processus. -La tolérance aux pannes est essentielle, et même probablement les temps d'arrêts momentanés ne sont pas acceptables -Les principaux impacts sont environnementaux, perte de vie et des équipements de la production.
Système d'exploitation	-Les systèmes sont conçus pour être utilisés avec des systèmes d'exploitation standard. Les mises à jour sont simples avec la disponibilité d'outils automatisés.	-Les systèmes d'exploitation sont variés (selon le fournisseur), souvent sans capacités de sécurité intégrées. - Les modifications logicielles doivent être effectuées avec soin, généralement par les fournisseurs de logiciels, en raison d'algorithmes de contrôle spécialisés et leurs matériels spécifiques.
Contraintes de ressources	-Les systèmes ont suffisamment de ressources pour prendre en charge l'ajout d'applications telles que des solutions de sécurité (ex. Cryptage), protocoles de communication standard, réseaux principalement câblés et avec des réseaux sans fil.	-Les systèmes sont conçus pour prendre en charge le processus industriel et ne peuvent pas avoir des ressources de mémoire et de calcul pour prendre en charge l'ajout des solutions de sécurité. -De nombreux protocoles de communication. -Plusieurs types de supports de communication utilisés y compris sans fil (radio et satellite).
Cycle de vie des composants	-Durée de vie de 3 à 5 ans	-Durée de vie de l'ordre de 15 à 20 ans

TABLEAU 1.1 – Différences entre les systèmes IT et ICS

Attaque	Année	Description	Vecteur	Conséquences
Triton	2017	Attaque des automates de sécurité SIS(Triconex)	Remote Access Trojan (RAT)	Arrêt de l'installation, catastrophe industrielle potentielle
WannacryPetya	2017	Attaque massive touchant plus de 300 000 postes utilisant une faille de Windows et réalisant un chiffrement des données et demandes de rançon	Virus se propageant via une faille de Windows (EternalBlue)	Pertes financières (rançon), arrêt de production
Lappeenranta Building Attack	2016	Attaque de l'installation de chauffage d'un immeuble en Finlande (géré par Valtia)	DDos	Perte du chauffage
German SteelMill CyberAttack	2015	Prise du contrôle du système de pilotage d'un haut fourneau qui a généré des dommages massifs	Spear Phishing emailet Trojan	Dommages physiques
DragonFly	2014	Attaque contre des compagnies d'énergie en compromettant l'équipement ICS	Remote Access Trojan(RAT) : Havex/Energy bearEmail (pdf), Watering holeattack	Sabotage
Sandworm	2014	Attaque visant des logiciels de GeneralElectric et Siemens	Zero day vulnerability Windows CVE 2014 4114(OLE exec)	Sabotage
Telvent Canadaattack	2012	Accès aux outils d'administration du système de commande	Malware	Vol d'informations d'un logiciel SCADA

TABLEAU 1.2 – Attaques les plus connues sur les ICSs (Flaus, 2018)

1.2 Cybersécurité

1.2.1 Définitions

La cybersécurité concerne la sécurité informatique des systèmes connectés à l'Internet et appartenant au cyberespace. Les cyberattaques sont des attaques informatiques, qui s'ajoutent aux menaces existantes pour les systèmes d'information. Généralement, la cybersécurité porte sur la sécurité informatique des systèmes connectés à l'internet. Pour préciser le cadre des travaux, on introduit les principales définitions relatives à la cybersécurité.

1. **Système d'information :** le système d'information (IS) est un ensemble de ressources matérielles, logicielles, et humaines d'organisation qui permet de rassembler, traiter, sauvegarder, et distribuer de l'information.

2. **Biens ou actifs (Assets) :** un actif est un composant ou une ressource du système examiné, qui peut être de type matériels, logiciels, réseaux de communications (routers, switch,...,etc.), des données (fichiers, une base de données, mot de passe).

3. **Menace :** toute personne, circonstance ou événement susceptible de causer des pertes et des dommages à l'organisation ou avoir un impact négatif sur les fonctionnements des actifs, sur les personnes par le biais d'un système d'information via un accès non autorisé, la destruction, la divulgation, la modification des informations et/ou le refus de service (Stouffer et al., 2011).

4. **Vulnérabilité :** la vulnérabilité est toute faiblesse dans un système d'information qui peut être exploitée par un adversaire. Ces faiblesses proviennent de la conception, de l'intégration ou de l'exploitation d'un système.

5. **Attaque :** est une action malveillante visant à la violation d'un ou plusieurs attributs de sécurité informatique ou des équipements. Une attaque représente la manifestation d'une menace, et nécessite l'exploitation d'une vulnérabilité.

6. **Cyberespace :** un domaine global dans l'environnement de l'information constitué d'un réseau interdépendant des infrastructures de systèmes d'information y compris l'Internet, les réseaux de télécommunications, les systèmes informatiques, microprocesseur embarqué et contrôleurs (csr,).

7. **Cyberattaque :** une attaque, via le cyberespace, visant une entreprise ou une infrastructure dans le but de perturber, de mettre hors service, de détruire ou de contrôler malicieusement un environnement ou une infrastructure informatique (ou de calcul) ; ou de détruire l'intégrité des données ou de voler des informations contrôlées .

1.2.2 Attaques dans les ICS

Caractéristiques et conséquences des attaques dans les ICSs

Dans cette section, nous nous intéressons aux caractéristiques principales des menaces, vulnérabilités et attaques potentielles qu'un ICS peut rencontrer. Nous verrons que pour chaque attaque, on peut identifier son type attaquant (source), sa technique d'attaque (méthode), sa cible, et ses conséquences potentielles (résultats) voir la figure 1.2.

Acteurs d'attaque :

En comprenant mieux les capacités, les intentions et les opportunités de l'attaquant, nous pouvons mieux concevoir les défenses d'un ICS. Les types d'acteurs de la menace peuvent être divisés en trois catégories (ics,) :

- Groupe 1 : Menaces publiques (Mainstream)

Le groupe 1 est, historiquement, le groupe de menaces le plus important, bien qu'il ne soit généralement pas bien organisé. La motivation des acteurs de cette catégorie de groupe peut varier, mais traditionnellement, la motivation est liée à la notoriété ou à la célébrité. L'attaque d'un système est effectuée pour attirer l'attention sur soi.

- Groupe 2 : Menaces organisées

Le groupe 2 est constitué de menaces plus organisées. Elles sont généralement menées par des groupes particuliers. Elles peuvent être de nature financière pour venger, pour voler des secrets commerciaux ou attirer l'attention sur une cause (hacktivistes). Leurs attaques sont plus structurées et plus sophistiquées que celles du groupe 1, mais il n'est pas rare que les menaces du groupe 2 comprennent des membres, des capacités ou des compétences que l'on trouve traditionnellement dans les environnements du groupe 1.

- Groupe 3 : Menaces des terroristes et les États nations

Les objectifs des attaques de ce groupe 3 sont de perturber, terroriser ou éliminer des aspects majeurs de la société. L'impact ou les conséquences d'un attentat du groupe 3 pourraient être catastrophiques.

Techniques de l'attaque

Nous présentons les méthodes et/ou techniques les plus utilisées par les attaquants pour pénétrer les ICS :

1. **Exploit jour zéro :** c'est un exploit qui a pour but de trouver des vulnérabilités qui ne sont pas encore connues par la communauté et pour lesquelles aucune contre-mesure ou atténuation n'a encore été développée (vulnérabilité de type " zero-day ").

2. **Phishing :** c'est un E-mail contenant des fichiers malveillants ou des liens vers des sites web malveillants.

3. **Flooders :** sont des programmes malveillants utilisés pour surcharger la communication normale de l'Internet/du réseau et diminuer les performances globales du système infecté. On trouve deux types de Flooder
   - *Déni de service (DoS) :* cette technique d'attaque vise à rendre les services ou des ressources (réseau, CPU) informatiques indisponibles.
   - *Attaque MITM (Man In The Middle) :* Il s'agit d'attaque qui intercepte la communication entre deux parties et manipule les données échangées afin de se faire passer pour l'une des parties. L'attaque la plus fréquente est l'utilisation d'un hotspot WiFi comme moyen de se connecter au même réseau que la cible. Ensuite, en utilisant les faiblesses du protocole de communication et les dispositifs de routage, l'attaquant

oblige les communications à transiter par son poste et à la fin il peut décrypter toute la communication

4. **Injection d'attaque :** les injecteurs sont des outils ou des programmes qui sont utilisés pour injecter un virus dans le mémoire ou injecter un exploit. Les injecteurs de réseaux font partie de cette catégorie où il s'agit d'injection d'une trame des données spécifiques. Dans le cas des systèmes ICS, les injecteurs comprennent tout programme capable d'injecter des trames fabriquées ou modifiées (des commandes et des mesures erronées).

5. **Ingénierie sociale :** cette méthode utilisée consiste à obtenir des informations privilégiées d'un initié sur le système ou les réseaux informatiques ciblés.

6. **Malwares :** Ce sont des logiciels malveillants conçus intentionnellement pour causer des dommages à un ordinateur, un serveur, un client ou un réseau informatique. Cette nomination regroupe toutes les formes de : virus, cheval de Troie, rançongiciel (ransomware), ver informatique, espiongiciel (spyware), pubiciel (adware), alarmiciel (scareware), les rootkits, les backdoors et les botnets.

7. **Bombe logique :** une bombe logique est un programme malveillant dans une application légale. Ce programme pourrait provoquer un crash de l'application. Dans le cas d'une application critique cela peut causer des conséquences catastrophiques.

Cible de l'attaque

Dans un ICS, la bonne santé du système tels que les capteurs et actionneurs (niveau 0 : terrain), PLC (niveau 1 : contrôle local ou de base) , IHM (niveau 2 : contrôle de supervision) et IT (Niveau 3 et 4 : gestion des opérations et Enterprise Business Systems) et les réseaux des communications sont vitaux, car les réseaux travaillent ensemble et contribuent au bon fonctionnement du système. L'attaque peut cibler un ou plusieurs de ces systèmes.

Phases du cycle de vie d'une cyberattaque

Tout comme un charpentier utilise une variété d'outils pour construire une maison, un acteur de menace des ICSs utilise également un certain nombre d'outils et de techniques différents pour exécuter une attaque. Des outils spécifiques sont conçus pour chaque phase spécifique du cycle de vie de l'attaque. Les phases du cycle de vie d'une cyberattaque comprennent :

1. reconnaissance/ciblage ;

2. l'évaluation de la vulnérabilité ;

3. attaque / pénétration.

Conséquences potentielles

Cette catégorie décrit les résultats à la fin de l'attaque. Une attaque peut entraîner l'échec engendrant trois types de conséquences du point de vue contrôle :

- *Perte de supervision :* Dans ce cas, l'opérateur perd la supervision du processus (par exemple, l'IHM affiche de fausses mesures du processus). L'opérateur ne peut pas savoir si c'est le processus qui est toujours en fonctionnement nominal ou s'il est en panne. En général, l'opérateur prend des décisions sur la base des informations fournies par le système de supervision afin de garantir le bon fonctionnement et la sécurité du système. En effet, en exploitant la vulnérabilité, l'attaquant pourrait changer ou fabriquer les mesures des capteurs, modifier la configuration de l'équipement et désactiver les fonctions de sécurité en lançant l'attaque MITM (Morris et al., 2015).

- *Perte de commande :* Dans ce cas, l'opérateur est capable de voir et d'observer le processus, mais il perd la capacité de le contrôler (par exemple, une attaque de type "MITM" peut intercepter et modifier les commandes envoyées par l'opérateur à un appareil de terrain).

- *Déni de service Dos :* Cela inclut tout débordement qui consomme toutes les ressources, que ce soit en cycles de CPU ou en mémoire ou en bande passante de communications, et par conséquent, le service ou la fonction devient indisponible.

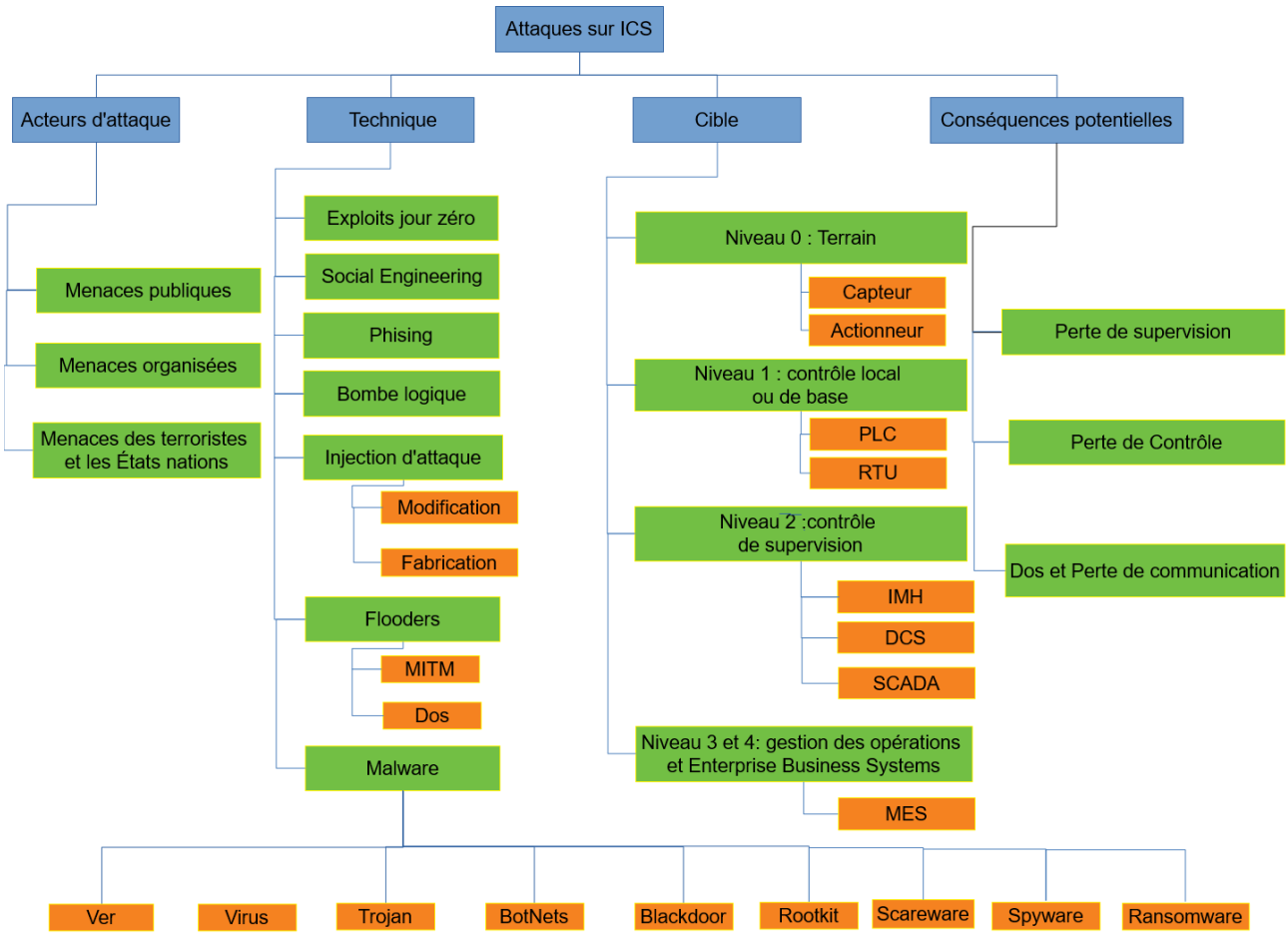


FIGURE 1.2 – Taxonomie des attaques des ICSs

Après avoir introduit les systèmes de contrôle industriels et les risques liés à la cybersécurité, nous allons nous intéresser aux différents aspects de la sûreté et de la sécurité.

1.3 Sécurité-innocuité et sécurité-immunité d'un système

1.3.1 Différence entre Dangers et Menaces (Hazard vs. Thread)

Les dangers et les menaces sont deux éléments distincts, mais ils sont liés. Les dangers sont considérés comme des situations qui présentent des périls inhérents et connus. La défaillance d'une pièce électronique qui fait déborder une chambre remplie d'acide est un exemple de danger. En général, les dangers font partie de la sécurité-innocuité. Dans ce cas, nous avons un historique des données éprouvées sur les défaillances d'équipement, et nous pouvons calculer des probabilités sur des événements indésirables qui peuvent se produire. Dans certains cas, nous pouvons calculer le temps moyen qu'il faudra pour qu'un système ou un appareil tombe en panne dans un environnement dans lequel il se trouve. Mais les données utilisées pour ce faire sont basées sur un comportement prévisible. Les menaces, par contre, ne sont pas prévisibles. Elles relèvent de la sécurité-immunité. Les cyberattaques, la météo, les animaux qui mâchent des câbles ou les arbres qui tombent sont autant d'exemples de menaces. Dans ce cas, nous n'avons pas de données ou d'informations précises pour nous aider à déterminer quand un évènement se produira. Pour les menaces humaines, cela peut être plus difficile, car nous ne pouvons pas généralement définir la valeur combinée qui définit la menace (les compétences d'attaquants, l'ensemble des conditions qui doivent être remplies pour qu'un adversaire soit sûr que son attaque soit menée avec succès , les motivations de l'attaque). La sécurité-innocuité et la sécurité-immunité jouent un rôle important dans la résilience et la fiabilité des ICSs. Les deux sont complémentaires, mais les disciplines elles-mêmes sont différentes.

Dangers (SAF)	**Menaces (SEC)**
Dangers connus et bien compris ; Dangers prédictibles basés sur les historiques des données ; Probabilité d'incident calculable.	Menaces pas bien comprises ; Ne sont pas prédictibles ou prédictibles difficilement.

TABLEAU 1.3 – Différence entre Dangers et Menaces (Hazard vs Thread)

Aujourd'hui, de nombreux travaux mettent en évidence les cyberattaques contre les ICSs. De nouveaux logiciels malveillants spécifiques aux secteurs du ICS sont régulièrement en création. Certaines de ces cyberattaques sont assez sophistiquées et nécessitent une grande connaissance du système. En effet, nous entrons peut-être dans une nouvelle époque où la sophistication des cyberattaques atteint un niveau élevé.

1.3.2 Terminologies de la sûreté de fonctionnement

Les définitions des termes anglais **sécurité-innocuité** (SAF) (se trouvent dans certains ouvrages sous le nom **sûreté**) et **sécurité-immunité** (SEC) varient selon les communautés. C'est pour la raison qu'il est important de clarifier les termes utilisés dans ce manuscrit. Par conséquent, nous utiliserons les définitions de "Avizienis" (Avizienis et al., 2004), sachant que les termes *sûreté* et *sécurité* n'ont pas les mêmes définitions dans la communauté d'énergie nucléaire et dans la communauté génie électrique (Kriaa, 2016) :

La sûreté de fonctionnement est définie comme l'aptitude à offrir un service avec une confiance prouvée ou justifiée. Cette dernière est définie comme une dépendance acceptée, implicitement ou explicitement. La dépendance d'un système envers d'autres

systèmes est définie comme l'influence potentielle ou réelle de la sûreté de fonctionnement de ces systèmes sur le système étudié. La sûreté de fonctionnement peut être vue selon des propriétés différentes, mais complémentaires, qui permettent de définir ses attributs :

- **La disponibilité** du système est définie comme la capacité à être prêt à l'utilisation.
- **La fiabilité** du système est définie comme sa capacité d'assurer la continuité de son service.
- **La sécurité-innocuité (en anglais Safety)** d'un système est définie comme l'assurance de l'absence de conséquences catastrophiques pour l'environnement et les personnes.
- **La confidentialité** d'un système est définie comme la non-divulgation de l'information sans une autorisation.
- **L'intégrité** d'un système est définie comme l'assurance de non-altération ou non-modification inappropriée de l'information.
- **La Maintenabilité** d'un système est définie comme l'aptitude aux réparations et aux évolutions.
- **La sécurité immunité (en anglais Security)** est définie comme la combinaison de la confidentialité, de l'intégrité et de la disponibilité envers des actions autorisées.
- On dit qu'**un service correct** est délivré par un système seulement s'il réalise la fonction définie par le concepteur autrement on dit il y a *une défaillance* du service ou *une panne* du service. Toutefois, on dit souvent simplement *défaillance*.

On parle de service défaillant lorsque celui-ci ne respecte plus les spécifications fonctionnelles. La transition d'un service défaillant à un service correct est obtenue par *la restauration* du service. Les modes de défaillances sont définis selon des formes de déviation du service correct. Le système peut comporter plusieurs fonctions élémentaires, une panne de service ou plusieurs services capables d'assurer ces fonctions peuvent conduire le système dans *un mode dégradé* dans lequel le système peut encore assurer un sous-ensemble du service délivré. La spécification permet d'identifier plusieurs de ces modes dégradés, par exemple, un service lent, un service limité, un service d'urgence, etc. Ici, on dit que le système a subi une défaillance partielle de sa fonctionnalité ou de sa performance.

1.3.3 Entraves à la sûreté de fonctionnement

Les attributs de sûreté de fonctionnement peuvent être mis à mal par des entraves. Une entrave est définie comme une circonstance indésirable. Ainsi, les attributs jouent le rôle de la cause et de la conséquence de la non-sûreté de fonctionnement. Par la suite, nous donnons les principales définitions de ces entraves (Avizienis et al., 2004) :

- **Erreur :** par définition si un service est une séquence des états externes du système, une panne de service signifie qu'au moins un (ou plusieurs) état externe du système s'écarte de l'état du service correcte. Cet écart est appelé une **erreur**.

- **Faute :** La cause jugée ou supposée d'une erreur est appelée une faute. Les fautes peuvent être internes ou externes à un système. La présence préalable d'une vulnérabilité est nécessaire pour qu'une faute externe provoque une erreur éventuellement ou un défaut ultérieur. Dans la plupart des cas, une faute provoque d'abord une erreur dans l'état de service d'un composant qui fait partie de l'état interne du système et l'état externe n'est pas immédiatement affecté.

Pour cette raison, la définition d'une *erreur* est la partie de l'état total du système qui peut conduire à sa *défaillance* ultérieure. Il est important de noter que de nombreuses *erreurs* n'atteignent pas l'état externe du système et par conséquent ne provoquent pas une défaillance. Une faute est active lorsqu'elle provoque une erreur, sinon elle est dormante. **Une défaillance** survient lorsque le système délivre un service incorrect.

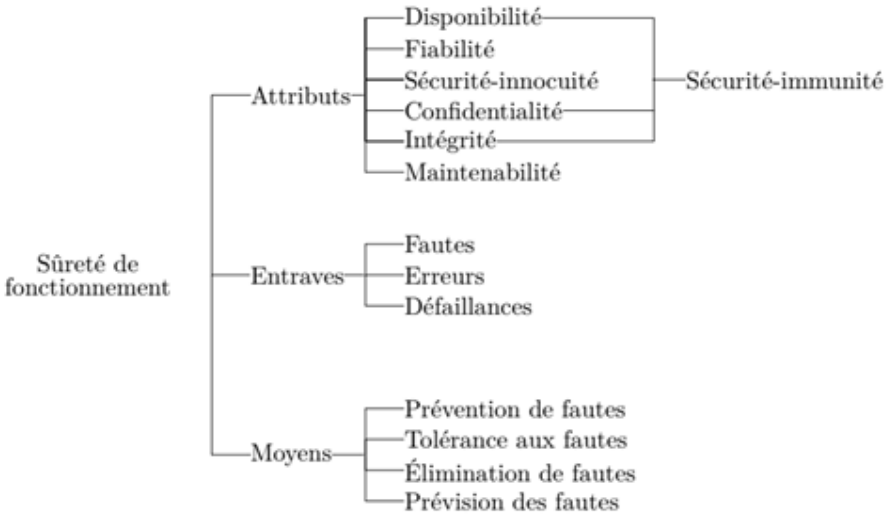


FIGURE 1.3 – Arbre de la sûreté de fonctionnement (Avizienis et al., 2004).

Relation entre les défauts, les erreurs et les défaillances

Lorsqu'une faute est activée, celle-ci va produire une erreur qui va se propager pour engendrer de nouvelles erreurs. Lorsque cette propagation d'erreur affecte le service délivré par le système, celle-ci va produire une défaillance. Si le système contient plusieurs composantes, l'enchaînement de ces entraves crée la chaîne fondamentale suivante :

$$\ldots \Longrightarrow \text{défaillance} \Longrightarrow \text{faute} \Longrightarrow \text{erreur} \Longrightarrow \text{défaillance} \Longrightarrow \ldots$$

1.3.4 Taxonomie des fautes

Toutes les fautes qui peuvent affecter un système pendant sa durée de vie sont classées selon huit points de vue de base, conduisant aux classes de défauts élémentaires, comme le montre la figure 1.4.
Dans la suite, nous ne nous intéressons qu'aux fautes malveillantes.

Fautes malveillantes

Des défauts malveillants d'origine humaine sont introduits dans le but de modifier le fonctionnement du système en cours d'utilisation. À cause de l'objectif, la classification

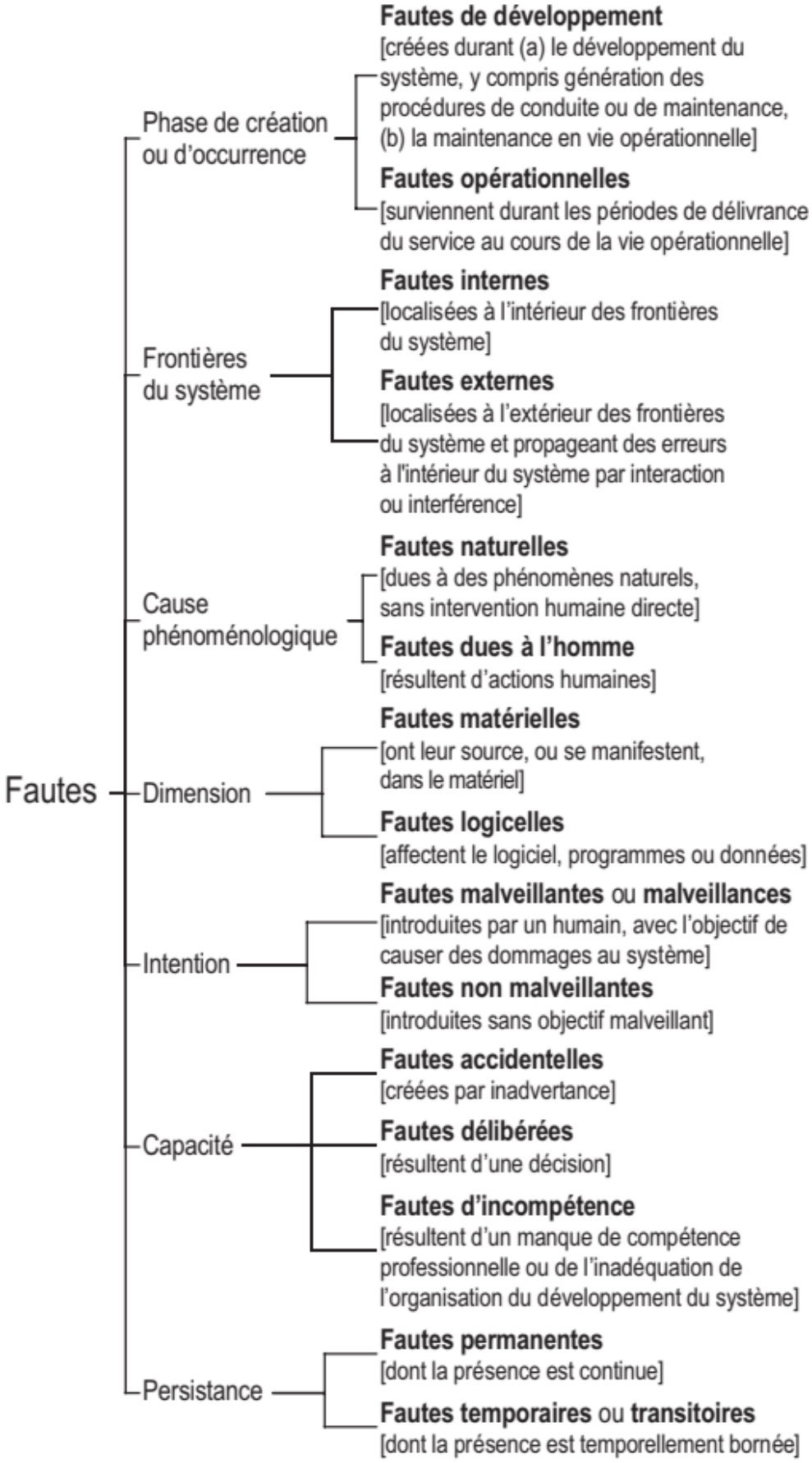


FIGURE 1.4 – Classes de fautes élémentaires (Arlat et al., 2006).

selon l'intention et la capacité n'est pas applicable. Les objectifs de ces fautes sont les suivants : 1) d'interrompre ou d'arrêter le service, causant ainsi un déni de service; 2) d'accéder à des informations confidentielles; 3) de modifier incorrectement le système.

Elles sont regroupées en deux classes :

- **Les fautes de logique malveillante :** lorsqu'une portion de système est conçue dans le but d'arrêter le service; de provoquer des dégâts (bombe logique), ou d'augmenter la chance de futures intrusions (une vulnérabilité créée volontairement) dans ce cas on parle de **logique malveillante**. Cette dernière peut être injectée dès la phase de conception (par un concepteur malveillant), la phase d'utilisation ou la phase opérationnelle (exemple installation d'un logiciel contenant un virus.
  Les fautes de logique malveillante englobent les fautes de développement (voir les colonnes 5 et 6 sur la figure 1.6) telles que *les chevaux de Troie, les bombes logiques* ou *les bombes à retardement* et *les trappes*, ainsi que les fautes opérationnelles (voir la colonne 25 sur la figure 1.6) tels que *les virus, les vers* ou *les zombies*.

- **Attaques ou Tentatives d'intrusion :** Ce sont des défauts externes opérationnels (voir les colonnes 22 et 24 sur la figure 1.6) qui provoque une faute d'interaction malveillante visant à enfreindre un ou plusieurs attributs de la SEC. Elle est considérée comme une faute externe créée avec l'intention de provoquer des dégâts, incluant les attaques lancées par des outils automatiques (vers, virus).
  En outre, une **intrusion** est définie comme le résultat d'une attaque qui a réussi à exploiter une faute interne **(vulnérabilité)**.

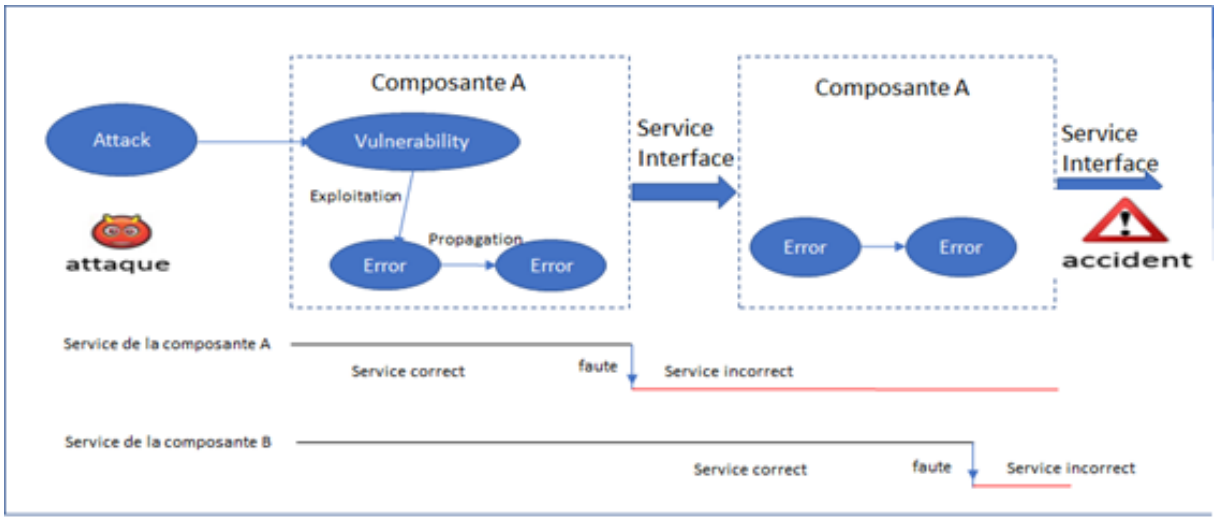


FIGURE 1.5 – Exploitation de la vulnérabilité par une attaque.

1.3.5 Sécurité-immunité (SEC)

La sécurité-immunité vise à assurer la sécurité de systèmes contre les fautes malveillantes (ou malveillances). Ces fautes pourraient survenir lors de la conception ou de l'utilisation. Des attributs plus spécifiques peuvent s'ajouter aux trois attributs principaux (Confidentialité, Intégrité, Disponibilité) et constitué également des objectifs de sécurité-immunité :

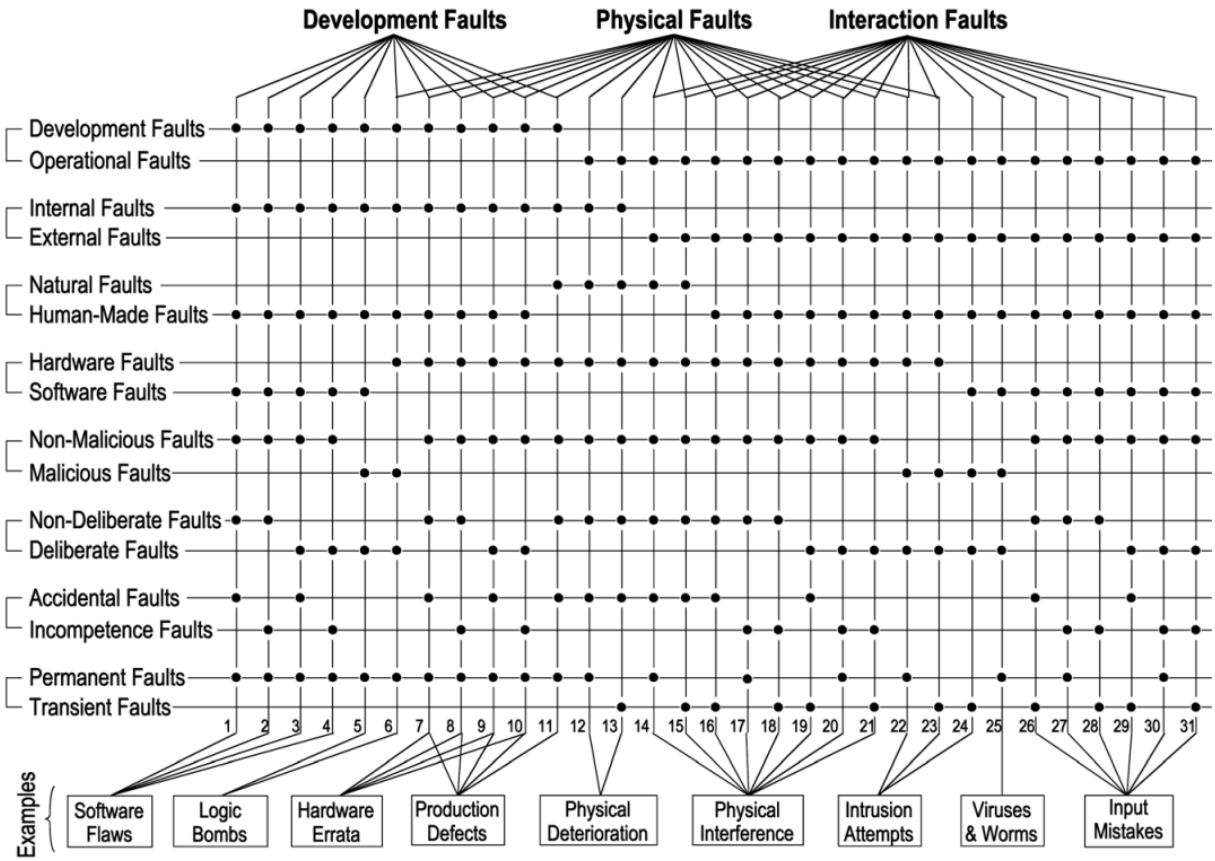


FIGURE 1.6 – Classes de défauts combinés (Avizienis et al., 2004).

- possibilité d'identifier le responsable d'une action donnée pour assurer sa traçabilité de toute infraction à la sécurité conduit à l'**Imputabilité(Accounting)**. P exemple un processus de suivi (traking) de l'activité des utilisateurs et qui enregistre ces activités dans des journaux (logs).

- irréfutabilité d'une action ayant eu lieu conduit à la **Non-répudiation** . Par exemple : La non-répudiation empêche la personne qui envoie le message de démentir avoir envoyé le message dans l'avenir. Un mécanisme qui permet d'assurer de la non-répudiation est la signature digitale.

1.4 Principales mesures de cybersécurité

L'impact des spécifications est direct sur la conception des ICSs. Ces spécifications plus sécurisées sont parfois très bénéfiques **dans cette sécurisation**. Dans cette section, nous allons présenter les principales mesures mises en place dans le cadre de la cybersécurité, cette liste est non exhaustive.

1.4.1 Cryptographie

Cette mesure est considérée comme l'une des plus importantes dans la cybersécurité. La cryptographie permet d'assurer l'intégrité, la confidentialité, l'authentification des informations grâce aux fonctions hachages, de scellement, de chiffrement et enfin les mécanismes de signature respective. Cependant, ces mécanismes posent parfois quelques

problèmes. En effet, le mécanisme de chiffrement des communications dans les automates programmables est utilisé pour assurer la *confidentialité* or cette utilisation peut consommer beaucoup de ressources et ajouter une nouvelle charge, en respectant les contraintes de temps réel et **déterminisme** sur les actions/réactions pourrait être une tâche très compliquée. De plus vérifier l'*intégrité* du *firmware* du programme applicatif et celle des données d'un équipement doit se faire à travers la récupération du contenu de sa mémoire. Dans le cas des automates programmables, cela est très difficile, car les équipements d'aujourd'hui **n'embarquent** pas la solution nécessaire pour le faire. Concernant le contrôle d'*authentification*, celui-ci est possible malgré les ressources limitées des équipements. D'ailleurs, il existe certains protocoles de communication (par exemple, DNPSec, IEC 61850, OPC) qui permettent la mise en oeuvre de contrôle de l'authentification. Enfin, il est nécessaire d'assurer l'authenticité et l'intégrité des *firmware*; des logiciels; des programmes applicatifs qui sont téléchargeables sur internet. La plupart des constructeurs ne signent pas leurs produits (cas de Stuxnet).

1.4.2 Mises à jour régulières

Dans les systèmes industriels, les changements (hardware, software, patch) ou la mise à jour n'ont pas pour objectif de corriger un dysfonctionnement opérationnel et sont peu déployés. De plus, le déploiement peut être coûteux en temps, car les appareils peuvent être nombreux et dispersés sur plusieurs sites. Ce temps de déploiement des mises à jour est d'autant plus important si l'on considère les temps de tests, afin d'assurer la non-dégradation du système. Par conséquence, avant de procéder à un déploiement, il devient alors nécessaire d'évaluer les bénéfices de réduction d'un ou plusieurs risques de cybersécurité et les coûts engendrés par un arrêt de production. Ainsi, il est primordial de pouvoir correctement identifier et estimer les risques du système à travers une analyse de risques au contexte de l'*utilisateur*. La mise à jour peut être ignorée ou décalée et une mesure corrective alternative peut parfois être mise en œuvre si la vulnérabilité ou le risque traité est acceptable.

1.4.3 Sauvegardes régulières

La mise en place de sauvegardes régulières du système, au minimum, avant et après chaque modification est impérative afin de pouvoir restaurer le système en cas d'incident (cyber-incident ou panne matérielle). De nombreuses solutions permettent de sauvegarder régulièrement le disque dur du serveur SCADA. Cependant, peu de solutions existent pour la prise en compte de la sauvegarde pour des programmes d'application des automates. En effet, dans la quasi-totalité des cas , le programme applicatif de l'automate n'est accessible qu'au travers du protocole propriétaire du constructeur.

1.4.4 Antivirus

L'antivirus ou l'anti-malware, appartient à la panoplie des incontournables de la cybersécurité. Vu le nombre croissant de logiciels malveillants qui apparaissent chaque jour, un antivirus cherche à détecter les logiciels malveillants par différents moyens avant de les neutraliser (Clu, 2005). La méthode " classique " effectue la recherche de signatures en comparant les fichiers analysés avec une base de données de signatures de virus. La méthode reste limitée, car il y a toujours de nouveaux virus **dont on n'a pas encore la signature**. De plus, certains logiciels malveillants, les virus polymorphes, sont capables de

modifier des parties de leur code changeant leur signature. Par conséquent, ils deviennent indétectables.

Une autre méthode plus sophistiquée dite heuristique existe. Elle comporte une émulation de code afin d'avoir le comportement du fichier analysé. Par contre, cette méthode demande beaucoup de ressources en mémoire et en calcul. Elle peut générer de faux positifs, ce qui est non tolérable dans les systèmes comme les ICSs. Une suppression d'un ficher dans un serveur SCADA peut causer un arrêt de production de plusieurs jours, ou avoir des conséquences importantes sur les humains et/ou l'environnement.

1.4.5 Contrôle d'accès logique

Contrôle d'accès logique
Les mesures de contrôle d'accès satisfont aux besoins ou aux principes :

- du moindre privilège et du besoin de savoir : elles n'autorisent l'accès aux informations qu'aux utilisateurs qui en ont réellement besoin dans l'exercice de leurs fonctions ;
- la traçabilité des actions des utilisateurs.

1.4.6 Dispositifs de filtrage du réseau (pare-feu)

Les pare-feu sont généralement des solutions de filtrage réseau qui permettent de suspendre le trafic soupçonné selon un ensemble de règles. En revanche, peu de dispositifs permettant d'analyser les protocoles industriels existants. La plupart des équipements permettent d'intégrer principalement le Modbus TCP qui ne représente qu'une partie (moins de 25%) du marché. L'intégration d'un pare-feu et de son principe de filtrage peut être difficile pour certains systèmes de contrôle. Puisque chaque paquet doit être scanné, le temps de filtrage de ce type de solution ajoute un temps de latence non nul. Cette latence supplémentaire, bien que très faible (de l'ordre de 1 ms), peut ne pas être compatible avec les contraintes du temps de réponse d'un système de contrôle industriel, en particulier dans les couches 0 et 1 du modèle PURDUE (voir la figure 1.1) (ou le temps de traversée sur réseaux est de l'ordre de millisecondes).

1.4.7 Système de détection d'intrusion IDS

Un SDI ou (IDS en anglais) présente une solution de cybersécurité très puissante dans le monde des systèmes en temps réel dans lesquels les changements sont laborieusement acceptés, car le fonctionnement nominal est bien défini dans le cahier des charges et également dans l' analyse fonctionnelle.... Par conséquent, cela facilite la détection des anomalies. Toutefois, cette technique est difficile à mettre en oeuvre, car la plupart des équipements souffrent d'un manque de ressources en mémoire et en calcul.

1.4.8 Systèmes de Supervision

Les systèmes de supervision analysent, contrôlent les événements et émettent des alertes. Ils sont indispensables afin de réagir efficacement et rapidement dans le cas d'un imprévu pouvant conduire à une conséquence catastrophique. Un système de supervision collecte des événements se produisant dans le système ICS à travers les systèmes de sécurité comme firewalls, IDS..., mais les informations transmises par les automates

sont parfois limitées du point de vue de la cybersécurité. Dans le domaine de la sécurité des systèmes informatiques, on distingue la sécurité offensive qui consiste à tester des attaques pour déterminer des vulnérabilités du système, la sécurité défensive qui permet de se protéger (cryptographie, firewall, supervision par exemple) de certaines attaques , et la sécurité opérationnelle qui est un ensemble d'étapes à mettre en place et évaluer régulièrement pour garantir la sécurité des informations et des systèmes.

1.5 Sécurité opérationnelle OPSEC (OPerationnelle SECurity)

L'un des principaux objectifs de l'OPSEC est de contrôler l'information d'une infrastructure afin d'éviter qu'elle soit exploitée. Plus il faut de temps à un adversaire pour obtenir des informations critiques, plus vous avez de temps pour découvrir les problèmes et bloquer l'accès à l'information et à l'installation. L'OPSEC se compose de cinq étapes simples (ics,) :
- Identifier l'information critique ;
- Analyser la menace ;
- Analyser les vulnérabilités ;
- Évaluer le risque ;
- Appliquer des contre-mesures.

L'OPSEC est un processus continu, il ne se termine pas lorsque vous terminez la cinquième étape. En effet, les étapes ne doivent pas nécessairement s'enchaîner dans un ordre particulier.
Nous allons, par la suite, nous intéresser à l'évaluation des risques.

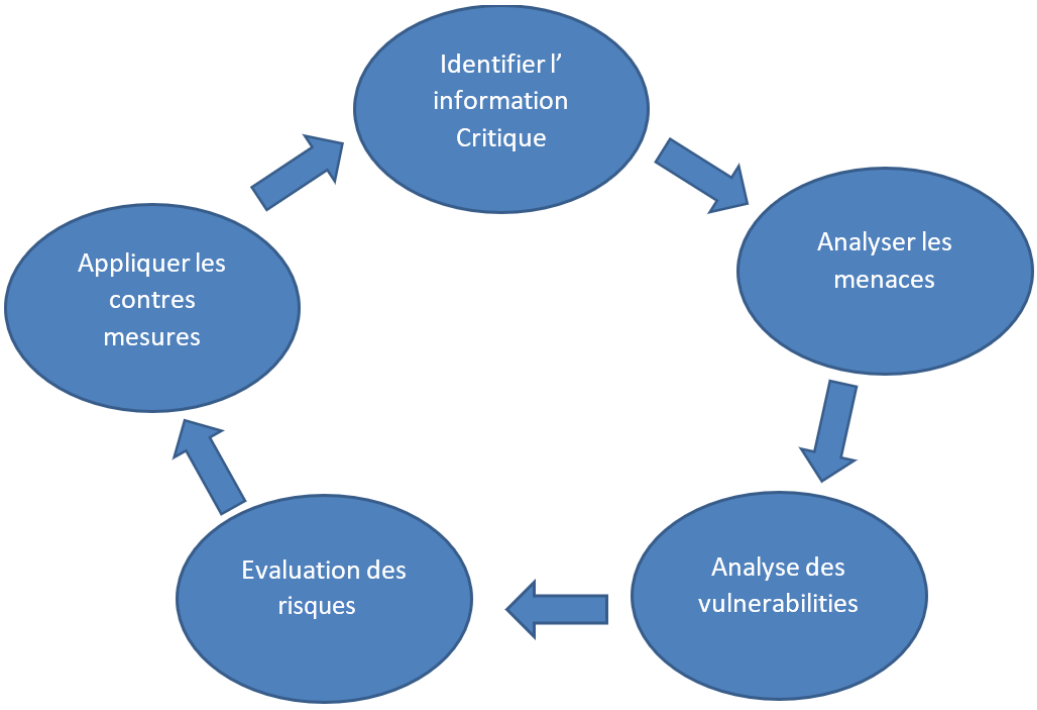


FIGURE 1.7 – Processus OPSEC(ics,)

1.5.1 Évaluation des risques

Le risque est la probabilité qu'un attaquant capte et exploite les informations critiques, ce qui aura un impact négatif sur les installations industrielles. Différentes organisations définissent le risque différemment. En général, le risque est défini, comme suit, dans la plupart des disciplines d'ingénierie (par exemple la norme EN50126 (Wolf and Scheibel, 2012) :

$$Risque = Probabilité\ de\ l'accident \times Impact. \tag{1.1}$$

Une formule très proche spécifique aux risques des cyberattaques est donnée par l'agence américaine de cybersécurité et sécurité des infrastructures (Cybersecurity and Infrastructure Security Agency CISA) (ics,). La formule représente la probabilité comme une produit scalaire de la *Menace* et la gravité de la *vulnérabilité*.

$$Risque = Menace \times Vulnérabilité \times Impact \tag{1.2}$$

Impact : l'impact négatif (perte ou dommage) que l'organisation subirait si une attaque était réussie.
Dans le contexte de la cybersécurité, un hacker informatique est un exemple de menace. Une faiblesse exploitable dans l'ordinateur d'un système bancaire est un exemple de vulnérabilité. Le vol de données de cartes de crédit est un exemple de conséquence. Toutes les menaces ne sont pas intentionnelles. Des facteurs comme les conditions météorologiques, la fatigue des matériaux ou les erreurs humaines peuvent tous contribuer au risque et entraîner des conséquences qui pourraient être plus graves que celles causées par des menaces intentionnelles. Nous nous concentrerons, par la suite, sur les menaces intentionnelles.

1.6 Conclusion

Après une présentation des systèmes de contrôle industriels, nous avons mis en évidence les spécificités et les nouveaux défis de ces systèmes et introduit la problématique de la cybersécurité. Puis, nous avons clarifié la signification des termes "SEC et SAF" tels qu'ils sont utilisés dans le contexte de ce travail et souligné leurs similitudes et leurs différences. Nous avons également montré les interdépendances potentielles entre la SAF et la SEC, en termes de risques et d'exigences dans le contexte des systèmes de contrôle industriel (ICS). Nous fournissons dans le chapitre suivant une classification des approches existantes qui prennent en compte les questions de SAF et de SEC pour les systèmes industriels. Nous présentons également une analyse critique de ces approches et identifions leurs limites.

Chapitre 2

État de l'art

Contents

Avec la prise de conscience croissante que les analyses de SAF et de SEC doivent être coordonnées dans l'évaluation des risques pour les ICSs, plusieurs travaux ont été faits pour combler le fossé entre la SAF et la SEC. Nous décrivons dans cette section les différentes approches qui proposent des processus ou des méthodologies dans lesquels les préoccupations de SAF et de SEC sont prises en compte conjointement. Ces approches sont classées selon différents critères, et la classification est reprise sous forme de tableaux. Le chapitre se termine avec une analyse critique de ces approches.

2.1 Méthodes d'évaluation des risques de sûreté dans ICSs

2.1.1 Évaluation des risques de la SAF

Analyse de l'arbre de défaillance (Fault Tree Analysis FTA)

L'Analyse de l'arbre de défaillances (FTA) (Sabaliauskaite and Mathur, 2015) est la technique la plus ancienne dans l'évaluation des risques de la SAF. C'est aussi une technique graphique répandue et utilisée pour l'évaluation des dangers et des risques dans les ICSs. L'objectif principal du FTA est de présenter les éventuels événements normaux et défectueux qui peuvent provoquer l'événement indésirable de niveau supérieur. L'arbre de défaillances se compose des éléments suivants : les nœuds (événements indésirables dans le système), les portes (relations entre les nœuds ; peuvent être des portes ET ou OU) et les bords (cheminement d'évènements indésirables dans le système).

Analyse des Modes de Défaillance et de leurs Criticités -AMDEC

L'Analyse des Modes de Défaillance et de leurs Criticités (AMDEC) (en anglais Failure Modes and Effects Analysis FMEA) est une méthode structurée et basée sur le travail d'équipe pour l'analyse de la SEC des systèmes afin d'identifier, d'évaluer et de noter les défaillances potentielles et leurs effets. La méthode est décrite dans la norme CEI 60812 (Commission et al., 2006a). Le mode de défaillance fait référence à la manière dont une entité peut tomber en panne. L'analyse AMDEC est utilisée pour évaluer la gravité des différents modes de défaillance. Le terme "numéro de priorité du risque" (Risk Priority Number RPN) fait partie de l'analyse quantitative de l'AMDEC; il est le résultat du produit de la gravité, de la probabilité d'occurrence et de la probabilité de détection (Nourian and Madnick, 2015). Grunske et al (Grunske et al., 2007) ont proposé "l'AMDEC probabiliste", qui est une extension de l'AMDEC originale. Elle aide les ingénieurs de sécurité à identifier si un mode de défaillance se produit avec une probabilité supérieure à son taux de risque tolérable. L'AMDEC est réalisée dés la phase de conception du cycle de vie du système. Pour plus d'information sur la méthode, la référence (Ebeling, 2004) présente une bonne revue.

Méthodologie de danger et de Opérabilité HAZOP

La méthodologie de danger et d'Opérabilité (HAZard and OPerability HAZOP) (Dunjó et al., 2010) est un processus d'analyse des dangers (Process Hazard Analysis PHA) utilisée pour étudier non seulement les dangers d'un système, mais aussi ses problèmes d'opérabilité, en explorant les effets de toute déviation par rapport aux conditions de conception. Cette analyse permet de déterminer comment un processus s'écarte de son fonctionnement nominal et entre dans un état indésirable en identifiant les dangers et les problèmes de fonctionnement potentiels des installations (Kennedy and Kirwan, 1998). Dans (Rausand, 2013), la procédure d'analyse HAZOP est décrit en détail.

Ingénierie basée sur des modèles (Model-based engineering MBE)

L'ingénierie basée sur les modèles (MBE) (Banerjee et al., 2011) est une méthode permettant de développer des modèles comportementaux de systèmes et d'analyser les modèles pour la vérification des exigences afin de garantir la SAF des CPS. La procédure considère d'abord la sûreté du système pour déterminer un ensemble de propriétés attendues, puis extrait les propriétés de l'environnement physique, des unités de calcul et des interactions cyberphysiques, et enfin, analyse le modèle abstrait pour évaluer les propriétés attendues et vérifier la satisfaction des exigences de la sécurité.

Arbre des Objectifs - Arbre des Succès et Diagramme Logique Principal (Goal Tree - Success Tree and Master Logic Diagram GTST-MLD)

L'arbre de réussite ou objectifs et le diagramme logique principal (GTST-MLD) (Modarres and Cheon, 1999) est un cadre d'analyse de la fiabilité et des risques basés sur les fonctions. Il se compose de GT (Goal Tree) , ST (Success tree) et MLD (Master Logique Diagramme). Ce modèle peut représenter les systèmes physiques complexes en termes de relations logiques, physiques et floues. Brissaud et ses collaborateurs (Brissaud et al., 2009) ont proposé un modèle en trois étapes pour l'analyse de la fiabilité, qui est un modèle GTST-MLD étendu qui intègre les défauts et les défaillances. En plus de la relation entre les fonctions et les structures, ce modèle représente également la relation entre les

défauts et les défaillances. Ces relations permettent d'évaluer l'impact des défauts ou des défaillances au sein des composants ou des fonctions.

Analyse des processus de la théorie des systèmes (System Theoretic Process Analysis STPA

Les techniques traditionnelles d'analyse des risques mentionnées ci-dessus ont été difficiles à adapter dans de nombreux systèmes complexes à forte intensité logicielle, c'est pourquoi l'analyse théorique des processus du système (STPA) a été proposée. La STPA est une technique d'analyse des risques, basée sur le modèle d'accident théorique du système et des processus (System-Theoretic Accident Model and Processes STAMP), qui est une nouvelle causalité modèle de contrôle des structures, développé par Leveson dans(Lee et al., 2013). Lorsque le STAMP est exécuté, le système est traité comme une structure de contrôle hiérarchique. Les interactions entre chaque couche de la structure de contrôle imposent les contraintes requises sur le comportement des couches inférieures suivantes, ces contraintes peuvent affecter le comportement du système. Le fonctionnement à chaque couche de cette structure de contrôle est basé sur une boucle de contrôle à rétroaction. La méthode ne distingue pas les dangers d'un système, mais les causes des dangers.

2.1.2 Évaluation des risques de la SEC

Dans la plupart des ICSs, le risque de la SEC n'a pas été pris en compte (Schmittner et al., 2015) au stade de la conception. Mais l'évaluation et la gestion des risques de la SEC deviennent une question de plus en plus importante surtout avec la migration vers industrie 4.0. La question de la sécurité devrait être traitée de manière aussi importante que la question de la sûreté dans ICSs. Les méthodes les plus connues de gestion et évaluation des risques de SEC sont examinées dans cette section.

Analyse des arbres d'attaques

L'Analyse des Arbres d'Attaques (ATA) (Kriaa et al., 2015) est une technique largement utilisée pour l'évaluation des risques de sécurité. L'arbre d'attaque présente les étapes du processus d'attaque sous la forme d'un graphe. Il utilise les mêmes symboles de base que les arbres de défaillance (FT) : les nœuds (représentent les attaques), les portes (portes ET ou OU) et les bords (chemin des attaques à travers le système). Basés sur les arbres d'attaque, les arbres de contre-mesures d'attaque (Attack Contermeasure Trees ACT) (Roy et al., 2012) prennent en compte les attaques ainsi que les contre-mesures sous la forme de mécanismes de détection et de techniques d'atténuation. Ce modèle analytique ACT permet aux utilisateurs d'effectuer une analyse qualitative et probabiliste complète de l'état de sécurité de l'infrastructure.
(Tran et al., 2019) présentent une méthodologie très intéressante de gestion et évaluation des risques de la cybersécurité pour de systèmes aériens sans pilote (Unmanned Aircraft Systems). Les auteurs proposent une nouvelle version de l'arbre d'attaque pour l'identification du risque. L'arbre d'attaque commence par l'objectif de l'attaque (par exemple, "crash du drone" ou "divulgation de la vidéo d'observation"). Chaque dysfonctionnement est considéré comme une violation d'un des trois attributs de sécurité (confidentialité, intégrité, disponibilité). En suite, une matrice de risque a été définie qui prend *la criticité de l'attaque* et *la difficulté de l'attaque (Difficulty Of the Attack DOA)* comme deux dimensions. En revanche, cette partie nous semble un peu subjective. En effet, cette méthode

souffre d'un manque terrible des métriques pour l'évaluation de *la difficulté de l'attaque (DOA)*, ce qui complique la mission de l'évaluateur. Donc, la méthode requiert un haut niveau d'expertise.

Approche Cyber-Physical Security CYPSec

Les solutions de la SEC des systèmes cyberphysiques (Cyber-Physical Security CYPSec) sont proposées pour la surveillance de la santé de la SEC des systèmes par Krishna et al. dans (Banerjee et al., 2011). Elle prend en compte les propriétés des composants informatiques et l'interaction des composants avec l'environnement physique. Les solutions CYPSec sont réalisées en combinant les primitives de SEC traditionnelles avec la connaissance de l'environnement. Le cœur de cette approche est d'utiliser la capacité de surveillance du CPS (Cyber Physical System) pour protéger le système contre les menaces. Les solutions CYPSec peuvent utiliser pleinement les caractéristiques complexes et dynamiques de l'environnement physique pour assurer la sécurité du CPS.

2.2 Approches combinant SAF et SEC pour les ICSs

Notre revue de la littérature est motivée par un objectif spécifique traduit en un ensemble de questions de recherche, ce qui constitue la première étape de ce travail. Nous formulons les questions de recherche où les critères suivants en nous concentrant sur le domaine de recherche de la co-analyse de la SAF et de la SEC.
Question-1 : Quelles sont les méthodes d'analyse adoptées pour aborder l'interaction de la SAF et de la SEC aux premiers stades de conception et en phase opérationnelle ?
La principale raison pour laquelle le champ d'application des travaux est limité aux premiers stades de développement du système est l'importance de l'harmonisation de la sûreté et de la sécurité à ces stades pour le coût global et l'effort nécessaire pour concevoir un système sûr et sécurisé. Cependant, de nouvelles menaces en termes de cyberattaques apparaissent chaque jour. Cela remet en question la SEC et en conséquence la SAF des systèmes déjà opérationnels.
Question-2 : Comment les méthodes d'analyse identifiées abordent l'interaction entre la SAF et la SEC ?
Question-3 : Comment les méthodes d'analyse abordent l'évaluation du risque des cyberattaques ? considérant que le risque est égal au produit scalaire entre menace, vulnérabilité et impact.
Question-4 : Comment les méthodes d'analyse abordent la questions des mises à jour dans ICSs des cyberattaques ?

On se basant sur ces questions, nous avons identifié à partir de la littérature, plusieurs critères que nous détaillons.

Critère : les étapes de processus de gestion des risques

Cherdantseva et al (Cherdantseva et al., 2016) ont utilisé les "étapes de processus de gestion des risques" comme critères pour analyser les méthodes d'évaluation des risques de cybersécurité pour les systèmes SCADA. Ce critère nous permettra d'identifier la ou les étapes prédominantes du processus d'évaluation des risques traitées par les méthodes d'évaluation conjointe des risques de SEC et SAF. Un processus d'évaluation des risques comporte généralement trois étapes :

- *Identification des risques :* C'est le processus qui consiste à trouver, reconnaître et décrire les risques (ISO., 2009).
- *Analyse des risques :* C'est le processus qui consiste à comprendre la nature, les sources et les causes des risques qui ont été identifiées et à estimer le niveau de risque (ISO., 2009).
- *Évaluation des risques :* C'est le processus qui consiste à comparer les résultats de l'analyse des risques avec les critères de risque pour prendre des décisions sur la gestion des risques (ISO., 2009).

Critère : cycle de vie

Les risques de la cybersécurité sont de nature très dynamiques, car chaque jour la communauté des chercheurs identifie et publie de nouvelles vulnérabilités. Cela justifie la nécessité d'avoir un critère qui définit à quelle phase dans le cycle de vie ces méthodes d'évaluation interviennent, dans la phase de développement ou dans la phase opérationnelle.

Critère : indépendance entre SAF et SEC

Nous avons adopté deux sous critères de classification : 1) les approches combinées de SEC/SAF ; et 2) la SEC basée sur la SAF.

Les approches *combinées* effectuent des analyses de SEC et de SAF en *parallèle*, qui nécessitent une étape séparée d'intégration pour harmoniser les résultats de ces analyses. Elles demandent un nombre plus important d'itérations pour intégrer les exigences de la SEC et les exigences SAF. Cette étape est la plus importante dans ces approches.
Les approches de la *SEC basée sur la SAF* prennent en compte les résultats d'analyses de SAF et de SEC effectuées en parallèle et analysent l'influence de la SEC sur la SAF. Ce que nous pouvons dire pour toutes les approches parallèles, tout comme pour le groupe précédent, c'est que l'activité d'intégration des analyses de sûreté et de sécurité est l'aspect le plus important. Alors que dans le groupe précédent, l'activité comprenait l'analyse des dépendances de la SEC sur la SAF et vice versa, dans ce groupe, seule l'influence de la SEC sur la SAF est prise en compte. Cela convient aux systèmes où la SEC n'est pertinente que si elle influence la SAF. Mais si l'intention est d'avoir également un système sécurisé au-delà des questions de SEC pertinentes pour SAF, ces approches ne sont pas appropriées pour ces systèmes, car elles ne couvrent pas l'analyse de l'influence de la SAF sur la SEC.

Critère : unifiée/ parallèle

Nous avons cherché à savoir si les travaux proposent une manière unifiée l'analyse des interdépendances entre la SEC et la SAF ou une approche parallèle lorsqu'une harmonisation supplémentaire des interdépendances est nécessaire.

Nous adoptons les mêmes définitions établie par (Kriaa, 2016), pour faire la différence entre les approches d'unification et d'intégration parallèle : - Les approches d'unification visent à réunir les techniques de SEC et de SAF dans une seule et même méthodologie. Le résultat de ces approches est un ensemble unique d'exigences décrivant les fonctions de SEC et de SAF du système.

- Les approches d'intégration ou d'harmonisation parallèle visent à étudier les similitudes et les différences entre les techniques de SEC et de SAF afin de les rapprocher. Ces approches donnent indépendamment les exigences de SEC et de SAF , en utilisant

des concepts et des méthodologies classiques standards. Ensuite, elles montrent leur interaction afin d'identifier les conflits. Bien que la réduction du nombre d'itérations pour harmoniser les études SAF et SEC soit un objectif important, la limite de ces méthodes est qu'elles sont généralement plus complexes et qu'il faudrait plus de temps pour les réaliser avec deux activités distinctes de l'analyse de la SAF et de la SEC. En outre, ces approches peuvent être plus difficiles à mettre en œuvre dans la pratique, car elles nécessitent davantage de changements dans les pratiques pour les processus de l'étude de la SAF et de la SEC utilisés dans les entreprises. Une préoccupation générale concernant les approches de ce groupe est la mesure dans laquelle elles soutiennent la SAF et la SEC, c'est-à-dire si elles réussissent à identifier les dangers et les menaces au moins aussi bien que les méthodes indépendantes.

Critère : évaluation des vulnérabilités

Ce critère permet de voir si l'approche offre une méthode d'évaluation des vulnérabilités. En fait, d'après l'équation de risque de la cybersécurité qui est un produit scalaire entre menace, vulnérabilité, et impact (voir le chapitre 1), nous constatons que la partie la plus objective, d'un point de vue pratique, est l'évaluation des vulnérabilités et leur impact.

Critère : quantitative/qualitative

Le critère permet de voir la nature de résultat : qualitative ou quantitative.

Critère : standard utilisé

Ce critère permet de voir le standard utilisé. Est ce que cette approche est spécifique à un domaine ou est-elle générique ?

Critère : approche basée sur les modèles

Ce critère permet de voir si l'approche demande une modélisation du système avant de faire la démarche d'évaluation des risques. En réalité, la complexité des modèles dans du système ICSs empêche parfois l'application de plusieurs des approches proposées dans le cas pratique.

Critère : évaluation probabiliste de la SEC

Le critère permet de voir si la méthode est probabiliste de point de vue SEC.

Les différentes approches identifiées dans l'état de l'art ont été classées en deux grandes catégories : les approches orientées processus et les approches basées sur des modèles, affinées par la suite selon plusieurs critères que nous allons voir dans les prochaines sections.

2.2.1 Approches orientées processus

Cette catégorie regroupe les approches qui proposent de nouveaux cycles de vie et des méthodologies qui prennent en compte la SAF et la SEC à un niveau macroscopique de la conception des systèmes ou de l'évaluation des risques. Elles s'appuient sur des exigences, généralement spécifiées par des normes de la SAF et/ou de la SEC, et fournissent

des descriptions génériques des cycles de vie, indiquant quels types d'activités doivent être effectuées, dans quel ordre. Dans cette section, les approches importantes de cette catégorie sont présentées.

Analyses des Modes de Défaillance, de leurs Effets (Failure Modes, Vulnerabilities and Effect Analysis FMVEA)

(Schmittner et al., 2014a) proposent l'approche FMVEA, une méthode basée sur l'approche l'AMDEC. La méthode intègre à la fois les modes de défaillances et leur effets pour l'analyse cause-effet pour la SAF et la SEC. Il s'agit d'une approche de haut niveau adaptée à la phase de la conception et de la vérification. Dans cette approche, les menaces sont quantifiées en utilisant des agents de menace qui représentent les attaquants ; les modes de menace sont extraits en utilisant un modèle STRIDE (Spoofing, Tampering Repudiation, Information, disclosure, Denial of service and Elevation of privilege) (Corporation, 2005) qui donne les effets de la menace et les probabilités d'attaque. L'un des avantages de l'approche est la possibilité de réutiliser les résultats acquis précédemment et de refaire l'analyse au cas où une nouvelle menace ou vulnérabilité serait identifiée (Schmittner et al., 2015).

(Plósz et al., 2017) proposent une méthode combinant des parties de méthodologies existantes, STRIDE (Corporation, 2005), et FMEA (Commission et al., 2006a). Ces analyses de SAF et de SEC sont divisées en deux parties, avec une étape d'intégration après les premières activités parallèles qui fournit un catalogue combiné des menaces pour la SAF et la SEC. Les résultats de l'intégration sont ensuite intégrés dans la deuxième partie des deux méthodes pour l'évaluation de l'impact du côté de la SEC et l'évaluation de la probabilité du côté de la SAF. Les avantages de l'approche sont les suivants : économie d'efforts grâce à la prise en compte des points communs des évaluations séparées en une seule fois, utilisation du catalogue combiné pour sensibiliser aux questions ayant un impact ou une probabilité élevée dans les deux domaines, et soutien des décisions multidimensionnelles prises en abordant la SEC et la SAF ensemble.

Méthodes basées sur la méthodologie NIST 800-30

Chen et al. (2014) (Chen et al., 2014) s'appuient sur l'extension de la méthodologie NIST 800-30 (NIST, 2012) pour prendre en compte les aspects de sécurité contribuant à l'évaluation des risques en établissant une relation fonctionnelle entre les vulnérabilités, les menaces et les dangers. Les niveaux d'occurrence des dangers sont attribués en fonction de la valeur d'une probabilité conditionnelle de danger-menace. L'impact est attribué en fonction d'une caractérisation numérique des actifs.

Approches basées sur SAHARA

Macher et .al (Macher et al., 2014), (Macher et al., 2015), (Macher et al., 2016) décrivent l'analyse des dangers et des risques en matière de sécurité (Security-Aware HAzard and Risk Analysis SAHARA). La méthode combine deux approches bien connues, HARA(ISO, 2011) provenant du domaine automobile et STRIDE du domaine sécurité IT pour retracer l'impact de la SEC sur la SAF au niveau du système (Corporation, 2005). STRIDE est l'acronyme de Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, and Elevation of privileges. Le concept clé de cette approche de modélisation des

menaces est l'analyse de chaque composante du système pour la susceptibilité aux menaces et l'atténuation de toutes les menaces afin de faire valoir qu'un système est sécurisé. La méthode se concentre sur la modélisation des menaces, pour examiner la conception du système de manière méthodique. Au départ, l'analyse de la SAF est effectuée en respectant la norme ISO 26262 et en utilisant l'analyse HARA, tandis que l'analyse de la SEC est effectuée de manière indépendante sur la base de la méthode STRIDE. Les résultats de l'analyse de sécurité sont ensuite utilisés dans un concept de quantification ASIL (Automotive Safety Integrity Level) fournissant le niveau de SAF résultant. Tout comme le SAHARA, l'US^2 (Cui and Sabaliauskaite, 2018) effectue également une co-analyse de la SAF et de la SEC. Pour une attaque, l'US^2 quantifie d'abord son niveau de SEC, puis détermine si l'attaque introduit des risques pour la SAF ; si c'est le cas, les contre-mesures de sécurité et les contre-mesures de SAF sont nécessaires ; sinon, seules les contre-mesures de la SEC sont nécessaires.

Cadre d'évaluation des risques pour les systèmes embarqués dans l'automobile RAFAES (Risk Assessment Framework for Automotive Embedded Systems)

Islam et al. (2016) (Islam et al., 2016) proposent un cadre pour l'analyse et l'évaluation des risques inspirés de la norme ISO 26262 (ISO, 2011). En raison du lien étroit avec la norme de sécurité automobile et inspiré par l'industrie, le document vise à fournir un cadre facilement applicable dans le domaine automobile. Ce cadre traite des risques de SEC et combine l'analyse de SEC proposée sur le processus de développement de la norme ISO 26262. Le travail vise à faciliter la co-certification de la SAF et de la SEC pour un système donné. En proposant une analyse de la SEC alignée sur l'analyse de la SAF existante, l'approche porte sur l'identification de toutes les propriétés pertinentes pour la SAF ou la SEC.

Approches basées sur des mots-clés (SGM Security Guideword Method)

Durrwang et al. (Dürrwang et al., 2017) décrivent une approche de la méthode des mots-guides de SEC (Security Guideword Method SGM) utilisée pour identifier les actifs d'information et les objectifs de protection pertinents pour la sécurité lorsque des artefacts de la norme ISO 26262 sont réutilisés. La méthode SGM est basée sur des mots-guides de SEC, utiles pour identifier des scénarios d'attaque possibles, similaires au HAZOP du domaine de la SAF. L'approche fournit des modèles unifiés de SAF et de SEC qui minimisent l'effort d'intégration de la SAF et de la SEC au domaine automobile, et permettent aux ingénieurs non spécialisés dans la sécurité d'identifier les actifs d'information et les objectifs de protection.

Méthodes d'analyses basées sur la norme SAE J3061

La norme SAE (Society of Automotive Engineers)-J3061 (Sae, 2016) propose un moyen d'intégrer les processus de la SAF des véhicules (ISO 26262) et de SEC (SAE J3061) en établissant des voies de communication entre la SAF et cybersécurité. Par exemple, la norme SAE J3061 affirme que les chercheurs doivent effectuer des analyses sur les menaces à la SEC et l'analyse des dangers pour la SAF simultanément afin de garantir qu'aucun défaut ou attaque n'a été manqué. Toutefois, la manière d'intégrer l'analyse de la SAF et de la SEC n'est pas proposée dans cette norme.

Cui et al. (Cui et al., 2019) proposent un cadre pour l'analyse des questions de SAF et de SEC, qui comprend une méthode intégrée de SEC et de SAF avec les normes interna-

tionales de SAF et de SEC des véhicules ISO 26262 et SAE J3061. L'applicabilité du cadre proposé est démontrée à l'aide d'un exemple de modèle de véhicule autonome typique. Grâce à ce cadre, on peut clairement comprendre les fonctions et la structure du véhicule, les défaillances et les attaques associées, et voir également les vulnérabilités qui ne sont pas encore traitées par des contre-mesures, ce qui permet d'améliorer la SAF et la SEC des véhicules du point de vue de la recherche et de l'ingénierie.
Dürrwang et al.(Dürrwang et al., 2018) présentent une approche visant à réutiliser les résultats d'une analyse de la menace pour les tests de sécurité automobile. La méthodologie proposée permet de conduire des cas de test à l'aide d'arbres d'attaque. En outre, l'approche présentée montre exactement comment les résultats d'une analyse de la SAF peuvent être réutilisés pour identifier les menaces qui peuvent compromettre la SAF des véhicules. L'approche proposée est appliquée sur l'étude d'un test de pénétration d'une unité de contrôle électronique (UCE) d'airbag d'automobile.

Approche HEAVENS (HEAling Vulnerabilities to ENhance Software Security and Safety)

Le projet HEAVENS (Olovsson, 2018) vise à identifier les vulnérabilités de sécurité dans les systèmes E/E (Électrique/ Électronique) dans l'automobile et à définir des méthodologies ainsi que des outils pour effectuer une évaluation de la SEC. La méthode STRIDE est utilisée pour identifier les menaces. Comme la méthode HEAVENS aborde la question de la SAF après avoir identifié les menaces à la SEC. Une valeur de risque de SEC est affectée, si la menace influence la SAF.

Dans cette section, nous avons constaté que les approches orientées processus se focalisent sur les menaces pour évaluer les risques. Partant du fait que la façon la plus pratique pour réduire le risque réside dans l'évaluation des vulnérabilités plutôt que des menaces. De plus, il n'y a pas d'évaluation quantitative. Finalement, plusieurs approches sont spécifiques un domaine d'application (en particulier beaucoup de travaux relèvent de l'automobile) et ne sont pas génériques.

2.2.2 Approches basées sur des modèles

Contrairement aux approches orientées vers les processus, les approches basées sur des modèles reposent sur une représentation formelle ou semi-formelle des aspects fonctionnels/non fonctionnels du système et sont généralement soutenues par des outils. Nous classons ensuite les approches fondées sur des modèles identifiées selon qu'elles reposent sur des modèles graphiques ou non graphiques.

Approches basées sur GTST-MLD

(Di Maio et al., 2019) propose un cadre de schéma logique principal de l'arbre de réussite Goal Tree (GTST-MLD) pour traiter conjointement les aspects de la SAF et de la SEC dans l'analyse des risques des ICSs, les interdépendances entre les composantes du ICSs et la gestion de la rareté des informations liées aux menaces de cybersécurité. Le GTST-MLD a été adopté pour la première fois en tant qu'approche orientée vers un objectif pour une analyse quantitative des risques d'un CPS, en tenant compte des défaillances et des menaces de cybersécurité. La GTST-MLD a montré qu'elle offrait une alternative appropriée aux méthodes conventionnelles telles que l'AT-BT (Attack Tree-Bow Tie). La méthode permet de :
1) modéliser les interdépendances entre les composants ;

2) prendre en compte les différents types de cyberattaques et leur influence sur les différentes parties du système.
(Francesco Di Maio, 2019) propose une méthode basée GTST-MLD pour attribuer des pondérations pour la méthode GTST-MLD et utilisant la méthode OS (Order Statistic) pour traiter conjointement la SEC et la SAF. Les auteurs utilisent une méthode de simulation (Monte Carlo) pour évaluer les poids basés sur des modèles physiques imitant le comportement du ICSs sous les attaques. Les auteurs appliquent la méthode sur un réacteur ALFRED. Cependant, la méthode se base sur la collecte des données expérimentales sur les menaces et les vulnérabilités. Cela rend la méthode difficile à appliquer.

Evaluation des risques et vulnérabilité des menaces TVRA (Threat Vulnerability and Risk Assessment)

(Reichenbach et al., 2012) proposent une approche de l'analyse d'un modèle combinée des risques de la SEC et de la SAF en étendant une technique d'évaluation des vulnérabilités et des risques de la menace TVRA (Threat Vulnerability and Risk Assessment) avec des niveaux d'intégrité de la sécurité (SIL) à partir de la norme de sécurité fonctionnelle générique CEI 61508. Le risque associé à une fonction dans cette technique TVRA étendue est calculé sur la base des facteurs de sécurité ainsi que des SIL de la fonction considérée. La technique ne dépend pas de l'analyse de la SEC, mais fournit des moyens d'identifier l'influence des vulnérabilités sur la SAF.

Approches basées sur STPA (System Theoretic Process Analysis)

(Young and Leveson, 2013) présentent une méthode STPA-Sec. La méthode est basée sur la méthode d'analyse classique (STPA) de la SAF. Cette méthode nécessite une équipe multidisciplinaire composée d'experts en sécurité et en fonctionnement du système pour identifier et empêcher le système d'entrer dans des états vulnérables qui entraînent des pertes durant la phase de conception. Dans cette approche, les dangers sont présentés comme des problèmes de contrôle. Chaque action de contrôle est examinée sous un ensemble de conditions et de mots-clés différents afin d'identifier les scénarios de pertes. L'approche permet de se concentrer sur les états vulnérables afin d'éviter les menaces d'exploitation, et les dommages éventuels.

La méthode permet d'analyser la cybersécurité, en basant sur un modèle de contrôle fonctionnel. Les étapes du processus de base de l'analyse STPA-sec sont similaires à celles de la STPA :
(i) identifier les menaces et les vulnérabilités ;
(ii) développer les unités de contrôle du système ;
(iii) identifier les opérations de contrôle qui placent le CPS dans un état dangereux ou les fuites d'informations ;
(iv) déterminer comment les actions de contrôle se déroulent sous les menaces et les perturbations.

Le STPA-sec est appliqué sur la base des mêmes boucles de contrôle que son homologue STPA basé sur le modèle de causalité de la théorie des systèmes, le STPA-sec peut être appliqué à un stade plus précoce du processus de conception et dans les situations où les données relatives aux composants spécifiques ne sont pas disponibles. La méthode STPA-sec estime que la sécurité est uniquement liée à son impact sur la SAF ; elle n'étend pas la relation de cause à effet du domaine de la SAF au domaine de la SEC, ce qui ne favorise pas l'analyse des risques, et limite la comparabilité des différents résultats d'analyse, et en outre, elle n'apporte pas de solution intégrée à l'analyse de sécurité. Une fois qu'une

partie critique est identifiée dans la CPS, la STPA-sec ne fournira aucune orientation pour l'analyse de la SEC.

Pereira et al. (2017) (Pereira et al., 2017) présentent une analyse fondée sur une combinaison de la STPA et des directives de la SP800-30 du NIST. La raison d'être de cette analyse est la fusion d'une approche systémique de la SAF et d'une approche par composants axée sur les menaces et les vulnérabilités. Les auteurs montrent comment aligner les flux de travail de la SEC et SAF où ils doivent se chevaucher.

En tenant compte à la fois la SEC et SAF, le STPA-SafeSec est proposé dans (Friedberg et al., 2017), ils présentent une méthode d'analyse combinée, basée sur la STPA (Pereira et al., 2017) et la STPA-Sec (Young and Leveson, 2013), et utilisée pour choisir les stratégies d'atténuation les plus efficaces pour assurer la SAF et la SEC du système. Cette approche présente l'avantage de prendre en compte de manière unifiée la SAF et la SEC tout en choisissant des stratégies d'atténuation appropriées, la possibilité de prioriser les composants les plus critiques du système pour une analyse de sécurité approfondie (par exemple, les tests de pénétration). L'analyse permet d'identifier les pertes potentielles du système, causées par une vulnérabilité spécifique en matière de SEC ou de SAF, et de meilleures stratégies d'atténuation.

Schmittner et al. (2016) (Schmittner et al., 2016) se concentrent sur l'amélioration d'une approche existante STPA-Sec (Young and Leveson, 2013) à la phase de conception. Ils ont constaté que les orientations pour l'identification des scénarios occasionnels intentionnels n'étaient pas suffisamment claires et ont proposé quelques modifications, ainsi que la nécessité d'inclure des éléments pertinents pour la SEC dans un modèle de boucle de contrôle.

Shapiro (2016) et al. (Shapiro, 2016) proposent une modification de la STPA-SEC (Young and Leveson, 2013) pour soutenir une analyse de risque technique pour l'ingénierie de la confidentialité (privacy engineering), à savoir la STPA-Priv. L'approche est basée sur celle qui existe déjà tout en introduisant l'analyse systématique des contrôles du système et de leur capacité à limiter les comportements susceptibles de nuire à la vie privée.

Howard et al. (2017) (Howard et al., 2017) proposent une méthode pour identifier et analyser formellement les exigences de la SEC et de SAF. Cette approche est basée sur la méthodologie de la STPA (Pereira et al., 2017) et combinée avec la modélisation, la traçabilité et la vérification formelle par l'utilisation de la méthode formelle de l'événement B (Event-B). L'objectif est de générer des exigences critiques afin de pouvoir prévenir les états indésirables du système. En utilisant le langage Event-B et la boîte à outils Rodin, ils démontrent et vérifient que ces exigences critiques réduisent complètement les états indésirables du système.

Temple et al. (2017)(Temple et al., 2017) proposent une approche combinant le STPA-Sec (Young and Leveson, 2013) et la FMVEA (Schmittner et al., 2014b), en les intégrant dans un processus analytique unifié appelé analyse théorique de probabilité et criticité des systèmes (Systems Theoretic Likelihood and Severity Analysis STLSA). La STLSA se concentre sur les actions de contrôle fonctionnel des systèmes, inclut l'aspect humain dans la boucle et intègre une évaluation semi-quantitative des risques conforme à la norme EN 50126.

Troubitsyna (2016)(Troubitsyna, 2016) propose une approche pour la dérivation et l'analyse intégrées des contraintes de SAF et de SEC qui s'appuie sur le paradigme de la réflexion systémique présenté par le STAMP (System Theoretic Accident Model and Processes), et la structuration des cas d'assurance par la notation structurée des objectifs (Goal Structuring Notation GSN). L'approche proposée consiste en un modèle de GSN inspiré de celui de STAMP. Ce document propose un traitement conjoint des exigences de

SAF et de SEC en utilisant le modèle GSN décrit pour leur structuration.

Spécifications Non-Fonctionnelles (Non-Functional Requirements -NFRs)

Les exigences non fonctionnelles (Non-Functional Requirements NFR) (Chung et al., 2012) constituent une approche systématique et pragmatique pour spécifier le fonctionnement du système, couvrent les attributs de qualité et de sûreté de fonctionnement des systèmes, tels que la performance, la disponibilité, la fiabilité, la maintenabilité, la sécurité et la facilité d'emploi (usability), et tiennent également compte des objectifs fonctionnels et des contraintes du système. Les NFR ont été appliquées pour évaluer simultanément les propriétés de SEC et de SAF dans un système SCADA dans l'industrie pétrolière(Subramanian and Zalewski, 2014). L'étude de cas montre que les NFR sont réalisables pour une analyse intégrée de la SEC et de SAF dans le CPS (Cyber-Physical System).

Approches de modélisation stochastique

Dans (Sallhammar et al., 2006), les auteurs présentent une revue sur les techniques de quantification basées sur les modèles en partant des méthodes combinatoires vers les méthodes séquentielles (basées sur les états) comme les chaînes de Markov recomposées (Markov reward models) et les réseaux de Petri stochastiques (SPNs).Les auteurs essayent de montrer que les méthodes de la sécurité-innocuité liées aux fautes accidentelles pourraient être utiles dans l'évaluation de la sécurité-immunité liée aux fautes causées par les fautes intentionnelles.

Dans (Chen et al., 2011), pour avoir une modélisation plus complète qui évite l'explosion de l'espace d'états, les auteurs suggèrent l'utilisation des réseaux de Petri stochastiques. Ces derniers proposent ainsi de modéliser les possibles combinaisons entre les cyberattaques et les attaques physiques dans les réseaux électriques intelligents. Les auteurs expliquent que la réalisation d'une attaque physique sur les appareils intelligents d'un réseau informatique pourrait faciliter une cyberattaque par la suite pour pénétrer dans le réseau. Ensuite, les dommages physiques intentionnels peuvent correspondre à une vulnérabilité exploitable par l'attaquant. Ensuite, ils présentent une étude basée sur l'utilisation des réseaux de Petri pour une modélisation conjointe entre les attaques physiques et les cyberattaques offrant plus de flexibilité par rapport aux méthodes traditionnelles comme les arbres d'attaques. Cependant, l'utilisation de modèles à base de réseaux de Petri demande beaucoup d'expertises dans les attaques cyberphysiques et fait appel à des connaissances interdisciplinaires. Pour cette raison, l'article propose une méthodologie hiérarchique de modélisation pour construire des réseaux de Petri larges et complexes à partir de plus petits réseaux de Petri construits par des équipes différentes (de disciplines différentes). D'après la démarche adoptée dans l'article, nous constatons la possibilité à l'attaquant d'exploiter des fautes accidentelles pour déclencher son attaque.

Le réseau de croyances bayésiennes (Bayesian Belief Network BBN) a été appliqué au cours des deux dernières décennies dans les domaines industriels pour la prise de décision, le traitement de l'incertitude et l'évaluation des risques. Le BBN (Kornecki et al., 2013) utilise l'estimation de la probabilité prédéfinie pour évaluer quantitativement si la CPS satisfait les exigences et les objectifs de la SEC et de la SAF. L'estimation de la probabilité comprend les taux de défaillance entre les composants, les connexions et les accidents possibles, etc.

Un cadre unifié d'évaluation des risques(Huang et al., 2017) a été proposé dans les réseaux SCADA, qui intègrent un arbre d'attaque, un arbre de défaillance et un arbre

d'événements pour construire un modèle de réseau bayésien (Bayesian Network BN). La plupart des méthodes quantitatives d'évaluation des risques de sécurité (Security Risk Assessment SRA) dans les CPS reposent sur l'expérience et les connaissances d'experts. Ce type d'approche permet d'ajuster les paramètres du modèle à partir de données historiques limitées par autoapprentissage, et d'évaluer dynamiquement le risque du SCADA en cas d'attaques connues ou inconnues. Une modélisation de sécurité basée sur la théorie des jeux a été proposée dans (Orojloo and Azgomi, 2017b), afin de réaliser une quantification avec des métriques comme MTTSD (Mean-Time-To-Shutdown), disponibilité... . Ainsi, le système évolue entre différents états (selon une machine à états), avec des transitions modélisées par des équations différentielles (comme pour un système Hybride). La machine à états est divisée en deux phases : une phase d'intrusion et une phase de perturbation. Pour chaque phase, un paradigme de théorie des jeux avec des paramètres qui diffèrent permet de prédire les interactions entre le système et l'attaquant (comme le coût pour mener une attaque, le coût pour empêcher les attaques sur les systèmes, l'intrusion des connaissances de l'attaquant sur le système, probabilité de faire l'attaque, récompense).
Dans (Xiang et al., 2014), une nouvelle méthode de modélisation de comportement probabiliste des cyberattaques avec les SMC (Semi Markov Chain) incluant : les ressources disponibles pour l'attaquant, les vulnérabilités du système, les architectures de réseaux ciblés et enfin, l'impact d'une réussite cyberattaques. Une démarche de mesure de la fiabilité a été proposée à la fois pour les composants physiques et pour les cyberattaques dans le cas d'un réseau intelligent type IEEE RST79.

Huang et ses collègues (Huang et al., 2018) ont également proposé un cadre quantitatif précis pour l'évaluation des risques dans les CPS, qui est basé sur le modèle BBN et le Système Hybride Stochastique (SHS). Le BBN est utilisé pour modéliser le processus de propagation des attaques dans la couche cyber et calculer la probabilité que les actifs du système soient compromis. Le modèle SHS (Stochastic Hybrid System) est utilisé pour quantifier le risque en évaluant la disponibilité du système attaqué. En particulier, la méthode se concentre sur le risque de cyber-attaque dans la couche physique, appelé le risque "cyber-to-physical" (C2P) dans (Huang et al., 2018).

Face au manque de données historiques, une approche de probabilité floue (Fuzzy Probability Bayesian Network FPBN) a été présentée pour l'évaluation dynamique des risques de cybersécurité dans les ICSs (Zhang et al., 2017b). La complexité de la structure du réseau des ICSs pose quelques problèmes pour l'évaluation de la sécurité, mais le BN peut facilement décrire les interdépendances entre les composants du réseau.

Zhang et .al (Zhang et al., 2015) ont conçu une nouvelle approche multi-modèle de prédiction des incidents et d'évaluation dynamique des risques de cybersécurité pour les ICSs. Leur méthode est également basée sur un réseau bayésien à plusieurs couches. Dans les travaux de (Zhang et al., 2017b), le modèle FPBN est utilisé pour analyser et prévoir le risque de cybersécurité, l'algorithme d'inférence dynamique approximative floue vise à évaluer le risque de cybersécurité. L'approche FPBN est expliquée en détail dans leur article.

Une approche d'évaluation dynamique de l'impact basée sur les actifs a été présentée dans(Li et al., 2017) pour l'analyse des risques. Cette approche se compose de deux parties : un modèle d'actifs dynamique et orienté objet et un modèle de propagation de l'impact des cyberattaques, où le modèle d'actifs dynamique est construit sur la base de réseaux de Petri (Petri Nets PN), et le modèle de propagation de l'impact des cyberattaques est construit en intégrant les cyberattaques dans le modèle d'actifs, ce qui permet

de déduire comment les cyberattaques se multiplient.

Popov (2015) (Popov, 2014) présente une approche pour la modélisation stochastique des systèmes critiques de sûreté en tenant compte à la fois des défaillances aléatoires et des attaques malveillantes. En particulier, l'approche ne prend en compte que les attaques qui peuvent conduire à l'état de non-sûreté de fonctionnement du dispositif. En tenant compte une modélisation probabiliste des défaillances et des attaques, il est possible de quantifier le risque des cyberattaques.

Approches basées sur HAZOP

(Wei et al., 2015) décrivent une approche basée sur HAZOP, dans laquelle ils s'efforcent d'inclure les informations relatives à la sécurité dans l'analyse des dangers en incluant des mots-guides issus de la taxonomie des attaques d'organisation CERT (Computer Emergency Response Team). Les auteurs se concentrent sur la phase de conception du système et étendent des mots-guides en réutilisant la taxonomie des attaques de l'équipe CERT. L'approche fournit des informations détaillées sur un ensemble de mots-guides primaires et secondaires et leurs combinaisons. (Ito, 2014) propose une analyse pour l'identification des menaces et des dangers comme extension de l'approche d'identification des dangers CARDION. L'approche est itérative et comprend quatre phases : description du système ; identification de l'objectif principal et sa décomposition ; application des mots-guides de l'étude des dangers et de l'opérabilité (HAZOP) à chaque objectif et l'identification des menaces et des dangers. La description du système peut être réalisée avec UML(Unified Modeling Language) , SysML (Systems Modeling Language) (D'souza and Wills, 1998).

Formalisme des processus de Markov à logique booléenne Boolean logic Driven Markov Process BDMP

(Kriaa et al., 2014) proposent une étude de cas sur un système de contrôle industriel dans lequel le formalisme des processus de Markov à logique booléenne (BDMP), précédemment développé, est utilisé pour modéliser les interdépendances entre la SAF et la SEC. L'approche permet de réfléchir sur les contradictions entre SAF et SEC, ainsi que sur la dépendance conditionnelle et le renforcement mutuel entre les deux. L'étude de cas illustre la capacité des BDMP non seulement à évaluer les risques, mais aussi à optimiser le choix des contre-mesures contre les attaques. L'analyse est effectuée comme une seule activité conjointe pour traiter à la fois de la SAF et de la SEC, mais elle peut dépendre d'autres activités de SAF/SEC pour sa contribution.

(Kriaa et al., 2015) présentent une approche de l'évaluation conjointe des risques qui peut être appliquée à la fois pour la conception et les phases opérationnelles du système. L'approche S-cube (modélisation de la SAF et de la SEC SCADA) prend en compte l'architecture du système et fournit des scénarios d'attaques et de défaillances pouvant entraîner des risques donnés. Elle s'appuie sur une base de connaissances des risques en matière de SAF et de SEC et utilise le langage Figaro pour modéliser différents composants du système, chacun étant associé à des modes de défaillance et des attaques connexes.

Approches basées sur UML

Apvrille et Roudier (2015) (Apvrille and Roudier, 2015) proposent d'utiliser SysML-Sec pour étudier l'impact éventuel de la mise en place de solutions de sécurité sur les fonctions de la SAF des systèmes embarqués et cyberphysiques (CPS). SysML-Sec adapte une

approche orientée vers les objectifs pour la capture des exigences et une approche orientée vers les modèles pour la spécification de l'architecture et des menaces. Dans le cadre de l'analyse, les ressources à protéger et leur lien avec les exigences de SAF et de SEC sont identifiées. La méthode d'analyse est basée sur Y-chart (Balarin et al., 2003) et le cycle en V. L'analyse est assistée par un logiciel libre TTool pour la spécification et la vérification du modèle, et par AVATAR pour l'analyse des exigences et des attaques. SysML-Sec évalue la compatibilité des exigences de SEC en ce qui concerne la SAF du système aux stades de la conception.

Nicklas et al. (2016) (Nicklas et al., 2016) proposent une approche basée sur l'ingénierie des systèmes qui consiste un modèle basé sur le SySML afin d'établir une conception sûre et sécurisée des CPS. Dans un premier temps, une définition du système est fournie par l'analyse générique de l'ingénierie des systèmes. Ensuite, identifier les scénarios d'attaques possibles. Une évaluation qualitative des probabilités d'occurrence d' attaque. Dans l'étape finale, les éventuels conflits de SAF-SEC liés au cas d'utilisation sont harmonisés dans un diagramme de séquence pour atteindre un niveau de SEC et de SAC suffisant.

(Raspotnig et al., 2012) présentent l'évaluation combinée des dangers de la SAF et de la SEC des systèmes d'information (Combined Harm Assessment of Safety and Security for Information Systems - CHASSIS) qui est une approche de haut niveau combinant des méthodes de la SAF et SEC afin de fournir une approche d'évaluation conjointe notamment utilisée aux premières phases de la conception. L'approche est basée sur la modélisation Misuse et des diagrammes de séquences dans un diagramme de comportement UML et fournit comme résultat les spécifications de la SEC et de la SAF.

Approche : D-MILS (Distributed Multiple Independent Levels of Security)

Cimatti et al. (2015) (Cimatti et al., 2014) présentent une vue d'ensemble de l'approche D-MILS pour la vérification des exigences de la SAF et de la SEC. Les deux types d'exigences sont attribués aux composants du système et formalisés par des contrats de composants. La vérification des exigences dans un système donné peut être effectuée en vérifiant le raffinement des contrats entre les contrats des composants du système. Le résultat de l'analyse de raffinement peut être visualisé sous forme d'arbres de défaillance montrant les dépendances des défaillances du système et de ses composants.

Approches basées sur GORE (Goal-Oriented Requirements Engineering)

Ponsard et al. (Ponsard et al., 2016) présentent une approche qui utilise les techniques de l'ingénierie des exigences orientées vers des buts (Goal-Oriented Requirements Engineering GORE), pour co-ingérer la SAF et la SEC. L'approche prend les résultats de l'analyse de la SAF et de la SEC pour créer un arbre de buts reliant les exigences aux dangers et aux menaces où chaque objet peut être marqué comme étant pertinent pour la SAF ou la SEC. L'analyse des exigences en matière de SEC et de SAF est effectuée conjointement, bien que la contribution à cette technique des activités d'identification des dangers/menaces puisse provenir de différentes sources.

Approches basées sur l'analyse systématique des défauts et des erreurs (Systematic Analysis of Faults and Errors SAFE)

Procter et al. (Procter et al., 2017) étendent l'analyse systématique des défauts et des erreurs (Systematic Analysis of Faults and Errors SAFE) afin de mieux intégrer le concept

de la SEC dans la SAF. Dans cet article, les auteurs soutiennent que le modèle Dolev-Yao permet une meilleure intégration de la SEC et de la SAF, le modèle est étendu avec des mots-clés pour tenir compte à la fois de la SAF et de la SEC.

Approches basées sur l'AFT (Attacks Faults Tree)

Ruijters et al. (Ruijters et al., 2017) présentent un modèle uniformisé permettant de fusionner l'analyse de l'arbre d'attaque (ATA) et analyse de l'arbre de fautes (AFA) dans un seul arbre d'analyse AFT (Attacks Faults Tree). L'outil développé fournit une transformation bidirectionnelle entre le modèle AFT joint et les modèles indépendants. Le modèle AFT peut être validé par un l'outil UPPAAL qui est un environnement pour la modélisation, la validation et la vérification de systèmes cyber-physiques afin d'avoir une analyse quantitative.
Steiner et Liggesmeyer (2015)(Steiner and Liggesmeyer, 2014) proposent une analyse des arbres de défaillance des composants de sécurité renforcée (Security Enhanced Component Fault Trees SeCFTs). Afin de déterminer les probabilités des causes liées à la SAF, c'est-à-dire de mener une analyse quantitative, les événements de base sont regroupés en ensembles de coupes minimales (Minimal Cut Sets MCS), et les probabilités sont attribuées à des ensembles plutôt qu'à des événements. Les valeurs des probabilités sont choisies dans l'ensemble discret conforme à la classification de la norme IEC 61025 (Commission et al., 2006b). L'analyse qualitative dans le cadre de l'approche est basée sur l'identification de tous les MCS et leur traitement en fonction de la nature des événements inclus, c'est-à-dire la SEC, la SAF ou un mélange des deux.

(Silva and Lopes, 2013) décrivent les mesures qui ont été prises pour certifier un système de sécurité critique dans le domaine ferroviaire et expliquent comment la sécurité peut être assurée sans mettre en danger la fiabilité ou la sûreté. Dans cet article, ils emploient l'analyse des modes de défaillance, des vulnérabilités et des effets (Failure Modes, Vulnerabilities and Effect Analysis FMVEA) et l'analyse des Arbres de Défaillance (Fault Tree Analysis FTA), où pour chaque événement de défaillance de SAF, ils déduisent les événements défaillances de SEC possibles.

Approche IFDs (Diagrammes de Flux d'Information)

Sabaliauskaite et al. (Ruijters et al., 2017) étendent le modèle en six étapes de conception des CPSs sûrs et sécurisés avec un soutien pour l'identification des défaillances possibles et des cyberattaques. Dans les deux premières étapes de l'approche, les fonctions/ exigences sont définies en même temps que l'architecture du système. Au cours des deux étapes suivantes, les défaillances et les mesures de sûreté correspondantes sont ajoutées au modèle. Au cours des deux dernières étapes, les attaques et les contre-mesures de sécurité correspondantes sont ajoutées au modèle.

Approche EVITA (E-safety Vehicle Intrusion Protected Applications)

EVITA (E-safety vehicle intrusion protected applications) (SIT, 2008) est un modèle d'analyse des risques qui a été proposé pour évaluer le risque associé aux attaques, mais aussi la gravité des conséquences possibles pour les parties prenantes et la probabilité qu'une telle attaque puisse être menée à bien. Ce modèle adopte une approche de l'analyse des risques centrée sur l'attaquant. EVITA identifie quatre objectifs de sécurité de haut niveau : (a) la SEC opérationnelle, (b) la protection de la vie privée, (c) la SEC financière et (d) la SAF. Pour effectuer l'évaluation des risques en considérant la SAF comme

un objectif de la SEC, EVITA adopte l'approche de détermination ASIL (Automotive Safety Integrity Level) telle que proposée dans la norme ISO 26262 [ISO (International Organization for Standardization). Road vehicles — Functional safety — Part 3 : Concept phase (ISO 26262-3 :2011). ISO 26262-3 :2011. 2011 (page 18).]. D'une manière générale, la "probabilité d'attaque combinée" utilisée dans EVITA est analogue à la détermination de l'ASIL dans la norme ISO 26262. L'objectif du projet EVITA est de concevoir, de vérifier et de prototyper une architecture pour les réseaux automobiles embarqués où les composants importants pour la sécurité sont protégés contre les manipulations des données sensibles et contre les compromis. Ainsi, EVITA fournira une base pour le déploiement d'électroniques de SAF basées sur la communication de véhicule à véhicule (V2V) et de véhicule à infrastructure (V2I). Une activité clé du projet EVITA est la saisie des exigences de sécurité pour l'architecture du système sûr et les composants logiciels et matériels associés, sur la base d'un ensemble de cas d'utilisation et des scénarios de menace (dark-side scenarios) de la sécurité. La méthode EVITA aborde la question de la SAF après avoir identifié les menaces à la SEC. Une valeur de risque de la SAF est affectée, si la menace influence la SAF. Cela signifie que ces techniques ne se concentrent pas explicitement sur l'identification de la menace concernant la SAF. Les méthode n'intègrent pas ou ne revendiquent pas une analyse de la SAF dans leur description.

L'inconvénient des méthodes basées modèle est la difficulté de générer des modèles lorsque il s'agit d'un système réel complexe. Pour comparer les différentes méthodes de la littérature, nous avons pour chacune d'elle, identifier les critères que nous avons définis. La classification est présentée dans les tableaux (2.1, 2.2, 2.3, 2.4).

Méthodes	GTST-MLD (Di Maio et al., 2019)	CHASSIS (Raspotnig et al., 2012)	TVRA (Reichenbach et al., 2012)	FMVEA (Silva and Lopes, 2013) (Schmittner et al., 2014a)	STAP-SEC (Shapiro, 2016) (Schmittner et al., 2016) (Schmittner et al., 2016) (Howard et al., 2017)	STAP-SEC SAFE (Pereira et al., 2017)	BBA (Kornecki et al., 2013)	Nist 800-13 (Chen et al., 2014)
Identification des risques	✓	✓	✓	✓	✓	✓	✓	✓
Analyse des risques	✓		✓	✓	✓	✓	✓	✓
Évaluations des risques			✓				✓	✓
Domaine d'application	Générique	Trafic aérien	ICS	Ferroviaire Automobile	Générique	Générique	Générique	Nucléaire
Quantitative	✓						✓	✓
Qualitative			✓	✓	✓			
Parallèle			✓					
Unifiée		✓		✓	✓			✓
SEC basé sur la SAF	✓	✓	✓	✓				
Co-Analyse SAF et SEC					✓	✓	✓	
Phase de conception	✓	✓	✓	✓	✓		✓	✓
Phase opérationnelle	✓	✓		✓	✓		✓	✓
Graphique	✓							
Évaluation des vulnérabilités								
Standard	Non	Non	IEC61508	61508 IEEE1474 13 IEC 61508 27000 18	Non	Non	Non	NIST -800 30
Évaluation probabiliste de sécurité	✓		✓				✓	✓

TABLEAU 2.1 – Résumé d'une partie des approches existantes

Méthodes	CARDION+ HAZOP (Ito, 2014)	BDMP (Kriaa et al., 2014)	SysML-SEC (Apvrille and Roudier, 2015)	D-MILS (Cimatti et al., 2014)	S-cube (Kriaa et al., 2015)	SAHARA (Macher et al., 2014)	Modélisation Stochastique (Popov, 2014)	SecTFS (Steiner and Liggesmeyer, 2014)
Identification des risques	✓	✓	✓	✓	✓	✓	✓	✓
Analyse des risques	✓	✓	✓	✓	✓	✓	✓	✓
Évaluations des risques		✓			✓	✓	✓	✓
Domaine d'application	Automobile	Générique	Automobile	Générique	SCADA	Automobile	Automobile	Générique
Quantitative		✓	✓	✓	✓	✓	✓	✓
Qualitative	✓	✓	✓	✓	✓	✓		✓
Parallèle			✓					
Unifiée	✓	✓		✓	✓	✓	✓	✓
SEC basé sur la SAF	✓		✓			✓		✓
Co-Analyse SAF et SEC	✓	✓		✓	✓		✓	
Phase de conception	✓	✓	✓	✓	✓	✓	✓	✓
Phase opérationnelle	✓	✓			✓	✓	✓	✓
Graphique		✓	✓	✓	✓		✓	✓
Évaluation des vulnérabilités								
Standard	ISO26262 ISO/IEC27000	Non	Non	Non	Non	26262	ISO26262	IEC61025 IEC60300
Évaluation probabiliste de sécurité		✓			✓	✓	✓	✓

TABLEAU 2.2 – Résumé d'une partie des approches existantes

Méthodes	HAZOP-SEC (Wei et al., 2015)	RAFAES (Islam et al., 2016)	Y-chart + SysML (Apvrille and Roudier, 2015)	Basé GORE (Ponsard et al., 2016)	STAMP (Troubitsyna, 2016)	SGM (Dürrwang et al., 2017)	FMEA+ STRIDE (Plósz et al., 2017)	SAFE (Procter et al., 2017)
Identification des risques	✓	✓	✓	✓	✓	✓	✓	✓
Analyse des risques	✓	✓	✓	✓	✓	✓	✓	✓
Évaluations des risques	✓	✓				✓		
Domaine d'application	Automobile	Automobile	Automobile	Automobile	Générique	Automobile	Générique	Médicale
Quantitative	✓	✓				✓		
Qualitative	✓	✓	✓	✓	✓	✓	✓	✓
Parallèle			✓					
Unifiée	✓	✓		✓	✓	✓	✓	✓
SEC basé sur la SAF	✓	✓	✓		✓	✓		✓
Co-Analyse SAF et SEC				✓			✓	
Phase de conception	✓	✓	✓	✓	✓	✓	✓	✓
Phase opérationnelle		✓	✓			✓	✓	✓
Graphique			✓	✓	✓	✓		
Évaluation des vulnérabilités								
Standard	Non	ISO26262 SAE3061	Non	61508 SAE3061	Non	ISO26262	Non	Non
Évaluation probabiliste de sécurité			✓					

TABLEAU 2.3 – Résumé d'une partie des approches existantes

Méthodes	basée AFT (Ruijters et al., 2017)	basée IFDS, (Ruijters et al., 2017)	STPA-sec + FMVEA (Temple et al., 2017)	Basé ISO26262 SAEJ3061 (Sae, 2016)	US^2 (Cui and Sabaliauskaite, 2018)	CAFSSAV (Cui et al., 2019)	EVITA (SIT, 2008)
Identification des risques	✓	✓	✓	✓	✓	✓	✓
Analyse des risques	✓	✓	✓	✓	✓	✓	✓
Évaluations des risques	✓		✓		✓		
Domaine d'application	Générique	Générique	Générique	Automobile	Automobile	Automobile	Automobile
Quantitative	✓		✓		✓	✓	✓
Qualitative			✓	✓	✓		✓
Parallèle							
Unifiée	✓	✓	✓	✓	✓	✓	✓
SEC basé sur la SAF			✓		✓	✓	✓
Co-Analyse SAF et SEC				✓			✓
Phase de conception	✓	✓	✓	✓	✓	✓	✓
Phase opérationnelle		✓		✓			✓
Graphique		✓	✓			✓	
Évaluation des vulnérabilités							
Standard	Non	IS9 99	EN501261	26262 SAE3061	26262 SAE3061	26262 SAE3061	ISO26262
Évaluation probabiliste de sécurité							

TABLEAU 2.4 – Résumé d'une partie des approches existantes

2.3 Critique et synthèse

D'abord, nous avons constaté que de nombreux travaux sont abstraits et manquent d'évaluation approfondie. De plus, en analysant ses travaux nous nous sommes rendus compte que la difficulté de l'analyse conjointe entre la SAF et la SEC réside dans le manque de langage commun standard qui permet d'établir une communication claire. En outre, nous avons remarqué que les approches présentées n'ont pas traité la problématique des mises à jour et les recommandations proposées par les fournisseurs des technologies, lors la découverte d'une nouvelle vulnérabilité. En fait, la SEC est de nature dynamique (Johnson et al., 2016) ce qui implique des mises à jour fréquentes des systèmes en réponse à une nouvelle attaque en cours de développement ou à une nouvelle vulnérabilité exploitée. Une telle mise à jour nécessite une analyse de leur impact sur la sûreté de fonctionnement. C'est pour cette raison, que nous allons proposer un système d'évaluation de risque qui va intégrer des métriques temporelles qui mesurent les corrections proposées par les fournisseurs (exp. dans le chapitre suivant : La métrique de remédiation (RL)). Il est évident que des efforts supplémentaires sont nécessaires pour proposer de nouvelles approches et évaluer les approches existantes en vue d'offrir un langage standard qui facilite la collaboration et la communication entre des équipes qui viennent de deux communautés différentes (la SAF et la SEC). En conséquence, nous devons proposer une approche :

- qui doit être plus dynamique et plus rapide, applicable à la fois dans la phase de conception et dans la phase opérationnelle. En effet, à chaque fois qu'il y a de nouvelles menaces, il y aura une suite des étapes qui devront être appliquées pour assurer la SAF et la SEC.

- qui soit facile à appliquer dans le cas des systèmes complexes. C'est pourquoi nous orientons notre recherche vers les méthodes orientées processus plutôt que les mé-

thodes basées sur les modèles. Par exemple, le manque de données sur les attaques et la nature dynamique des cyberattaques empêchent de trouver un fondement mathématique pour calculer la probabilité des attaques.

- qui permet d'avoir des résultats quantitatifs et qualitatifs, en vue d'offrir un langage standard qui facilite la collaboration et la communication entre des équipes interdisciplinaire.
- qui doit être générique et applicable à tous les domaines et qui doit suivre la norme générique IEC/ISA 62443 qui est adoptée par les organisations pour réduire le risque des cyberattaques.
- qui permettent d'évaluer les vulnérabilités et leur impact dans le cas d'une éventuelle exploitation en prenant en considération les recommandations et les mises à jour proposées par les fournisseurs des technologies. Car, nous sommes convaincus que la façon la plus pratique et la plus objective pour évaluer le risque des cyberattaques réside dans l'évaluation de la criticité des vulnérabilités et leur impact (voir l'équation 1.2).

A cet égard, plusieurs travaux ont été effectués dans ce sens par les grandes entreprises ou les fabricants de matériel et de logiciels afin de garder une trace des vulnérabilités associées à leurs produits. En effet, au cours des dernières années, certaines grandes compagnies de sécurité informatique et des organisations ont fourni des systèmes de notation pour classer les vulnérabilités des systèmes d'information (IT). Ces systèmes d'évaluation des risques ou de notation utilisent des systèmes de qualification simple. De nombreuses sociétés comme IBM, Symantec, Microsoft et Secunia ont créé leur propre système de notation des vulnérabilités appelé respectivement X Force, Symantec Security Response Threat Severity Assessment, Security Bulletin Severity Rating System (Sym, a; Spanos et al., 2013a). Le NVD (National Vulnérabilité Database) est une base de données qui a été créée par le gouvernement américain pour la gestion de la vulnérabilité (nvd,). Le NVD inclut des bases de données des défauts de logiciels liés à la sécurité, aux mesures d'exploitation et à leurs impacts. Le NVD est compatible avec les normes CVSS (Common Vulnerability Scoring System) v2.0 et v3.0 (nvd,). La base de données du NVD fournit des mesures de base CVSS qui donnent le score quantitatif de chaque vulnérabilité. L'équipe ICS-CERT (Industrial Control Systems Cyber Emergency Response Team) collabore avec les équipes CERTs (Computer Emergency Response Teams) et du secteur privé pour partager les incidents de sécurité liés aux systèmes de contrôle et les mesures correctives ou d'atténuation des risques (ics,). Le Symantec Security Response Threat Severity Assessment (Sym, b) évalue les menaces informatiques (virus, vers, chevaux de Troie et macros) et les classe dans des catégories de risque clairement définies pour les utilisateurs (Sym, c). Chaque menace est classée par ordre de criticité (élevée, moyenne ou faible) basée sur le nombre de systèmes informatiques touchés. Les trois principales composantes de la menace prises en compte par Symantec pour déterminer le niveau de criticité sont la mesure dans laquelle un programme malveillant est invisible, les dommages qu'il cause et sa vitesse de propagation. En 2005, le National Infrastructure Assurance Council (NIAC) du gouvernement des États-Unis a publié le premier système ouvert de notation des vulnérabilités, CVSS, à travers la version 1 (FIR, b). Par la suite, plusieurs améliorations ont été publiées (Mell and Scarfone, 2007; Scarfone and Mell, 2009). De plus, CVSS a été utilisé dans plusieurs études pour estimer les paramètres de sécurité, tels que le temps moyen de compromis MTTC (McQueen et al., 2006).

Au cours de ces dernières années, plusieurs chercheurs ont tenté d'adapter le CVSS aux systèmes d'OT (Opération Technologies). Le réseau sans fil Bluetooth à basse consommation (BLE) est utilisé pour démontrer la faiblesse de la version 2 de CVSS (Qu and Chan, 2016). Ensuite, le système de notation des vulnérabilités dans la robotique (RVSS) (Open Robot Vulnerability Scoring System) est proposé pour les systèmes robotiques (Vilches et al., 2018).
Nous pensons à exploiter ce principe de notation pour avoir une modélisation plus raffinée basée sur des métriques de sécurité qui modélisent mieux les risques pour les systèmes industriels.

Dans les chapitres suivants, nous allons présenter une méthodologie basée sur le CVSS qui focalise sur l'évaluation des vulnérabilités et leur impact et qui respecte les critères présentés dans ce chapitre.

Chapitre 3

ICVSS : Nouvelle méthodologie pour noter les vulnérabilités des systèmes de contrôle-commande industriel

Contents

3.1 Introduction

L'évaluation des risques des cyberattaques dans un système industriel nécessite un inventaire et une classification des vulnérabilités en fonction de leurs gravités. En effet, la gravité d'une vulnérabilité est déterminée par son impact sur la vie des personnes, sur

l'environnement.
Comme nous venons de le voir, un certain nombre de systèmes de notations ou de score des vulnérabilités ont été présentés au cours des deux dernières décennies qui permettent d'estimer la gravité des vulnérabilités. En 2005, le premier système ouvert de notation des vulnérabilités CVSS ((Common Vulnerability Scoring System) avec la version 1 (FIR, b) a été publié par le National Infrastructure Assurance Council (NIAC) du gouvernement américain. En 2007, le FIRST (The Forum of Incident Response and Security Teams) a adopté et amélioré le système de notation par le biais de la version 2, en couvrant les lacunes de la version 1 (Spanos et al., 2013a). La version 3 du CVSS a été publiée en 2014. Le CVSS est le fruit d'un effort conjoint impliquant de nombreux groupes dont : CERT/CC, Cisco, DHS/MITRE, eBay, IBM, Internet Security Systems, Microsoft, Qualys, Symantec. Depuis, plusieurs travaux ont été publiés pour comparer les deux dernières versions et d'autres travaux pour présenter de nouveaux systèmes de notation (Anikin, 2017)(Ko et al., 2014)(Zhang et al., 2017a)(Keramati, 2016)(Spanos et al., 2013b)(Allodi et al., 2018)(Gallon and Bascou, 2011) .

Le CVSS est un système de score largement utilisé dans le monde de la cybersécurité et la "Cybersecurity and Infratructure Security Agency" (CISA) (ics,) publie systématiquement des vulnérabilités des ICSs en utilisant le CVSS.

L'avantage de CVSS réside dans sa simplicité et sa richesse avec des métriques qui captent la quasi-totalité des mesures de la cybersécurité qui sont réparties sur trois groupes de métriques : métriques de base, environnementales, et temporelles. L'objectif du groupe de base est de définir et de communiquer les caractéristiques fondamentales d'une vulnérabilité. Cette approche objective de la caractérisation des vulnérabilités fournit aux utilisateurs une représentation claire et intuitive d'une vulnérabilité. Les utilisateurs peuvent ensuite invoquer les groupes temporels et environnementaux pour fournir des informations contextuelles qui reflètent plus précisément la présence d'un risque pour leur environnement spécifique. Cela leur permet de prendre des décisions plus précises et efficaces pour atténuer les risques posés par les vulnérabilités selon l'environnement et/ou le temps.

De plus, le CVSS permet d'obtenir un score associé à un vecteur qualitatif qui exprime la valeur affectée à chaque mesure. En effet, un texte compressé est défini par CVSS pour représenter dans la forme d'un vecteur la valeur associée à chaque métrique. Les valeurs des métriques utilisées ont été établies par des experts (membres du CVSS-SIG) (Spanos et al., 2013a). Le CVSS décrit précisément les critères utilisés par chaque mesure. Ces métriques sont décrites dans les sections suivantes.

L'objectif de ce chapitre est dans un premier temps de présenter les différentes métriques du CVSS. Ensuite, nous montrons les limites du CVSS dans le cas des ICSs. Puis, nous proposons un premier système de notation destiné spécialement aux systèmes de contrôles industriels avec le souci de créer une voie de communication entre les ingénieurs de la SAF et ceux de la SEC. Le système proposé est basé sur la version 2 du CVSS. Elle offre une meilleure précision de l'évaluation des vulnérabilités, qui permet de se rapprocher le plus possible du risque réel en tenant compte des spécifications des ICSs.

3.2 Système commun de notation de la vulnérabilité CVSS Version 2 d'un IT

Actuellement, la gestion des risques des cyberattaques consiste à identifier et à évaluer les vulnérabilités de nombreuses plateformes matérielles et logicielles variées. Les ingénieurs étudiant les cyberattaques doivent classer ces vulnérabilités par ordre de priorité et remédier à celles qui présentent le plus grand risque. Dans le passé, les instituts de recherches publiaient chaque jour des nouvelles vulnérabilités à corriger, et chacun utilisait une évaluation selon une échelle différente (kb.,) (Mell et al., 2007). Ensuite, les chercheurs ont posé la question : Comment pouvons-nous convertir cette grande quantité de données publiées chaque jour sur les vulnérabilités en informations exploitables? Le système commun de notation des vulnérabilités (CVSS) est un cadre de travail ouvert qui aborde cette question. L'utilisation de CVSS offre les avantages suivants :

- **Scores de vulnérabilité standardisés :** La normalisation des scores de vulnérabilité sur l'ensemble de ses plateformes logicielles et matérielles, cela permet aussi par la suite de mettre en place une politique unique de gestion des vulnérabilités. Cette politique peut être similaire à un accord de niveau de service (SLA / Service-Level Agreement) qui indique la rapidité avec laquelle une vulnérabilité particulière doit être validée et corrigée. Cette rapidité doit être proportionnelle avec la gravité de la vulnérabilité.
- **Cadre de travail ouvert :** Tout le monde peut voir les caractéristiques, les configurations ou l'ensemble des métriques qui permettent d'avoir le score final.
- **Priorisation des Risques :** les scores de vulnérabilité sont représentatifs du risque réel de l'organisation. Les utilisateurs connaissent l'importance ou la gravité d'une vulnérabilité donnée par rapport à d'autres vulnérabilités.
  Le CVSS est composé de trois groupes métriques : métriques de base, temporelle et environnementale. Chacun consistant en un ensemble de mesures, comme le montre la figure 3.1.

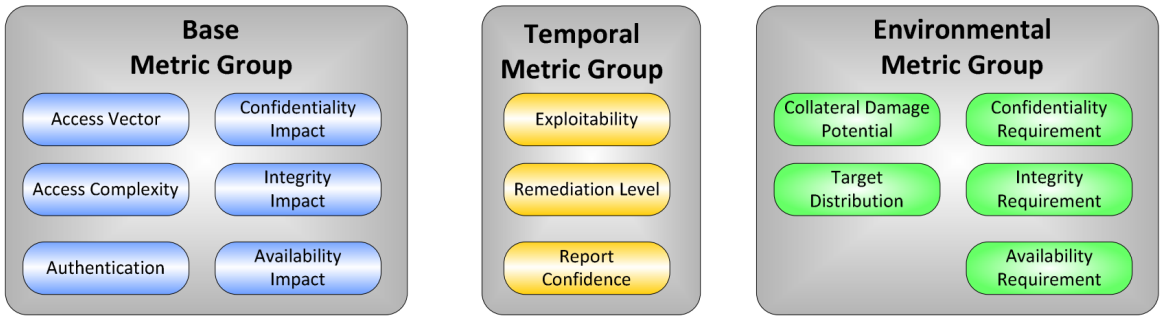


FIGURE 3.1 – Groupes de métriques CVSS (Mell et al., 2007).

3.2.1 Comment CVSS fonctionne?

Le fonctionnement du CVSS consiste à calculer trois groupes de métriques de : base, temporelle et environnementale. Lorsque des valeurs sont attribuées aux métriques de base, nous obtenons un score compris entre 0 à 10 et un vecteur contenant les valeurs qualitatives correspondantes (voir la figure 3.2). Le vecteur représente ici la nature "ouverte" du cadre. Il s'agit d'une chaîne de texte qui contient les valeurs attribuées à chaque

métrique et qui est utilisée pour indiquer exactement comment le score de chaque vulnérabilité est obtenu. Par conséquent, le vecteur doit toujours être affiché avec le score de la vulnérabilité. Les vecteurs sont expliqués en détail dans les sections suivantes.

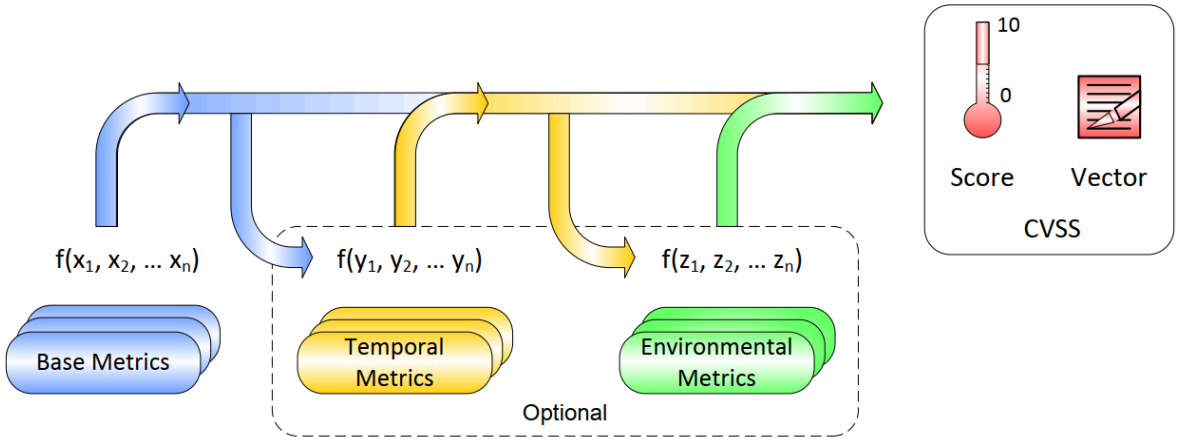


FIGURE 3.2 – Métriques et équations du CVSS (Mell et al., 2007).

3.2.2 Métriques de base

Les métriques de base reflètent les caractéristiques intrinsèques et fondamentales d'une vulnérabilité qui sont constantes au fil du temps et indépendants de l'environnement des utilisateurs. Les mesures du vecteur d'accès, de la complexité de l'accès et de l'authentification montrent comment une vulnérabilité est accessible et s'il faut réunir d'autres conditions supplémentaires pour l'exploiter. Les trois paramètres de l'impact mesurent les conséquences d'une vulnérabilité. L'impact est défini comme le degré de perte de confidentialité (C), d'intégrité (I) et de disponibilité (A). Par exemple, une vulnérabilité pourrait entraîner une perte partielle d'intégrité et de disponibilité, mais non pas de perte de confidentialité. Les métriques de base sont :

Vecteur d'accès (Access Vector AV)

Cette mesure reflète la manière dont la vulnérabilité est exploitée. Le principe est simple, plus l'attaquant a la capacité de pirater l'actif ou la cible, plus le score de vulnérabilité est élevé. Elle spécifie si pour exploiter une vulnérabilité, l'attaquant aurait besoin : a) d'un contact physique avec la machine (Physique),

b) d'un accès aux réseaux adjacents (Réseau adjacent),

c) d'un accès à une structure de réseau local au sein de l'organisation ou accès depuis un réseau externe (Network).
Les valeurs possibles (voir le tableau 3.1) pour cette mesure sont énumérées comme suit :

- *Local (L = 0.2) :* Une vulnérabilité exploitable avec uniquement un accès local nécessite que l'attaquant ait soit un accès physique au système vulnérable, soit un compte local (shell). Les exemples de vulnérabilités exploitables localement sont les attaques périphériques telles que les attaques Firewire/USB DMA (Direct Memory Access), et les mécanismes locaux permettant à un utilisateur d'obtenir des privilèges supérieurs à

Métrique ou critère	**Notation**		
Vecteur d'accès	Local (L)	Réseau adjacent (A)	Réseau (Network N)
Valeur	0,2	0.646	1.0

TABLEAU 3.1 – Métrique : vecteur d'accès

ceux qu'il a normalement (escalade de privilèges local, par exemple la commande *sudo*) (kb.,).

- *Réseau adjacent (A =0.646) :* Une vulnérabilité exploitable avec un accès à un réseau adjacent nécessite que l'attaquant ait l'accès au domaine de diffusion d'actif vulnérable. Parmi les exemples de réseaux locaux : sous-réseau IP local, Bluetooth, IEEE 802.11 et le segment Ethernet local.

- *Réseau (Network N = 1.0) :* Une vulnérabilité exploitable avec un accès au réseau signifie que l'actif vulnérable est lié à la couche réseau et que l'attaquant n'a pas besoin d'un accès au réseau local ou d'un accès local. Une telle vulnérabilité est souvent appelée "exploitable à distance "(remotely exploitable). Un exemple d'attaque de réseau est RPC (Remote Procedure Call) qui cause un dépassement de tampon.

Les pondérations ont été conçues en conséquence et supposent que l'accès physique est généralement le plus difficile (donc moins pondéré), puisque les produits logiciels fonctionnent dans des environnements de serveurs restreints et surveillés. Cette hypothèse ne s'applique toutefois pas à tous les systèmes. Par exemple, dans le cas des robots organisées en réseaux, ils sont alors considérés comme un système OT. Certains types de robots peuvent travailler dans des installations industrielles dont l'accès physique est restreint, tandis que d'autres peuvent opérer dans des zones publiques, où n'importe qui peut physiquement accéder aux robots (par exemple : robots-car, robots de soins de santé, etc.). De même, les robots sont généralement conçus avec plusieurs - au moins deux - couches de réseau. En général, un réseau externe - utilisé pour faire fonctionner et surveiller le robot - ou un réseau interne - où tous les composants et modules distribués échangent des informations pour réaliser le comportement souhaité - sont souvent accessibles par un contact physique.

Complexité d'accès (AC)

Cette métrique mesure la complexité de l'attaque nécessaire pour exploiter la vulnérabilité une fois que l'attaquant a accédé au système cible. D'autres vulnérabilités, cependant, peuvent réclamer des mesures supplémentaires afin d'être exploitées. Par exemple, une vulnérabilité au niveau d'un client de messagerie n'est exploitée que lorsque que l'utilisateur télécharge et ouvre une pièce jointe. Trois valeurs possibles existent : faible, moyenne et élevée. Plus la complexité requise est faible, plus le score de vulnérabilité est élevé :

- *Élevée (High / H = 0.35) :* Des conditions d'accès spéciales existent. Par exemple :
  - Dans la plupart des configurations, l'attaquant doit déjà disposer de privilèges supérieurs à la normale (par exemple, DNS hijacking).
  - L'attaque dépend des méthodes d'ingénierie sociale (une méthode de manipulation

Métrique ou critère	**Notation**		
Complexité d'accès (AC)	Élevée (High H)	Moyenne (Médium M)	Faible (L)
Valeur	0.35	0.61	0.71

TABLEAU 3.2 – Métrique : Complexité d'accès

utilisée par les attaquants pour inciter les victimes à partager leurs informations confidentielles. facilement détectables par des personnes bien informées. Par exemple, la victime doit effectuer plusieurs actions suspectes ou atypiques.
- La configuration vulnérable est très rarement observée dans la pratique.

- *Moyenne (Médium /M = 0.61) :* Les conditions d'accès sont plutôt spécialisées ; en voici quelques exemples : - La partie attaquante est limitée à un groupe de systèmes ou d'utilisateurs ayant un certain niveau d'autorisation.
  - Certaines informations doivent être recueillies avant qu'une attaque ne soit lancée avec succès.
  - La configuration affectée n'est pas celle par défaut, et n'est pas couramment configurée (par exemple, une vulnérabilité présente lorsqu'un serveur effectue l'authentification d'un compte utilisateur via une configuration spécifique, mais non présente pour une autre configuration d'authentification).
  -L'attaque nécessite un peu d'ingénierie sociale qui pourrait parfois tromper les utilisateurs attentifs (par exemple, les attaques de phishing qui modifient la barre d'état d'un navigateur web pour afficher un faux lien).

- *Faible (Low /L = 0.71) :* Dans ce cas, les conditions d'accès spéciales ou des circonstances atténuantes n'existent pas. En voici quelques exemples :
  - Le produit concerné nécessite généralement l'accès à un grand nombre de systèmes et d'utilisateurs, éventuellement anonymes et non fiables (par exemple, un serveur web).
  - La configuration affectée est omniprésente.
  - L'attaque peut être effectuée manuellement et ne nécessite que peu de compétences ou de collecte d'informations supplémentaires.

Authentification (Au)

Cette métrique mesure le nombre de fois qu'un attaquant doit s'authentifier auprès d'une cible afin d'exploiter une vulnérabilité. La métrique ne mesure pas la force ou la complexité du processus d'authentification, mais seulement le fait qu'un attaquant doit fournir des informations d'identification avant de lancer une attaque. Si la commande n'est disponible qu'après une authentification réussie, alors la vulnérabilité doit être classée comme "Unique" sinon elle est classée comme "Multiple", en fonction du nombre de fois que l'authentification doit avoir lieu avant d'exploiter la commande.

Il est important de noter que la métrique d'authentification est différente du vecteur d'accès. Les valeurs possibles sont les suivantes :

- *Multiple (M = 0.45) :* L'exploitation de la vulnérabilité exige que l'attaquant s'authentifie deux fois ou plus, même si les mêmes identifiants sont utilisés à chaque fois. Par exemple, un attaquant s'authentifie sur un système d'exploitation en plus de fournir des informations d'identification pour accéder à une application hébergée sur ce système.

Métrique ou critère	**Notation**		
Authentification (Au)	Aucun (N)	Unique (S)	Multiple (M)
Valeur	0.704	0.56	0.45

TABLEAU 3.3 – Métrique : authentification

- *Unique (Single / S = 0.56) :* Une seule authentification est nécessaire pour accéder à la vulnérabilité et l'exploiter.
- *Aucun (None / N = 0.704) :* L'authentification n'est pas nécessaire pour accéder à la vulnérabilité et l'exploiter.

Critères relatifs à l'impact de la vulnérabilité.

L'impact d'une attaque est décrit à travers 3 métriques : l'impact sur la Confidentialité (C) des données traitées , l'impact sur l'Intégrité (I) des données utilisées par le système et l'impact sur la Disponibilité (A) du système ou du service.

Impact sur la confidentialité (C)

Cette métrique mesure l'impact sur la confidentialité d'une vulnérabilité exploitée avec succès. La confidentialité consiste à limiter l'accès aux informations et leur divulgation aux seuls utilisateurs autorisés, ainsi qu'à empêcher l'accès ou la divulgation d'informations par des personnes non autorisées. L'augmentation de l'impact de la confidentialité augmente le score de vulnérabilité. Pour cette métrique, les valeurs possibles sont :

- *Aucune (None /N=0) :* Il n'y a pas d'impact sur la confidentialité du système.
- *Partiel (P=0.275) :* Il y a une divulgation considérable d'informations. L'accès à certains fichiers du système est possible, mais l'attaquant n'a pas de contrôle sur ce qui est obtenu, ou l'ampleur de la perte est limitée. Par exemple, une vulnérabilité qui ne divulgue que certains tableaux dans une base de données.
- *Complète (C=0.660) :* Il y a une divulgation totale des informations, ce qui entraîne la divulgation de tous les fichiers du système. L'attaquant est capable de lire toutes les données du système (mémoire, fichiers, etc.).

Impact sur l'intégrité (I)

Cette métrique mesure l'impact sur l'intégrité d'une vulnérabilité exploitée avec succès. L'intégrité fait référence à la garantie de la fiabilité et la véracité des informations. Un impact plus important sur l'intégrité augmente le score de vulnérabilité. Les valeurs possibles pour cette métrique sont :

- *Aucune (None /N=0.0) :* Il n'y a aucun impact sur l'intégrité du système.
- *Partiel (P=0.275) :* La modification de certains fichiers ou informations du système est possible, mais l'attaquant n'a pas de contrôle sur ce qui peut être modifié ou la portée de l'attaque est limitée. Par exemple, les fichiers du système ou des applications peuvent être écrasés ou modifiés. Dans ce cas, l'attaquant n'a soit aucun contrôle sur les fichiers qui sont affectés, soit il ne peut modifier les fichiers que dans un contexte limité.

- *Complète (C=0.66)* Il y a un compromis total de l'intégrité du système. Il y a une perte totale de la protection du système, ce qui compromet l'ensemble du système. L'attaquant est capable de modifier n'importe quel fichier du système cible.

Impact sur la disponibilité (Availability /A)

Cette métrique mesure l'impact sur la disponibilité d'une vulnérabilité exploitée avec succès. La disponibilité fait référence à l'accessibilité des ressources d'informations. Les attaques qui consomment la bande passante du réseau, les cycles de processeur ou l'espace disque ont toute un impact sur la disponibilité d'un système. Le score de la vulnérabilité est propositionnel à l'impact de la disponibilité. Les valeurs possibles pour cette métrique sont :

- *Aucun (None /N = 0.0) :* Il n'y a pas d'impact sur la disponibilité du système.
- *Partiel (P = 0.275) :* Les performances sont réduites ou la disponibilité des ressources est interrompue. Par exemple une attaque par inondation (Flooding attack) limitant le nombre de connexions réussies au service de l'Internet.
- *Complète (C = 0.66) :* Il y a un arrêt total de la ressource affectée. L'attaquant peut rendre la ressource complètement indisponible.

Métrique ou critère	**Notation**		
Impact de C-I-A	Aucun (N)	Partiel (P)	Complète (C)
Valeur	0.0	0.275	C = 0.66

TABLEAU 3.4 – Métrique : Impact sur la confidentialité (C), disponibilité (A), intégrité (I).

3.2.3 Métriques temporelles

Ce groupe de métrique représente les caractéristiques d'une vulnérabilité qui évoluent avec le temps, mais qui ne dépendent pas de l'environnement des utilisateurs. Le risque posé par la vulnérabilité peut être modifié au fil du temps. Il existe trois métriques pour mesurer ces changements à savoir : la confirmation des détails techniques d'une vulnérabilité, l'état de la correction ou la solution de la vulnérabilité proposée par la communauté et la disponibilité du code ou la technique à l'exploitation par le public. Comme les métriques temporelles sont facultatives, elles comprennent chacune une valeur métrique par défaut qui n'a pas d'effet sur le score. Cette valeur est utilisée lorsque l'utilisateur estime que la métrique particulière ne s'applique pas et souhaite l'ignorer. La description des métriques est présentée ci-dessous :

Facilité d'Exploitation ou Exploitabilité (E)

L'exploitabilité est un indicateur de l'état actuel de la disponibilité des codes ou des techniques pour le public. Cette disponibilité augmente la probabilité d'exploitation de la vulnérabilité. Au départ, l'exploitation dans le monde réel peut être essentiellement théorique. Cela pourrait être suivi par la publication d'une preuve de concept (de l'anglais : proof of concept, POC), une démonstration de faisabilité, un exploit fonctionnel, ou des détails techniques suffisants et nécessaires pour exploiter la vulnérabilité. En outre, le

code disponible peut passer d'une démonstration de preuve de concept (POC) à un code d'exploitation qui sert à exploiter la vulnérabilité d'une manière systématique. Plus une vulnérabilité peut être facilement exploitée, plus le score de vulnérabilité est élevé. Les valeurs possibles de cette métrique sont :

- *Non prouvé (Unproven U = 0.85) :* lorsqu' aucun code d'exploitation n'est pas disponible, ou un exploit est entièrement théorique.
- *Preuve de concept (Proof-of Concept / POC = 0.9) :* lorsqu' il existe une démonstration d'attaque qui n'est pas pratique pour la plupart des systèmes. Le code ou la technique n'est pas fonctionnel dans toutes les situations et peut nécessiter une modification par un attaquant compétent.
- *Fonctionnel (F=0.95) :* le code ou la technique fonctionne dans la plupart des situations où la vulnérabilité existe.
- *Élevé (High H = 1.0) :* le code ou la technique fonctionne dans toutes les situations, l'activation fournie par un agent mobile autonome (tel qu'un ver ou un virus) ;
- *Non défini (ND = 1.0) :* L'attribution de cette valeur à la métrique n'influencera pas le score final.

Métrique ou critère	**Notation**				
Exploitabilité(E)	Non prouvé (U)	Preuve de concept (POC)	Fonctionnel (F)	Élevé (H)	Non défini (ND)
Valeur	0.85	0.9	0.95	1.0	1.0

TABLEAU 3.5 – Métrique : Facilité d'Exploitation ou Exploitabilité (E).

Niveau de remédiation ou correction (RL)

Lorsque la vulnérabilité est publiée pour la première fois, la vulnérabilité n'est pas encore résolue jusqu'à la publication d'une correction par des solutions temporelles, d'un patch ou d'une mise à jour officielle. La vulnérabilité typique n'est pas corrigée lors de sa publication initiale. Des solutions de contournement ou des correctifs peuvent offrir une remédiation provisoire jusqu'à ce qu'un correctif ou une mise à niveau officiels soient publiés. Chacune de ces étapes respectives ajuste le score temporel à la baisse, reflétant la gravité décroissante avec les solutions proposées au fil du temps. Toutes ces étapes qui modélisent le résultat d'une remédiation ajustent le score final. Plus le correctif ou la solution proposée est officiel et permanent, plus le score de vulnérabilité est à la baisse.

Les valeurs possibles pour cette métrique sont :

- *Correction officielle (Official Fix /OF =0.87) :* Une solution complète du fournisseur est disponible. Soit le vendeur a publié un patch officiel, soit une mise à jour est disponible.
- *Correction temporelle (Temporary Fix /TF = 0.9) :* Il existe une correction officielle, mais temporaire. Cela inclut les cas où le fournisseur publie un correctif, un outil ou une solution de contournement temporaire.

- *Solution de contournement (Workaround /W = 0.95) :* Il existe une solution non officielle, non liée à un fournisseur. Dans certains cas, les utilisateurs de la technologie concernée créeront leur propre patch ou fourniront des mesures pour contourner ou atténuer la vulnérabilité.
- *Indisponible (Unavailable / U = 1.0) :* Soit il n'y a pas de solution disponible, soit il est impossible de l'appliquer.
- *Non défini (ND = 1.0) :* L'attribution de cette valeur n'influencera pas le score. C'est une valeur qui permet à l'utilisateur d'ignorer cette métrique.

Métrique ou critère	**Notation**				
Niveau de remédiation	OF	TF	W	U	ND
Valeur	0.87	0.9	0.95	1.0	1.0

TABLEAU 3.6 – Métrique : Niveau de remédiation ou correction.

Rapport de confiance (RC)

Cette métrique décrit la confiance de la vulnérabilité existante ou la crédibilité de celle qui est connue. Parfois, les chercheurs ou les utilisateurs publient avec certitude une vulnérabilité. Enfin, le vendeur confirme l'existence de la vulnérabilité, donc le degré de confiance change dans ce cas. La gravité d'une vulnérabilité est plus grande lorsque l'on sait avec certitude qu'elle existe. Plus une vulnérabilité est validée par le vendeur ou par d'autres sources réputées, plus le score est élevé. Quatre valeurs sont possibles :

- *Non Confirmée (Unconfirmed /UC = 0.9) :* Il y a une seule source non confirmée ou plusieurs rapports contradictoires. La confiance dans la validité des rapports est faible.
- *Présumée (Uncorroborated /UR =0.95/) :* Il existe de nombreuses sources non officielles, dont peut-être des sociétés de sécurité indépendantes ou des organismes de recherche. À ce stade, il peut y avoir des détails techniques contradictoires ou une autre ambiguïté persistante.
- *Confirmée (C = 1.0) :* Dans ce cas, la vulnérabilité a été reconnue par le vendeur ou l'auteur de la technologie concernée. La vulnérabilité peut également être "confirmée" lorsque son existence est avérée par un événement externe tel que la publication d'une exploitation fonctionnelle du code ou de preuve de concept.
- *Non définie (ND = 1.0)* L'attribution de cette valeur n'influencera pas le score. C'est une valeur qui permet à l'utilisateur d'ignorer cette métrique.

Métrique ou critère	**Notation**			
Niveau de remédiation	Unconfirmed (UC)	Uncorroborated (UR)	Confirmée (C)	Non définie (ND)
Valeur	0.9	0.95	1.0	1.0

TABLEAU 3.7 – Métrique : Rapport de confiance et l'existence de la vulnérabilité (RC)

3.2.4 Métriques environnementales

Ce groupe de métriques représente les caractéristiques d'une vulnérabilité qui sont pertinentes et spécifiques à l'environnement d'un utilisateur particulier. L'environnement joue un rôle clé dans la gravité des risques. Le CVSS dispose des métriques qui mesurent les facteurs environnementaux. Ce groupe de métriques est également facultatif pour le calcul du score final. Cela donne l'impression que les concepteurs de la CVSS considèrent que l'environnement n'est pas important. Ceci est parfaitement applicable lorsqu'il s'agit d'un système informatique où l'environnement n'est pas hostile. Cependant, l'impact environnemental dans les ICSs est plus important et entraîne souvent des conséquences catastrophiques. Ce groupe comporte deux métriques :

Dommages collatéraux potentiels (CDP)

Cette métrique est la seule qui puisse mesurer le degré de la sécurité, que ce soit pour les pertes en vies humaines ou les dommages physiques. La métrique peut inclure aussi les dommages économiques. Les valeurs possibles pour cette métrique sont les suivantes :

- *Aucune (None /N = 0) :* Il n'y a pas de pertes potentielles de vies, de biens physiques, de production ou de revenus économiques.
- *Faible (Low /L = 0.1) :* Une exploitation réussie de cette vulnérabilité peut entraîner de légers dommages physiques ou matériels. Ou bien, il peut y avoir une légère perte de revenus ou de production pour l'organisation.
- *Faible-Moyenne (Low-Medium /LM = 0.3) :* Une exploitation réussie de cette vulnérabilité peut entraîner des dommages physiques ou matériels modérés. Ou bien, il peut y avoir une perte modérée de revenus ou de production pour l'organisation.
- *Moyenne-Élevé (Medium-High /MH = 0.4) :* Une exploitation réussie de cette vulnérabilité peut entraîner dommages ou pertes physiques ou matérielles importantes. Il peut aussi y avoir une perte importante de revenus ou de production.
- *Élevée (High /H = 0.5) :* Une exploitation réussie de cette vulnérabilité peut entraîner des pertes et des dommages physiques ou matériels catastrophiques. Ou bien, il peut y avoir une perte catastrophique de revenus ou de production.
- *Non Défini (ND = 0) :* L'attribution de cette valeur n'influencera pas le score. C'est une valeur qui permet à l'utilisateur d'ignorer cette métrique.

Chaque organisation doit déterminer elle-même la signification précise de "léger, modéré, significatif et catastrophique".

Métrique ou critère	**Notation**					
Dommages collatéraux potentiels (CDP)	Aucune (N)	Faible (L)	Faible -Moyenne (LM)	Moyenne -Élevée (MH)	Élevée (H)	Non Défini (ND)
Valeur	0.0	0.1	0.3	0.4	0.5	0

TABLEAU 3.8 – Métrique : dommages collatéraux potentiels (CDP).

Nombre de cibles impactées (Target Distribution- TD)

Cette métrique mesure la proportion de systèmes vulnérables. Il s'agit d'un indicateur spécifique à l'environnement qui permet d'évaluer approximativement le pourcentage de systèmes qui pourraient être affectés par la vulnérabilité. Plus la proportion de systèmes vulnérables est importante, plus le score est élevé. Les valeurs possibles pour cette métrique sont :

- *Aucune (N = 0) :* le système cible n'existe pas, ou bien les cibles sont si spécialisées qu'elles n'existent que dans un cadre de laboratoire. En fait, 0% de l'environnement est menacé.
- *Faible (Low/L = 0.25) :* Les cibles existent dans l'environnement, mais à petite échelle. Entre 1 % et 25 % de l'environnement total est menacé.
- *Moyenne (Medium /M = 0.75) :* Les cibles existent dans l'environnement, mais à une échelle moyenne. Entre 26% et 75 % de l'environnement total est menacé.
- *Élevé (High /H = 1.00) :* Les cibles existent dans l'environnement à une échelle considérable. Entre 76 % et 100 % de l'environnement total est considéré comme menacé.
- *(Non défini / ND= 1.00) :* L'attribution de cette valeur n'influence pas le score final.

Métrique ou critère	**Notation**				
Nombre de cibles impactées (TD)	Aucune (N)	Faible (L)	Moyenne (M)	Élevée (H)	Non Défini (ND)
Valeur	0.0	0.25	0.75	1.0	1.0

TABLEAU 3.9 – Métrique : nombre de cibles impactées (TD).

Exigences de sécurité (Security Requirement CR, IR, AR)

Ces métriques permettent aux utilisateurs d'ajuster le score en fonction de l'importance des paramètres de la sécurité C-I-A sur l'infrastructure ciblée. Elles permettent à l'analyste de personnaliser le score CVSS en fonction de l'importance du C-I-A pour le bien. En d'autres termes, si un bien soutient une fonction pour laquelle la disponibilité est la plus importante, l'analyste peut attribuer une plus grande valeur à la disponibilité (A), par rapport à la confidentialité (C) et à l'intégrité (I). Chaque exigence de sécurité a trois valeurs possibles : "faible L= 0.5", "moyen M=1.0", "élevé H = 1.5", "Non Défini=1.0".

Métrique ou critère	**Notation**			
Exigences de sécurité (CR, IR, AR)	Faible (L)	Moyenne (M)	Élevée (H)	Non Défini (ND)
Valeur	0.5	1.0	1.5	1.0

TABLEAU 3.10 – Métrique : Exigences de sécurité CR, IR, AR.

3.2.5 Vecteurs de base, temporels et environnementaux

Le vecteur des métriques se compose d'un nom abrégé d'une métrique, suivi d'un " :" (deux-points), puis de la valeur abrégée de la métrique. Le vecteur dénombre ces métriques dans un ordre prédéterminé, en utilisant le caractère "/" (barre oblique) pour séparer les métriques. Si une métrique temporelle ou environnementale ne doit pas être utilisée, elle reçoit la valeur "ND" (Non Définie). Les vecteurs de base, temporels et environnementaux sont présentés dans le tableau 3.11 :

Groupe des metriques	Vecteur
Base	AV :[L,A,N]/AC :[H,M,L]/Au :[M,S,N]/C :[N,P,C]/I :[N,P,C]/A :[N,P,C]
Temporelles	E :[U,POC,F,H,ND]/RL :[OF,TF,W,U,ND]/RC :[UC,UR,C,ND]
Environmentales	CDP :[N,L,LM,MH,H,ND]/TD :[N,L,M,H,ND]/CR :[L,M,H,ND]/ IR :[L,M,H,ND]/AR :[L,M,H,ND]

TABLEAU 3.11 – Vecteurs de base, temporels et environnementaux

Par exemple, une vulnérabilité avec des valeurs métriques de base de "Access Vector : Faible, Complexité d'accès : Medium, Authentification : Aucune, Impact sur la confidentialité : Aucune, Impact sur l'intégrité : Partiel, Impact sur la disponibilité : Complet" aurait le vecteur de base suivant : "AV :L/AC :M/Au :N/C :N/I :P/A :C."

Directives d'évaluations

Vous trouverez ci-dessous des directives (guidelines) pour aider les analystes à évaluer les vulnérabilités

1. La notation de la vulnérabilité ne doit pas tenir compte de l'interaction avec d'autres vulnérabilités. C'est-à-dire que chaque vulnérabilité doit être notée **indépendamment**.

2. Lors de l'évaluation de l'impact d'une vulnérabilité qui possède plusieurs méthodes d'exploitation, l'analyste doit choisir la méthode d'exploitation qui a le plus grand impact, plutôt que la méthode la plus courante ou la plus facile à mettre en œuvre. Lorsqu'une vulnérabilité peut être exploitée à la fois localement et à partir du réseau, la valeur "Réseau" doit être choisie. Lorsqu'une vulnérabilité peut être exploitée à la fois localement et à partir de réseaux adjacents, mais pas à partir de réseaux distants, la valeur "Réseau adjacent" doit être choisie. Lorsqu'une vulnérabilité peut être exploitée à partir du réseau adjacent et des réseaux distants, la valeur "Réseau" doit être choisie.

3. Les vulnérabilités avec une perte partielle ou complète d'intégrité peuvent également avoir un impact sur la disponibilité. Par exemple, un attaquant qui est capable de modifier des informations peut probablement aussi les supprimer.

Équations de calcul du score

Au cours du développement de CVSS v2, plusieurs versions des équations et des valeurs métriques ont été développées, examinées et analysées par le CVSS-SIG (CVSS-Special Interest Group). Une discussion plus approfondie sur l'origine des valeurs des métriques

Evaluation	CVSS Score
Low	0.0 - 3.9
Medium	4.0 - 6.9
High or critical	7.0 - 8.9

TABLEAU 3.12 – Échelle qualitative d'évaluation de la gravité

et la vérification de ces équations est disponible sur (FIR, a). Les équations et les algorithmes de notation pour les groupes métriques de base, temporels et environnementaux sont décrits ci-dessous :

- le score de base (BS) et leurs sous-scores, l'Exploitabilité (ES) et le score d'impact (IS), peuvent être calculés par la formule suivante :

$$\mathrm{ES} = 20 \times \mathrm{AV} \times \mathrm{AC} \times \mathrm{A}u \tag{3.1}$$

$$\mathrm{IS} = 10.41(1-(1-\mathrm{C})(1-\mathrm{I})(1-\mathrm{A})) \tag{3.2}$$

$$f(\mathrm{IS}) = \begin{cases} 0 & if \quad \mathrm{IS} = 0 \\ 1.176 & if \quad \mathrm{IS} \neq 0 \end{cases} \tag{3.3}$$

$$\mathrm{BS} = \mathrm{R}ound\mathrm{To}\mathrm{D}ec((0.6 \times \mathrm{IS} + 0.4 \times \mathrm{ES} - 1.5) \times f(\mathrm{IS})) \tag{3.4}$$

- L'équation temporelle combinera les mesures temporelles avec le score de base pour produire un score temporel allant de 0 à 10. En outre, le score temporel ne sera pas supérieur au score de base et ne sera pas inférieur de moins de 33 % à celui-ci. L'équation temporelle est définie comme suit :

$$\mathrm{T}emporal\mathrm{S}core = \mathrm{R}ound\mathrm{To}\mathrm{D}ecimal(\mathrm{BS} \times \mathrm{E} \times \mathrm{RL} \times \mathrm{RC}) \tag{3.5}$$

ou *RoundToDecimal* est fonction qui permet d'arrondir le score par un chiffre après la virgule.

- L'équation environnementale combinera les mesures environnementales avec le score temporel pour produire un score final allant de 0 à 10. En outre, cette équation produira une note qui ne sera pas supérieure à la note temporelle.

  La formule environnementale (En) est donnée par :

$$\mathrm{E}n = \mathrm{R}ound\mathrm{To}\mathrm{D}ecimal((\mathrm{T}emporal\mathrm{S}core + (10 - \mathrm{T}emporal\mathrm{S}core) \times \mathrm{CDP}) \times \mathrm{TD}) \tag{3.6}$$

La sous-équation d'impact (IS) de la formule BaseScore 3.10 est remplacée par l'équation d'impact Ajusté AdjustedImpac comme suit :

$$\mathrm{A}djusted\mathrm{I}mpac = min(10, 10.41 \times (1-(1-\mathrm{C} * \mathrm{CR})$$

$$\times (1-\mathrm{I} * \mathrm{IR}) \times (1-\mathrm{A} * \mathrm{AR})))$$

Le score final, défini entre 0.0 et 10 (voir la tableau 3.12), exprime la criticité globale de la vulnérabilité sur système.

Exemples

ces exemples sont extraits du site du FIRST.ORG (FIR, c) :

- **CVE-2002-0392 :** en juin 2002 la vulnérabilité CVE-2002-0392 (Apache Chunked-Encoding Memory Corruption) a été découvert dans les outils dans lequel le serveur traite les requêtes. Entreprise Apache a signalé que l'exploitation de cette vulnérabilité peut causer un DoS dans des situations particulières, et dans d'autres, à l'exécution de code malveillant lorsque l'attaquant utilise les privilèges du serveur Web.

  Dans ce cas, le vecteur d'accès (AV) est la valeur " Réseau ", car la vulnérabilité peut être exploitée à distance. Comme aucune circonstance n'est nécessaire pour que l'attaquant réussisse cet exploit et l'attaquant n'a qu'à envoyer un message approprié à l'auditeur web Apache, la valeur de la métrique complexité d'accès est "Faible". La métrique d'authentification (Au) est "Aucune", car aucune authentification n'est exigée pour l'exploit. Vu que cette vulnérabilité peut être exploitée par plusieurs méthodes. Nous devons calculer le score pour chaque méthode et ensuite nous prenons le score le plus élevé.

  Dans le cas où la vulnérabilité pourrait exécuter un code malveillant, modifiant ainsi le contenu web et permettant de divulguer les informations locales sur l'utilisateur ou la configuration (par exemple, les paramètres de connexion et les mots de passe de la base de données back-end), les métriques de l'impact de la confidentialité (C) et l'intégrité (I) sont affectées à la valeur "Partielles". Cela donne un score de base est 6.4.

  Si la vulnérabilité peut causer un DoS, la valeur de l'impact de la disponibilité (A) est "complet". Ce qui donne un score de base égale à 7.8.

  Enfin, nous devons choisir le score 7.8 au lieu de 6.4, car il s'agit du score de base le plus élevé parmi les scores de base possibles.

  La valeur de l'exploitabilité est "fonctionnelle", puisque le code d'exploitation est connu. L'entreprise Apache a proposé des correctifs, par conséquent le niveau de remédiation est donc "Official-Fix" et la confiance du rapport est "confirmée". Par la suite, ces métriques corrigent le score de base pour avoir un score temporel égal à 6.4.

  Si on suppose que la disponibilité est plus importante que d'habitude (c.-à-d. la valeur de (AR) égale à 1.5), et en fonction des valeurs des métriques du potentiel de dommages collatéraux (CDP) et de la distribution cible (TD), le score environnemental peut varier entre 0,0 (avec "Aucun", "Aucune" pour chacun) et 9,2 (pour "Élevé", "Élevé"). Les résultats sont résumés ci-dessous (FIR, c) :

Explication de la formule CVSS v2 et du développement de la valeur métrique

L'objectif de cette section est d'expliquer comment les formules et les valeurs métriques du CVSS v2 ont été établies. Une grande partie de ce processus est documentée via le site internet de FIRST (FIR, d). Toutefois, cette section énumère principalement les versions intermédiaires des formules et des métriques, et n'explique pas toujours le travail ou les modifications qui ont été effectués pour chaque version.
CVSS-SIG (CVSS Special Interest Group) est un groupe spécial d'experts qui propose des améliorations régulièrement sur les métriques, les valeurs et les formules de calcul.

```
-----------------------------------------------------
BASE METRIC                  EVALUATION         SCORE
-----------------------------------------------------
Access Vector                [Network]         (1.00)
Access Complexity            [Low]             (0.71)
Authentication               [None]            (0.704)
Confidentiality Impact       [None]            (0.00)
Integrity Impact             [None]            (0.00)
Availability Impact          [Complete]        (0.66)
-----------------------------------------------------
BASE FORMULA                                BASE SCORE
-----------------------------------------------------
Impact = 10.41*(1-(1)*(1)*(0.34)) == 6.9
Exploitability = 20*0.71*0.704*1 == 10.0
f(Impact) = 1.176
BaseScore = (0.6*6.9 + 0.4*10.0 - 1.5)*1.176

                                             == (7.8)
-----------------------------------------------------

-----------------------------------------------------
TEMPORAL METRIC              EVALUATION         SCORE
-----------------------------------------------------
Exploitability               [Functional]      (0.95)
Remediation Level            [Official-Fix]    (0.87)
Report Confidence            [Confirmed]       (1.00)
-----------------------------------------------------
TEMPORAL FORMULA                         TEMPORAL SCORE
-----------------------------------------------------
round(7.8 * 0.95 * 0.87 * 1.00)               == (6.4)
-----------------------------------------------------

-----------------------------------------------------
ENVIRONMENTAL METRIC         EVALUATION         SCORE
-----------------------------------------------------
Collateral Damage Potential  [None - High]  {0 - 0.5}
Target Distribution          [None - High]  {0 - 1.0}
Confidentiality Req.         [Medium]           (1.0)
Integrity Req.               [Medium]           (1.0)
Availability Req.            [High]             (1.51)
-----------------------------------------------------
ENVIRONMENTAL FORMULA              ENVIRONMENTAL SCORE
-----------------------------------------------------
AdjustedImpact = min(10,10.41*(1-(1-0*1)*(1-0*1)
         *(1-0.66*1.51))                      == (10.0)
AdjustedBase =((0.6*10)+(0.4*10.0)-1.5)*1.176
                                              == (10.0)
AdjustedTemporal == (10*0.95*0.87*1.0)         == (8.3)
EnvScore = round((8.3+(10-8.3)*{0-0.5})*{0-1})
                                        == (0.00 - 9.2)
-----------------------------------------------------
```

FIGURE 3.3 – Evaluation de vulnérabilité CVE-2002-0392 (FIR, c)

Le CVSS-SIG avait identifié plusieurs lacunes dans la version 1 du CVSS. Il y avait un manque de diversité dans les scores - trop de vulnérabilités avec des caractéristiques différentes recevant chacune le même score, alors que, dans de nombreux cas, il y avait un consensus sur le fait qu'une vulnérabilité était significativement plus grave qu'une autre (et aurait dû avoir un score plus élevé). Dans l'ensemble, de nombreuses vulnérabilités ont eu des scores plus bas à ce que les membres du SIG auraient pu s'attendre, et pour certains types de vulnérabilités, ils ont eu des scores significativement plus bas que d'autres vulnérabilités considérées comme moins graves. Des problèmes supplémentaires avec la spécification v1 ont été identifiés en comparant les scores calculés par les analystes de plusieurs organisations; les discussions concernant les différences de score ont permis de mettre en évidence un langage peu clair dans la spécification.
Après avoir été énumérés, les problèmes ont été résolus en utilisant une combinaison de deux méthodes. La première consistait à réviser les métriques, par exemple en ajoutant des valeurs possibles pour les métriques AC (Access Complexity)), AV (AccessVector) et Au (Authentication) (chacun passant de 2 à 3 valeurs possibles). Les mesures du biais d'impact ont été déplacées de la note de base à la note environnementale. Des modifications de formulation ont été apportées à toutes les descriptions des mesures. Ces changements visaient à améliorer la diversité des scores et à rendre la notation plus cohérente entre les organisations effectuant la notation. Les changements apportés aux mesures et à leur description sont énumérés dans les propositions 1 à 11 de l'annexe A de rubrique historique sur le site web de FIRST (FIR, d).
La deuxième méthode utilisée pour résoudre les problèmes était une révision des formules et des valeurs métriques. Cela a été nécessaire en partie à cause des changements apportés aux mesures de base. Mais elle était également essentielle parce que les formules et valeurs existantes généraient des scores qui ne tenaient pas compte des différences relatives de gravité entre les vulnérabilités. Les premiers efforts ont consisté à déterminer si les formules et valeurs existantes pouvaient simplement être un peu modifiées pour résoudre les problèmes de notation identifiés, mais aucune solution raisonnable n'a pu être trouvée.
Les statisticiens ont examiné la formule originale (version 1) et ont déterminé que les scores trop faibles de CVSS v1 sont dus en grande partie à la nature hautement multiplicative de la formule originale. Une seule mesure avec une valeur faible peut entraîner une baisse de 3 ou 4 points, et quelques mesures avec des valeurs non élevées peuvent entraîner des scores assez faibles. En conséquence, une décision a été prise pour élaborer une nouvelle formule. Une analyse du CVSS v1 a montré qu'il donnait en fait des pondérations de 0,572 et 0,428 aux sous vecteurs d'impact (IS) et d'exploitabilité (ES), respectivement. L'application de ces pondérations aux sous-vecteurs a produit des scores de base raisonnables. Enfin, la pondération simplifiée de 0,6 et 0,4 a été adoptée.

3.3 CVSS version 2 vs CVSS version 3

En juin 2015, CVSS v 3.0 a été publiée. La nouvelle version a conservé l'ossature de la v 2.0, mais avec quelques changements proposés qui comprenaient de nouvelles mesures telles que le champ d'application (S) et l'interaction avec l'utilisateur (UI), d'autres anciennes mesures telles que l'authentification ont été modifiées ou transformées en une notation plus récente telle que les privilèges requis (PR). Mais nous avons remarqué que ces modifications ont été faites pour accentuer en plus la tendance de système vers l'évaluation des systèmes informatiques (IT). En effet, les paramètres environnementaux cibles impactés (TD) et potentiels de dommages collatéraux (CDP) ont été remplacés par

des facteurs qui sont plus adaptés aux systèmes informatiques comme : Vecteur d'attaque modifié (MAV), Complexité d'attaque modifiée (MAC), Privilèges modifiés requis (MPR)... . Pour cette raison, nous avons choisi de travailler sur CVSS version 2 plutôt que la version 3, car la version 2 contient des métriques environnementaux (CDP et TD) qui sont plus adaptées à notre besoin de quantifier la SAF.

3.4 Système de score des vulnérabilités pour les systèmes de contrôles industriels

Malgré l'amélioration qui a été apportée par rapport à la version 1, la version 2 du CVSS classique n'est pas adaptée à l'évaluation des vulnérabilités pour le domaine des ICSs. En effet, les métriques environnementales considérées comme des métriques optionnelles dans le cas de IT. Par contre, elles sont essentielles à l'évaluation dans le cas des ICSs. La version actuelle du CVSS ne permet pas d'intégrer l'impact d'une attaque sur la boucle de contrôle en termes de perte de commande, ou de perte de supervision, ou de déni de service (DoS) qui peuvent avoir un impact sur la SAF et la SEC. De plus, le manque d'une métrique qui représente la SAF d'une façon efficace rende le système de score très loin de la réalité dans cas des ICSs.
Dans la section suivante, nous présentons des adaptations du CVSS pour les systèmes de contrôle industriel appelée ICVSS (Industrial Control Vulnerability Scoring System) basée sur la version 2 du CVSS. Nous allons améliorer et affiner chaque métrique, en conservant la même méthodologie CVSS.

L'ICVSS est une méthodologie proposée pour mesurer et quantifier les vulnérabilités des ICSs. Nous allons proposer d'autres métriques qui permettent de mieux représenter le risque avec des adaptations des formules si nécessaire. L'approche proposée repose sur le calcul de 14 métriques réparties en trois groupes. Ces métriques sont héritées du CVSS classique qui permettent d'affiner et d'adapter les résultats des scores pour les systèmes industriels. Ces groupes de métriques sont présentés en dessous :

3.4.1 Métriques de bases

Vecteur d'accès

La SEC vise à éviter les écoutes et les vols inattendus. Elle est essentielle pour protéger les communications et données. Les réseaux sans fil sont plus susceptibles d'être attaqués que les réseaux câblés, ce qui accroît les menaces pesant sur le réseau sans fil (A Ochang et al., 2016). Pour cette raison, cette métrique est divisée en deux sous-métriques qui reflètent l'architecture du réseau et type du réseau pour représenter le vecteur d'accès :

- **Moyens Physiques (Physical Media PM) :** Cette sous-métrique mesure le moyen qui pourrait être utilisé pour exploiter la vulnérabilité. Les valeurs possibles sont les suivantes :
  - *Dispositif physique (Phy=0.2) :* Lorsque l'intrusion besoin de dispositif physique pour réussir l'action de l'attaque par exemple une clé USB ;
  - *Filaire (Wired /W =0.395) :* Cette valeur est attribuée, quand l'attaquant pourrait exploiter la vulnérabilité par un moyen filaire ;
  - *Sans fils (Wireless / WL = 1.0) :* Cette valeur est attribuée, quand la vulnérabilité peut passer par un moyen sans fil.

Sous-métrique	Notation		
Moyens Physiques (PM)	Dispositif physique (Phy)	Filaire (W)	Sans fils (WL)
Valeur	0.2	0.395	1.0

TABLEAU 3.13 – Sous-métrique : Moyens Physiques (PM).

- **Couche d'accès (Access Layer AL) :** Cette sous-métrique mesure la couche où la vulnérabilité pourrait être exploitée. Les valeurs possibles sont les suivantes :
  - *Réseau (Network) (1.0) :* Cette valeur est attribuée quand l'attaquant exploite une vulnérabilité qui provient de l'Internet ;
  - *Réseau adjacent (0.646) :* Lorsque la menace provient d'un réseau privé virtuel (Virtual private network VPN) ;
  - *Réseau local (0.395) :* Lorsque la menace provient d'un réseau local (LAN Local Architecture Network) ;
  - *Physique (0.2) :* Cette dernière possibilité, lorsque l'attaquant a besoin d'un contact physique avec la cible du système ICS.

Métrique ou critère	Notation			
Vecteur d'accès (AL)	Physique (Phy)	Réseau Local (LN)	Réseau adjacent (A)	Réseau (N)
Valeur	0,2	0.395	0.646	1.0

TABLEAU 3.14 – Sous-métrique : Couche d'accès (AL)

Complexité d'accès (Access complexity AC)

Cette métrique mesure la complexité de l'attaque qui exploite la vulnérabilité. La métrique est divisée en deux sous-mesures :

- **Complexité du système (System Complexity - SC) :** Les systèmes distribués (par exemple, les systèmes SCADA de distribution d'électricité) sont plus vulnérables aux attaques, car ils sont physiquement répartis sur plusieurs sites éloignés géographiquement. La coordination entre les différents sites est assurée par les réseaux de communication (par exemple, WAN (réseaux étendus) ; et NAN (réseaux de voisinage) (Zhang, 2015). Par conséquent, l'attaquant peut utiliser des techniques moins sophistiquées pour compromettre le système si on le compare à un système qui est physiquement situé sur un seul site isolé. Les valeurs possibles sont les suivantes :
  - *Simple (S) (0.35) :* Quand l'installation est située sur un seul site isolé ;
  - *Distribué (D) (0.71) :* Quand l'installation est répartie sur plusieurs sites.

Sous-métrique	Notation	
Complexité du système (SC)	Simple (S)	Distribué (D)
Valeur	0.35	0.71

TABLEAU 3.15 – Sous-métrique : Complexité du système (SC).

- **Complexité de l'attaque (ATC) :** Dans cette métrique, nous conservons la même définition du CVSS qui mesure la complexité de l'attaque ou les techniques nécessaires pour exploiter la vulnérabilité (Access Complexity (AC)). Il y a trois valeurs possibles :
  -*Élevé (H) (0.35) :* Cette valeur est attribuée lorsque l'attaque nécessite beaucoup de temps, plusieurs étapes, des connaissances et des compétences pour exploiter la vulnérabilité. En général, ces attaques sont lancées par des menaces terroristes et des nations (groupe 1) (par exemple, l'attaque Stuxnet)(ics,).
  -*Moyen (M) (0.61) :* Cette valeur est attribuée lorsque l'attaquant a besoin de moins de connaissances et de compétences techniques que le groupe 1 pour exploiter la vulnérabilité. Habituellement, ces attaques sont lancées par des menaces organisées (groupe 2) dont la motivation peut être financière, ou de vengeance, ou de vol de secrets commerciaux, ou pour attirer l'attention sur une cause (hacktivistes) (ics,).
  -*Faible (0.71) :* Cette valeur est attribuée lorsque l'attaque a besoin des connaissances et des compétences techniques moins structurées et moins sophistiquées que le groupe (2). Ces attaques sont lancées par des menaces classiques (groupe 3) dont les motivations sont liées à la notoriété, à la célébrité ou à l'attaque d'un système pour attirer l'attention sur soi (ics,).

Sous-métrique	**Notation**		
Complexité de l'attaque (ATC)	Élevé (H)	Moyen (M)	Faible (L)
Valeur	0.35	0.61	0.71

TABLEAU 3.16 – Sous-métrique : Complexité d'attaque (ATC).

- **Cryptographie (C) :** La cryptographie (le chiffrement) des informations est un élément clé dans la sécurité des réseaux de communication. La définition la plus simple de la cryptographie est la transformation de l'information pour empêcher les intrus d'en observer le sens. cela empêche l'information d'atteindre un attaquant sous une forme utilisable. Les réseaux sans fil sont un bon exemple qui montre l'importance de cryptage. En effet, comme les réseaux sans fil diffusent les trames via l'air, quiconque possède un émetteur-récepteur sans fil peut intercepter les transmissions. Nous pouvons sécuriser les réseaux sans fil en plusieurs étapes, mais la mise en oeuvre œuvre un protocole de cryptage solide, tel que le Wi-Fi Protected Access II (WPA2) (Gibson, 2017). Une telle solution ajoute encore une couche de sécurité au système. Dans le chapitre cinq nous allons décrire en détail les principaux protocoles de sécurité disponibles pour les réseaux sans fil. Cette métrique présente le niveau de cryptage et chiffrement des données échangées (par exemple, le protocole de communication dispose d'un système de cryptage). Pour simplifier le problème, deux valeurs sont possibles : Aucun (0.71), Cryptée (0.35).

Sous-métrique	**Notation**	
Cryptographie (C)	Aucun (N)	Cryptée (C)
Valeur	0.71	0.35

TABLEAU 3.17 – Sous-métrique : Cryptographie (C).

Impact sur la sécurité (C, I, A)

Les mêmes définitions sont utilisées dans la version 2 du CVSS classique pour mesurer les impacts sur la confidentialité (C), l'intégrité (I) et la disponibilité (A). Voir la section 3.2.2 pour plus de détails.

Système de SAF (SS)

Cette métrique mesure la présence de systèmes de SAF dans l'installation qui devraient protéger les équipements et les personnes dans le cas des situations dangereuses qui se produisent durant l'exploitation. Les valeurs possibles sont : Aucun (0.9), couvert par le système de SAF (0.01).

Sous-métrique	**Notation**	
Système de SAF (SS)	Aucun (N)	Couvert par le Système de SAF (SS)
Valeur	0.9	0.01

TABLEAU 3.18 – Sous-métrique : couverture par le Système de SAF (SS).

3.4.2 Métriques temporelles

Exploitabilité (E)

Cette métrique contient trois sous-mesures :

- **Accès au système (System Access (SA)) :** Cette métrique présente le degré d'accessibilité à des informations utiles sur le matériel ou sur le logiciel. Les valeurs possibles sont les suivantes :

  - *Non Défini (ND = 1.0) :* Cette valeur est attribuée quand la métrique est ignorée.

  - *Open Source (OS = 1.0) :* Cette valeur est attribuée lorsque la technologie est disponible pour le public.
  - *Propriétaire (P = 0.85) :* Cette valeur est attribuée lorsque la technologie est propriétaire à un seul fournisseur.

Sous-métrique	**Notation**		
Accès au système (SA)	Non Défini (ND)	Open Source (OS)	Propriétaire (P)
Valeur	1.0	1.0	0.85

TABLEAU 3.19 – Sous-métrique : Accès au système (SA).

- **Maturité (M) :** Nous adoptons la même définition de l'exploitabilité (E) dans la version 2 du CVSS. Les valeurs possibles sont les suivantes : Élevées (1,0), Fonctionnelle (0.95), Preuve du concept (0.90), Non prouvée (0.85), Non définie (1.0).

Métrique ou critère	**Notation**				
Maturité	Non prouvé (U)	Preuve de concept (POC)	Fonctionnel (F)	Élevé (H)	Non défini (ND)
Valeur	0.85	0.9	0.95	1.0	1.00

TABLEAU 3.20 – Métrique : Maturité (M).

Niveau de correction ou "Remediation Level" (RL) :

Spécifie l'existence de contournement ou de solution pour cette vulnérabilité. Il peut exister un correctif officiel (OF – "Official Fix" (0.87)), exister un correctif temporaire (TF – "Temporary Fix" (0.9)), exister un contournement (W – "Workaround" (0.95)), n'exister aucune solution (U – "Unavailable"(1.0)), ou bien être indéfini (ND – "Not Defined" (1.0)).

Métrique ou critère	**Notation**				
Niveau de remédiation	OF	TF	W	U	ND
Valeur	0.87	0.9	0.95	1.0	1.0

TABLEAU 3.21 – Métrique : Niveau de remédiation ou correction.

Niveau de confiance ou "Report Confidence" (RC) :

Spécifie si cette vulnérabilité est confirmée ou supposée. Elle peut être non confirmée (UC – "Unconfirmed" (0.9)), présumée (UR – "Uncorroborated" (0.95)), confirmée (C – "Confirmed" (1.0)), ou bien être Non définie (ND – "Not Defined" (1.0)).

Sous-Métrique	**Notation**			
Niveau de remédiation	Unconfirmed (UC)	Uncorroborated (UR)	Confirmée (C)	Non définie (ND)
Valeur	0.9	0.95	1.0	1.0

TABLEAU 3.22 – Sous-Métrique : Rapport de confiance et l'existence de la vulnérabilité (RC)

3.4.3 Métriques Environnementales

Ce groupe de métrique est facultatif dans la version 2 du CVSS, mais dans notre cas, il est indispensable. En effet, il est important de mesurer l'impact de l'environnement (environnement hostile) dans le cas des ICSs. Ce groupe contient des sous-systèmes métriques arborescents.

Dommage collatéral potentiel ou "Collateral Damage Potential" (CDP) :

Cette métrique représente la gravité de dommages potentiels. Elle précise s'il y a une perte de revenu, de patrimoine, de productivité, de vie humaine ou des dommages physiques. Cette métrique contient trois sous-métriques :

- **Impact fonctionnel (FI) :** Cette métrique mesure la gravité des conséquences sur les installations en mesurant l'impact fonctionnel de la vulnérabilité sur la boucle de contrôle automatique. Trois valeurs sont possibles :

  - Perte de la supervision (Loss of View /LoV) (0.5) : Dans ce cas, l'opérateur perd la supervision du processus (par exemple, l'IHM affiche de fausses mesures du processus). Par conséquent, l'opérateur ne peut pas savoir si le processus est toujours en fonctionnement nominal ou le processus est défaillant. En outre, des informations incorrectes ou manquantes, dans le cas ICS, pourraient endommager les installations, causer des pertes humaines, ou des dégâts pour l'environnement. En général, l'opérateur prend des décisions sur la base des informations fournies par le système de supervision afin de garantir le bon fonctionnement et la sécurité du système. En fait, en exploitant une vulnérabilité, l'attaquant pourrait changer ou fabriquer des mesures de capteurs, modifier la configuration de l'équipement et désactiver les dispositifs de sûreté en lançant une attaque de l'homme du milieu (MITM) (Morris et al., 2015).
  - Perte de contrôle (Loss of Control /LoC) (0.3) : Dans ce cas, l'opérateur est capable d'observer le processus (à travers une interface homme-machine par exemple), mais il perd la capacité de commander le système (par exemple, une attaque de type "homme du milieu" peut intercepter et modifier les commandes envoyées par l'opérateur vers les actionneurs.
  - Déni de service (DoS) (0.4) : Il s'agit de tout débordement qui consomme toutes les ressources, que ce soit en cycles de CPU, en mémoire ou en bande passante de communications, et qui, par conséquent, rend le service ou la fonction indisponible (ics,) ("ICS-CERT" 2019).

Sous-métrique	**Notation**		
Impact fonctionnel	Perte de la supervision LoV	Perte de contrôle LoC	Déni de service DoS
Valeur	0.5	0.4	0.3

TABLEAU 3.23 – Métrique : Impact fonctionnel (FI) .

- **Impact sur la sûreté (SI) :** Cette métrique mesure l'impact de la vulnérabilité sur l'environnement, et sur les pertes des vies humaines. Nous adoptons la même définition métrique du potentiel dommage collatéral (CDP) du CVSS version 2. Dans ce cas, les impacts économiques ou de productivité n'ont pas été pris en considération. Cinq valeurs sont possibles : Aucune (0), Faible (0.1), Faible-moyenne (0.3), Moyenne-élevée (0.4) et Élevée (0.5).

Sous-métrique	**Notation**					
Impact sur la sûreté (SI)	Aucune (N)	Faible (L)	Faible -Moyenne (LM)	Moyenne -Élevée (MH)	Élevée (H)	Non Défini (ND)
Valeur	0.0	0.1	0.3	0.4	0.5	0

TABLEAU 3.24 – Métrique : dommages collatéraux potentiels (CDP).

Nombre de cibles impactées ou "Target Distribution" (TD) :

Dans cette métrique, nous utilisons la même définition que la version 2 du CVSS. Elle spécifie la proportion en pourcentage des systèmes vulnérables. Elle peut être Nulle (N – "None" (0.0)), Faible (L – "Low" (0.25)), Moyenne (M – "Medium" (0.75)), Élevé (H – "High" (1.0)) ou bien être Non défini (ND – "Not Defined" (1.0)).

Sous-métrique	**Notation**				
Nombre de cibles impactées (TD)	Aucune (N)	Faible (L)	Moyenne (M)	Élevée (H)	Non Défini (ND)
Valeur	0.0	0.25	0.75	1.0	1.0

TABLEAU 3.25 – Métrique : nombre de cibles impactées (TD).

Exigences de sécurité ou "Security requirements" (CR, IR et AR) :

Nous adoptons la même définition des métriques de la version CVSS. Elle permet d'affiner l'impact de la vulnérabilité sur le ICS donné. Chacune d'elles peut être Faible (L – "Low" (0.5)), Moyenne (M – "Medium" (1.0)), Élevé (H – "High" (1.51)) ou bien être Indéfinie (ND – "Not Defined"(1.0)).

Métrique ou critère	**Notation**			
Exigences de sécurité (CR, IR, AR)	Faible (L)	Moyenne (M)	Élevée (H)	Non Défini (ND)
Valeur	0.5	1.0	1.5	1.0

TABLEAU 3.26 – Métrique : Exigences de sécurité CR, IR, AR.

3.5 Équations de calcul du score

Vu que la couverture de la vulnérabilité par le système de SAF (SS) va influencer beaucoup plus la disponibilité (A) et l'intégrité (I) et pour donner plus d'impact au système de SAF dans les systèmes industriels, nous allons modifier l'équation de base (BS) afin de donner plus d'importance aux systèmes SAF (SS) comme suite :

- le score de base (BS) et leurs sous-scores, l'exploitabilité (ES) et le score d'impact (IS), peuvent être calculés par la formule suivante :

$$\mathrm{ES} = 20 \times \mathrm{AV} \times \mathrm{AC} \times \mathrm{A}u \tag{3.7}$$

$$\mathrm{IS} = 10.41(1-(1-\mathrm{C})(1-\mathrm{I}\times\mathrm{SS})(1-\mathrm{A}\times\mathrm{SS})) \tag{3.8}$$

$$f(\mathrm{IS}) = \begin{cases} 0 & if \quad \mathrm{IS} = 0 \\ 1.176 & if \quad \mathrm{IS} \neq 0 \end{cases} \tag{3.9}$$

$$\mathrm{BS} = \mathrm{R}ound\mathrm{To}\mathrm{D}ec((0.6\times\mathrm{IS}+0.4\times\mathrm{ES}-1.5)\times f(\mathrm{IS})) \tag{3.10}$$

Par contre, les équations et les algorithmes de notation pour les équations temporels et environnementaux restent sans changement.
Le tableau 3.27 présente une comparaison détaillée des métriques du CVSS et de l'ICVSS et de leurs valeurs. Les caractères italiques sont utilisés pour présenter les métriques.

CVSS v 2.0	**ICVSS**
Métriques de base	
Groupe d'exploitabilité	
Access Vector, AV	***Access Vector, AV***
Local (L) ; Adjacent Network (A) ; Network (N).	Sub-metrics group
	Physical Media (PM)
	Phyique (Phy) ; Wired (W) ; Wireless (WL) ;
	Access Layer (AL)
	Physical (P) ; Local (L) ; Adjacent Network (A) ; Network (N).
Access Complexity, AC	***Access Complexity, AC***
Low (L) ; Medium (M) ; High (H).	**System complexity (SC)**
	Simple (S) ; Distributed (D).
	Attack Complexity (ATC)
	High (H) ; Medium (M) ; Low (L).
	Cryptography (C)
	None (N) ; Encrypted (E).
Authentication, Au	***Authentication, Au***
Multiple (M), Single (S), None (N).	Multiple (M) ; Single (S) ; None (N).
Impact group	
Security Impact (C, I, A)	**Security Impact (C, I, A)**
None (N) ; Partial (P) ; Complete (C).	None (N) ; Partial (P) ; Complete (C).
	Safety System, SS
	None (N) ; Safety System (SS).
Métriques temporelles	
Exploitability, E	***Exploitability, E***
Unproven (U) ; Proof-of-Concept (PoC) ; Functional (F) ; High (H) ; Not Defined (ND).	**System Access (SA)**
	Open Source (OS) ; Proprietary (P) ; Not Defined (ND)
	Maturity, M
	Unproven ; Proof-of-concept ; Functional ; Not Defined (ND).
Remediation level, RL	***Remediation level, RL***
Official-fix (OF) ; Temporary-fix (TF) ; Workaround (W) ; Unavailable (U) ; Not Defined (ND) ;	Official-fix (OF) ; Temporary-fix (TF) ; Workaround (W) ; Unavailable (U) ; Not Defined (ND) ;
Report Confidence (RC)	***Report Confidence (RC)***
Unconfirmed (U) ; Uncorroborated (UC) ; Confirmed (C) ; Not Defined (ND).	Unconfirmed (U) ; Uncorroborated (UC) ; Confirmed (C) ; Not Defined (ND).
Métriques environnementales	
Collateral Damage Potential , CDP	***Collateral Damage Potential , CDP***
Low (L) ; Low-medium (LM) ; Medium-high (MH) ; High (H) ; Not Defined (ND).	***Functional Impact , FI***
	Loss of View (LoV) ; Loss of Control (LoC) ; Denial of Service (DoS).
	Safety Impact, SI
	Low (L) ; Low-medium (LM) ; Medium-High (MH) ; High (H) ; Not Defined (ND).
Target Distribution, TD	***Target Distribution, TD***
None (N) ; Low (L) ; Medium (M) ; High (H) ; Not defined (ND).	None (N) ; Low (L) ; Medium (M) ; High (H) ; Not defined (ND).
Security Requirements (CR, IR, AR)	***Security Requirements (CR, IR, AR)***
None (N) ; Low (L) ; Medium (M) ; High (H) ; Not defined (ND).	None (N) ; Low (L) ; Medium (M) ; High (H) ; Not defined (ND).

TABLEAU 3.27 – Comparaison entre les indices de la CVSS v 2.0 et de l'ICVSS

3.5.1 Vecteur ICVSS

Nous adoptons une nouvelle écriture du valeur ICVSS sous la forme suivante :
Vecteur ICVSS= Métrique 1 { sous-métrique 1 & sous-métrique 2 &,..., &sous-métrique n } / Métrique 2 { sous-métrique 1 & sous-métrique 2 &,..., &sous-métrique n } /.../ Métrique N { sous-métrique 1 & sous-métrique 2 &,..., &sous-métrique n }
ou & : représente une fonction définie par l'expert ou l'analyste. Cette fonction peut avoir plusieurs forme : Min, Max, Moyenne.

3.6 Remarque

Dans les sections suivantes, nous allons ignorer la métrique d'exploitabilité (E) et nous supposons que la valeur de cette métrique égale à indéfinie (ND). Cette hypothèse est valable dans les cas d'études de ce chapitre pour des raisons de simplification du problème.

3.6.1 Outil de calcul du score ICVSS

Afin d'automatiser l'obtention du score ICVSS, nous avons développé un outil de calcul avec le logiciel Excel. Sur les figures 3.4, 3.5 une illustration de l'outil.

Industrial Control Vulnerability Scoring System ICVSS

	Criteria	*Notation*	*Value*	*& function: MAX*	*& function: AVERAGE*
Access Vector, AV	**Physical Media (PM):**	Wired (W) : 0.395	0,395	0,646	0,5205
	Access Layer (AL) :	Adjacent Network (A): 0.646	0,646		
Access Complexity, AC	**System complexity [SC]**	Physical (P) : 0.2 Local (L): 0.395 Adjacent Network (A): 0.646 Network (N): 1.0	0,71	0,71	0,676666667
	Attack complexity [ATC]		0,61		
	Cryptography [C] :		0,71		
	Authentication, Au	None (N): 0.704	0,704		
	Confidentiality Impact (C):	None (N): 0	0		
	Integrity Impact (I):	Complete (C) : 0.660	0,66		
	Availablity Impact (A):	Complete (C) : 0.660	0,66		
Exploitability €	**System Access [SA]**	Open Source (OS) : 1.00	1	1	1
	Maturity [M]	not defined: 1.00	1		
	Remediation lavel [RL]:	not defined: 1.00	1		
	Report Confidence (RC):	not defined: 1.00	1		
Collateral Damage Potential (CDP):	**Functional Impact (FI)**	Loss of View (LV): 0.5	0,5	0,5	0,255
	Safety System (SS) :	Safety System (SS): 0.01	0,01		
	Safety Impact (SI):	high: 0.5			
	Target Distribution (TD):	not defined: 1.00	1		
	Security Requirements (CR)	not defined: 1.0	1		
	Security Requirements (IR):	not defined: 1.0	1		
	Security Requirements (AR):	not defined: 1.0	1		

FIGURE 3.4 – Outil de calcul ICVSS : choix des sous-métriques

	MAX FUNCTION	AVERAGE FUNCTION
Exploitability Score= 20* Access Vector * Access Complexity * Authentification.	6,4579328	4,9590464
Impact Score = 10.41*(1 - (1-Confidentiality Impact) * (1-integrity Impact*SS)*(1-Availability Impact*SS)	0,13695854	0,13695854
function impact Score	1,176	1,176
Base Score= round_to_1_decimal([0.6*impact Score + 0.4 * Exploitability Score - 1.5 | *f')	1,4	0,7
The temporal equation is: TemporalScore = round_to_1_decimal(BaseScore*Exploitability_maturity *RemediationLevel*ReportConfidence) .	1,4	0,7
AdjustedImpact = min(10,10.41*(1-(1-ConfImpact*ConfReq)*(1-IntegImpact*IntegReq)*(1-AvailImpact*AvailReq)))	0,13695854	0,13695854
AdjustedBase =((0.6*AjustedImpact)+(0.4*Exploitability score)–1.5)*1.176 == (10.0)	1,370449535	0,665373373
AdjustedTemporal ==AdjustedBase*Exploitability_maturity *RemediationLevel*ReportConfidence) .	1,370449535	0,665373373
	ICVSS	ICVSS
ICVSS = EnvironmentalScore = round_to_1_decimal((AdjustedTemporal+ (10-AdjustedTemporal)*CollateralDamage Potential)*TargetDistribution)	5,7	3,1
SCORE	*5,7*	*3,1*

FIGURE 3.5 – Outil de calcul ICVSS : calcul du score final

3.7 Cas d'étude : système à deux réservoirs

Dans cette section, nous proposons un cas d'étude pour comparer notre système de notation pour les systèmes industriels avec le CVSS V2. Le processus à deux cuves est utilisé (figure 3.6). Les cuves sont physiquement réparties sur deux sites distincts. La coordination entre les deux sites est assurée par un réseau de communication. Nous discutons des vulnérabilités qui affectent le réseau de communication dans lequel le protocole Modbus/TCP est utilisé.

Vulnérabilités du protocole MODBUS/TCP

La conception du protocole MODBUS/TCP contient de multiples vulnérabilités qui pourraient permettre à un attaquant d'effectuer une activité de reconnaissance ou d'émettre des commandes arbitraires (Byres et al., 2004).

- *Manque de confidentialité :* Tous les messages MODBUS sont transmis en texte clair sans aucun mécanisme de protection ou de cryptage lors de la transmission.

- *Manque d'intégrité :* Le Modbus/TCP manque de mécanismes pour assurer l'intégrité

des messages envoyés entre un maître et des esclaves (c'est-à-dire qu'il n'est pas possible de découvrir si le contenu du message original a été modifié par un attaquant).

- *Absence d'authentification :* Il n'y a pas d'authentification à aucun niveau du protocole MODBUS (c'est-à-dire qu'un dispositif compromis pourrait prétendre être le maître et envoyer des commandes aux esclaves). Une exception possible est constituée par certaines commandes de programmation non documentées.

- *Absence de structure de session :* Comme de nombreux protocoles de requête/réponse (c'est-à-dire SNMP, HTTP, etc.), MODBUS/TCP consiste en des transactions de courte durée où le maître lance une requête à l'esclave qui se traduit par une action unique. Si l'on ajoute à cela l'absence d'authentification et la mauvaise génération du numéro de séquence initial (Initial Sequence Number ISN) dans de nombreux dispositifs embarqués, il est possible pour les attaquants d'injecter de fausses commandes.

Les limites de sécurité de MODBUS peuvent être exploitées par des attaquants pour faire échouer des systèmes de contrôle industriels. Nous donnons certaines attaques (Fovino et al., 2009) :

1. *Exécution non autorisée de commandes :* l'absence d'authentification du maître et des esclaves signifie qu'un attaquant peut envoyer de faux paquets à un groupe d'esclaves. Afin d'exécuter cette attaque, l'attaquant doit pouvoir accéder au réseau qui héberge les serveurs SCADA ou au réseau de terrain qui héberge les esclaves. Carcano, et al. (Carcano et al., 2008) montrent que l'attaque peut être lancée en créant un logiciel malveillant qui infecte le réseau et provoque l'envoi automatique de messages malveillants aux esclaves.

2. *Attaques par déni de service (DoS) :* Un exemple d'attaque consiste à jouer le rôle du maître et d'envoyer des messages insignifiants aux RTU, ce qui consomme toutes les ressources de traitement.

3. *Reproduire les paquets :* L'absence de mécanismes d'intégrité permet à l'attaquant de réutiliser des messages Modbus légitimes envoyés vers ou depuis des appareils esclaves. Dans notre cas d'étude, des injections ou une fabrication de fausses trames (fausses mesures) pourraient être lancées en créant complètement de nouveaux paquets à envoyer entre les automates et l'IHM. Le but de l'attaque est de donner au système de supervision des mesures qui sont biaisées par rapport aux mesures réelles . Par exemple, l'envoi de la même valeur de la pression permet de figer affichage d'IHM dans la salle contrôle sur une valeur fixe, alors que la valeur réelle a dépassé seuil de danger.

Dans un premier temps, nous allons évaluer le processus de la figure 3.6 avec l'ICVSS et la CVSS v2. Nous allons construire le vecteur ICVSS en trois étape : Calcul de score de base (BS), calcul de score temporel (TS) et calcul de score environnemental(ES).

Calcul de score de base (BS)

- L'attaquant peut exploiter la vulnérabilité à travers le réseau filaire, la métrique moyen accès (PM) est égale la valeur (W) (filaire) ;

- L'attaquant exploit un réseau local cela implique que la métrique couche d'accès (AL) est égale à la valeur (A) ;

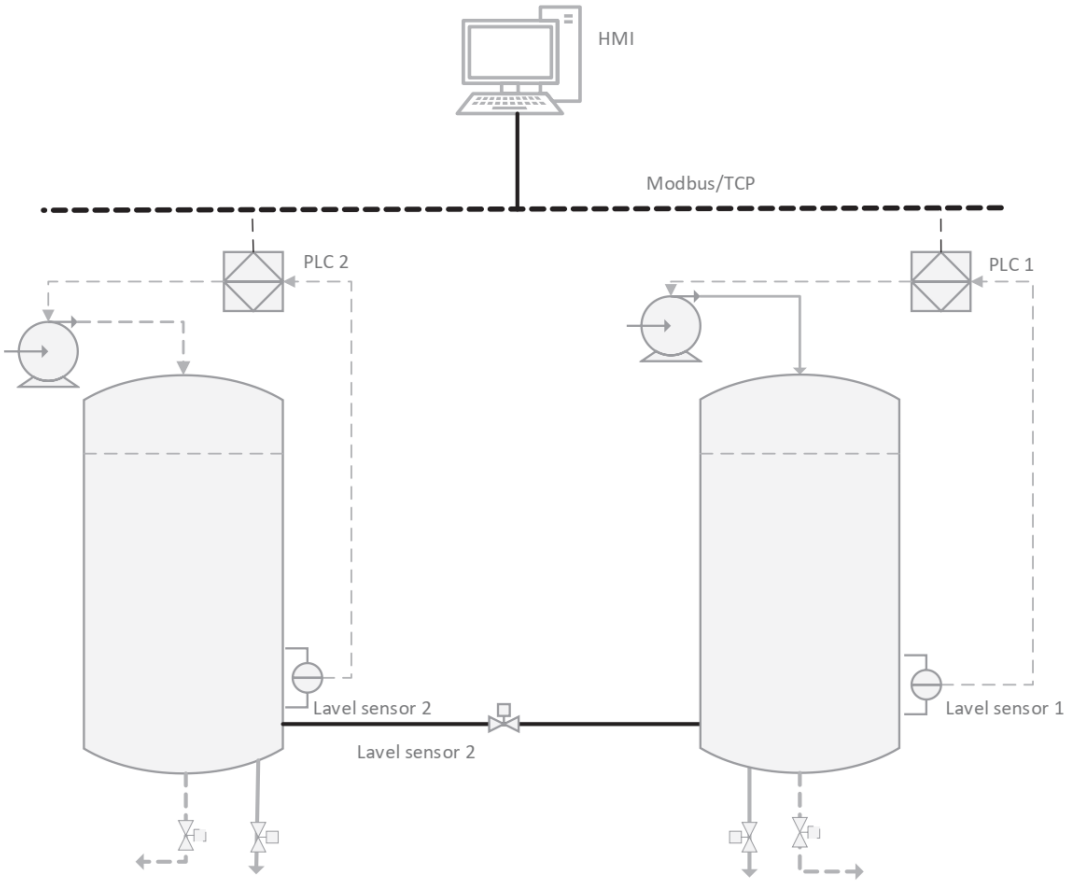


FIGURE 3.6 – Système à deux réservoirs sans système de SAF.

- Nous supposant que la complexité d'attaque (ATC) est égale la valeur Médium (M) ;
- Comme le système est réparti géographiquement sur plusieurs endroits ou sites, la métrique de complexité du système (SC) est égale à la valeur (D) ;
- Le système de communication n'est pas doté d'un système de chiffrement. Cela implique que la métrique cryptographie (C) est égale à la valeur Aucun (N) ;
- Le réseau de communication ne contient pas un système d'authentification (Au), en conséquence la métrique authentification est égale à la valeur Aucun (N) ;
- Le réseau de communication ne contient pas un système d'authentification (Au) égale à la valeur Aucun (N) ;
- L'impact de la confidentialité (C) égale à Aucun (N), car nous supposons que la divulgation des informations des capteurs n'aura pas un impact sur le fonctionnement du système où elle n'est pas utile pour une attaque potentielle ;
- L'impact de l'intégrité (I) égale à la valeur Complète (C), car lorsque l'attaquant réussit un exploit, il pourrait injecter de faux paquets et changer complément toutes mesures des capteurs ;
- l'impact de disponibilité (A) égale à la valeur complète (C), l'exploit peut impacter tout le système et peut causer un arrêt complet ;

- système de SAF (SS) égale à aucun (N), car il n'y a pas un système qui peut couvrir le défaut causé par une potentielle exploit.

La figure 3.7 illustre le choix des métriques qui permet d'avoir le score de base d'ICVSS. La figure aussi montre une comparaison entre le système de score ICVSS et le systèmes de score CVSS v2 dans chaque étape de calcul .

Critères	Sous-critères	Notation					Quantification	Fonction &
Groupe d'exploitabilité								
Vecteur d'accès (AV)	Physical Media (PM)	Phy (0,2)	W (0,395) X	WL (1,0)			0,395	Max(0,646, 0.395) = 0.646
	Couche d'accès (AL) :	P (0,2)	L (0,395)	A (0,646) X	N (1,0)		0,646	
Complexité d'accès (AC)	Complexité d'attaque (ATC)	H (0,35)	M (0.61) X	L (0,71)			0,35	Max(0.35, 0,71, 0.35) = 0.07
	Complexié du System (SC)	S (0,35)	D (0,71) X				0,71	
	Cryptographie (C)	N (0,71) X	C (0,35)				0,35	
Authentication (Au)	Authentication (Au)	N (0,704) X	S (0,56)	M (0,45)			0,704	0,704
Groupe d'impact								
Impact de confidentialité (C)	Impact de confidentialité (C)	N (0) X	P (0,275)	C (0,660)			0	0
Impact d'intégrité (I)	Impact d'intégrité (I)	N (0)	P (0,275)	C (0,660) X			0,66	0,66
Impact de disponibilité (A)	Impact de disponibilité (A)	N (0)	P (0,275)	C (0,660) X			0,66	0,66
Système de SAF (SS)	Système de SAF (SS)	N (0,9) X	SS (0,01)				0,9	0,9

ICVSS		CVSS	
ES= 20* AV * AC* Au	6,4	ES= 20* AV * AC* Au	5,5
Score d'impact (IS) = 10.41*(1 - (1-C*SS)*(1-I*SS)*(1-A*SS))	8,6	IS = 10.41*(1 - (1-C)*(1-I)*(1-A))	9,2
Score de Base (BS) = round([0.6* IS + 0.4 * ES - 1.5] *(1,176 ou 0))	7,5	BS = round([0.6* IS + 0.4 * ES - 1.5] *(1,176 ou 0))	7,4

FIGURE 3.7 – Score de base (BS) du système à deux réservoirs sans un système de SAF (SS)

Calcul de score temporel (TS)

Nous supposant que les sous-métriques : Accès au système (SA), Niveau de correction (RL), Niveau de confiance (RC) sont indéfinies dans ce cas particulier.

La figure 3.8 illustre le choix des métriques qui permet d'avoir les scores temporels.

Critères	Sous-critères	Notation						Quantification	Fonction &
Eploitabilité (E)	Accès au système (SA)	ND (1,0) X	OS (1,0)	P (0,85)				(1,0)	Min(1,0 , 1,0) = 1,0
	Maturité (M)	H (1,0)	F (0,95)	PoC (0,9)	U (0,85)	ND (1,0) X		(1,0)	
Niveau de correction (RL)	Niveau de correction (RL)	OF(0,87)	TF (0,9)	W(0,95)		U (1,0)	ND (1,0) X	1	1
Niveau de confiance (RC)	Niveau de confiance	UC(0,9)	UR (0,95)	C(0,95)		ND (1,0) X		1	1

ICVSS		CVSS	
Score Temporel (TS) = round(BS * E* RL * RC)	7,5	Score Temporel (TS) = round(BS * E* RL * RC)	7,4

FIGURE 3.8 – Score temporel (TS) du système à deux réservoirs sans un système de SAF (SS)

Calcul de score environnemental (ES)

- La métrique Impact fonctionnel (FI) est égale à la valeur LoV, car l'attaque consiste à envoyer de fausses mesures à la salle de contrôle c.-à-d entre les automates (PLC) et IHM qui pourrait causer une perte de la supervision.

- Nous supposons que le dysfonctionnement de la boucle de régulation -qui permet de régler le niveau dans les deux réservoirs- n'est pas toléré et elle peut causer des conséquences catastrophiques. De ce fait, la valeur SI est égale valeur élevée (H).

- Nous supposons que nous n'avons pas des informations sur nombres de cibles qui pourrait être impactés (TD). C'est pourquoi, la valeur TD est égale à valeur indéfini (ND).

- Nous supposons que les exigences de la sécurité : CR, IR, AR sont indéfinis dans ce cas.

La figure 3.9 illustre le choix des métriques qui permet d'avoir les scores environnementaux qui donnent aussi les scores finals de ICVSS et de CVSS.

Critères	Sous-critères	Notation						Quantification	Fonction &
Dommage collatéral potentiel (CDP)	Impact fonctionnel (FI)	LoV (0,5)	LoC (0,3)	Dos (0,4)				0,5	Max(0,5 , 0,5) = 0,5
		X							
	Impact de sûreté (SI)	N (0,0)	L (0,1)	LM (0,3)	MH (0,4)	H (0,5)		0,5	
						X			
Nombre de cibles impactée (TD)	Nombre de cibles impactée (TD)	N(0,0)	L (0,25)	M(0,75)		H (1,0)	ND (1,0)	1	1
							X		
Exigences de Confidentialité (RC)	Exigences de Confidentialité (RC)	L(0,5)	M (1,0)	H(1,51)		ND (1,0)		1	1
						X			
Exigences d'Intégrité (IR)	Exigences d'Intégrité (IR)	L(0,5)	M (1,0)	H(1,51)		ND (1,0)		1	1
						X			
Exigences de Disponibilié (AR)	Exigences de Disponibilié (AR)	L(0,5)	M (1,0)	H(1,51)		ND (1,0)		1	1
						X			

ICVSS		CVSS	
Impact ajusté (AI) = Min (10, 10,41 * (1- (1- C * CR) * (1 - I * *SS*IR) * (1 - A **SS* AR)))	8,6	= Min (10, 10,41 * (1- (1- C * CR) * (1 - I * IR) * (1 - A * AR	9,2
Score de Base ajusté (ABS) =round(((0.6*AI)+(0.4*ES)–1.5)*(1.176 ou 0))	7,4	ABS =round(((0.6*AI)+(0.4*ES)–1.5)*(1.176 ou 0))	7,3
Score Temporel ajusté(ATS)=round(ABS *E *RL*RC)	7,4	ATS=round(ABS *E *RL*RC)	7,3
Score ICVSS = round((ATS+ (10-ATS)*CDP)*TD)	8,8	CVSS = round((ATS+ (10-ATS)*CDP)*TD)	8,7

FIGURE 3.9 – Score final ICVSS du système à deux réservoirs sans un système de SAF (SS)

Le score obtenu est égal à 8.8. Le vecteur correspondant pour l'ICVSS est :

ICVSS = AV{PM :W & AL :A}/AC{ SC :D&ATC :M&C :N}/Au :N/ C :N/I :C/A :C/SS :N/E{SA :ND&M :ND}/RL :ND/RC :ND/CD{FI :LoV&SI :H}/TD :ND/ CR :ND/IR :ND/AR :ND.

Où & : représente la fonction de maximum ou minimum selon la métrique. il permet de calculer le résultat entre les sous-mesures. Dans le cas de CVSS v2, le score obtenu est égal à : 8.7. Le vecteur correspondant est :

CVSS = AV : A/AC : M/ C : N/ I :C / A :C / E : ND/ RL :ND/RC :ND/CDP :H/TD :ND/CR :ND/IR :ND/AR :ND.

D'après le tableau 3.12 le score obtenu est élevé ou critique. Nous devons améliorer une métrique ou plusieurs pour avoir un système plus sécurisé . Pour cette raison, un système de SAF a été adopté pour éviter les événements catastrophiques, tels que le débordement ou la vidange des deux réservoirs (voir la figure 3.10). Nous évaluons le nouveau processus, lorsque le système de SAF a été ajouté. En conséquence, nous devons changer la valeur de la métrique du système de SAF de la valeur : Aucun (N) à la valeur (SS), car le système SAF va couvrir le défaut causé par un exploit potentiel. Les figures (3.11 3.12 3.13) montrent les détails de calcul pour avoir le score final.

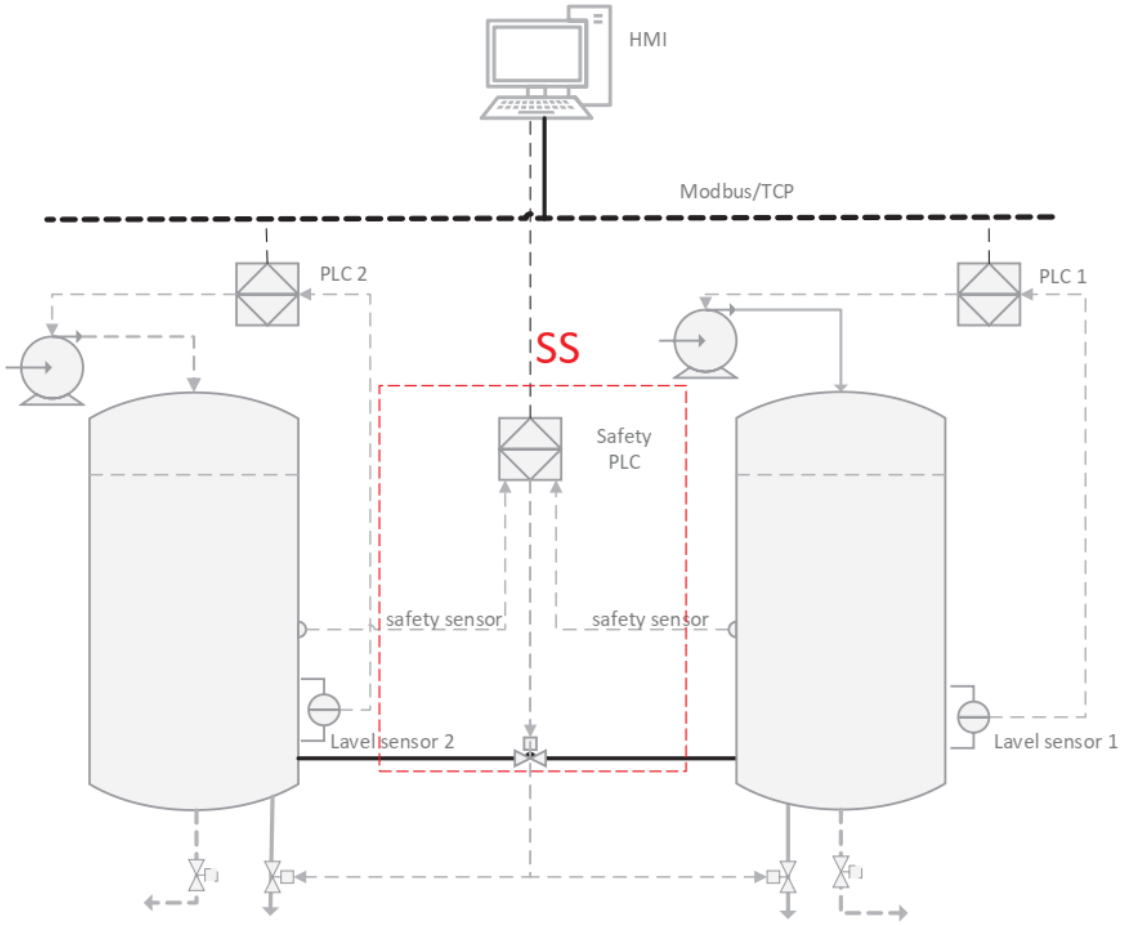


FIGURE 3.10 – Système à deux réservoirs avec un système de SAF (SS).

Critères	Sous-critères	Notation					Quantification	Fonction &
Groupe d'exploitabilité								
Vecteur d'accès (AV)	Physical Media (PM)	Phy (0,2)	W (0,395) X	WL (1,0)			0,395	Max(0,646, 0.395) = 0.646
	Couche d'accès (AL) :	P (0,2)	L (0,395)	A (0,646) X	N (1,0)		0,646	
Complexité d'accès (AC)	Complexité d'attaque (ATC)	H (0,35)	M (0.61) X	L (0,71)			0,35	Max(0.35, 0,71, 0.35) = 0.071
	Complexié du System (SC)	S (0,35)	D (0,71) X				0,71	
	Cryptographie (C)	N (0,71) X	C (0,35)				0,35	
Authentication (Au)	Authentication (Au)	N (0,704) X	S (0,56)	M (0.45)			0,704	0,704
Groupe d'impact								
Impact de confidentialité (C)	Impact de confidentialité (C)	N (0) X	P (0,275)	C (0.660)			0	0
Impact d'intégrité (I)	Impact d'intégrité (I)	N (0)	P (0,275)	C (0,660) X			0,66	0,66
Impact de disponibilité (A)	Impact de disponibilité (A)	N (0)	P (0,275)	C (0,660) X			0,66	0,66
Système de SAF (SS)	Système de SAF (SS)	N (0,9)	SS (0,01) X				0,01	0,01

ICVSS		CVSS	
ES= 20* AV * AC* Au	6,4	ES= 20* AV * AC* Au	5,5
Score d'impact (IS) = 10.41*(1 - (1-C*SS)*(1-I*SS)*(1-A*SS))	0,13	IS = 10.41*(1 - (1-C)*(1-I)*(1-A))	9,2
Score de Base (BS) = round([0.6* IS + 0.4 * ES - 1.5] *(1,176 ou 0))	1,4	BS = round([0.6* IS + 0.4 * ES - 1.5] *(1,176 ou 0))	7,4

FIGURE 3.11 – Score de base (BS) du système à deux réservoirs avec le système de SAF (SS)

Critères	Sous-critères	Notation						Quantification	Fonction &
Eploitabilité (E)	Accès au système (SA)	ND (1,0)	OS (1,0)	P (0,85)				(1,0)	Min(1,0 , 1,0) = (1,0)
		X							
	Maturité (M)	H (1,0)	F (0,95)	PoC (0,9)	U (0,85)	ND (0,85)		(1,0)	
						X			
Niveau de correction (RL)	Niveau de correction (RL)	OF(0,87)	TF (0,9)	W(0,95)		U (1,0)	ND (1,0)	1	1
							X		
Niveau de confiance (RC)	Niveau de confiance	UC(0,9)	UR (0,95)	C(0,95)		ND (1,0)		1	1
						X			

ICVSS		CVSS	
Score Temporel (TS) = round(BS * E* RL * RC)	1,4	Score Temporel (TS) = round(BS * E* RL * RC)	7,4

FIGURE 3.12 – Score temporel (TS) système à deux réservoirs avec un système de SAF (SS)

Critères	Sous-critères	Notation						Quantification	Fonction &
Dommage collatéral potentiel (CDP)	Impact fonctionnel (FI)	LoV (0,5)	LoC (0,3)	Dos (0,4)				0,5	Max(0,5 , 0,5) = 0,5
		X							
	Impact de sûreté (SI)	N (0,0)	L (0,1)	LM (0,3)	MH (0,4)	H (0,5)		0,5	
						X			
Nombre de cibles impactée (TD)	Nombre de cibles impactée (TD)	N(0,0)	L (0,25)	M(0,75)		H (1,0)	ND (1,0)	1	1
							X		
Exigences de Confidentialité (RC)	Exigences de Confidentialité (RC)	L(0,5)	M (1,0)	H(1,51)		ND (1,0)		1	1
						X			
Exigences d'Intégrité (IR)	Exigences d'Intégrité (IR)	L(0,5)	M (1,0)	H(1,51)		ND (1,0)		1	1
						X			
Exigences de Disponibilié (AR)	Exigences de Disponibilié (AR)	L(0,5)	M (1,0)	H(1,51)		ND (1,0)		1	1
						X			

ICVSS		CVSS	
Impact ajusté (AI) = Min (10, 10,41 * (1- (1- C * CR) * (1 - I * *SS*IR) * (1 - A **SS* AR)))	1,36	Min (10, 10,41 * (1- (1- C * CR) * (1 - I * IR) * (1 - A * AR)))	9,2
Score de Base ajusté (ABS) =round(((0.6*AI)+(0.4*ES)–1.5)*(1.176 ou 0))	1,37	ABS =round(((0.6*AI)+(0.4*ES)–1.5)*(1.176 ou 0))	7,3
Score Temporel ajusté(ATS)=round(ABS *E *RL*RC)	1,37	ATS=round(ABS *E *RL*RC)	7,3
Score ICVSS = round((ATS+ (10-ATS)*CDP)*TD)	5,7	CVSS = round((ATS+ (10-ATS)*CDP)*TD)	8,7

FIGURE 3.13 – Score final ICVSS du système à deux réservoirs avec un système de SAF (SS)

Le score obtenu avec l'ICVSS est égal à : 5.7.
Le vecteur correspondant est :

ICVSS = AV{PM :W & AL :A}/AC{SC : D & ATC :M & C :E}/ Au :N / C :N /I :C/A :C/SS :SS/ E{SA :ND& M :ND } /RL :ND/RC :ND/CDP{FI :LoV & SI :H}/TD :ND/CR :ND/IR :ND/AI

Le score obtenu est égal à 5,7, alors que le vecteur CVSS v2 est toujours sans modifications (égal à 8,7).

On constate que le CVSS v2 n'est pas capable d'évaluer les améliorations apportées à la sûreté dans le second système (figure 2). Cela revient à une méconnaissance des spécifications du ICS. Alors que dans la méthodologie ICVSS, le score passe d'une fourchette critique à une fourchette moyenne (voir la tableau 5.1).

En outre, l'identification de la source des incertitudes est essentielle pour développer une méthodologie d'évaluation de risques (comporte le nouveau contexte d'incertitude et de risques de la quatrième révolution industrielle). Ces modélisations ou quantifications ont fait l'objet de plusieurs projets de recherche qui proposent différents modèles mathématiques. Une grande partie de ces recherches présentées cidessous sont basées sur l'approche probabiliste quantifiant les deux types des incertitudes. En fait, le retrait d'une épistémie incertaine par distribution probabiliste est contradictoire. Pour cette raison, plusieurs recherches ont été faites pour trouver des solutions alternatives à ces approches probabilistes. Dans ce contexte, nous trouvons de nombreux concepts et théories

tels que : la théorie des possibilités (Zadeh, 1999), la théorie des évidences (Shafer, 1976) connue sous le nom de théorie de Dempster-Shafer (DST).
Dans le chapitre suivant, nous allons utiliser la logique floue pour modéliser l'incertitude épistémique telle que le manque des connaissances et le raisonnement humain. Cela pourrait améliorer l'évaluation de la vulnérabilité. Plusieurs études ont abordé la notion de l'incertitude dans sa classification. Elle est souvent liée aux interprétations de la probabilité. Il est souvent difficile de trouver un type d'incertitude en raison de leur chevauchement complexe dans la pratique. On trouve souvent dans la littérature, la classification suivante (Ferson and Ginzburg, 1996; Hoffman and Hammonds, 1994) :
-Les incertitudes provenant de la variabilité interne des processus à l'étude ;
-Les incertitudes épistémiques provenant d'un manque de connaissances des paramètres qui caractérisent le processus.
En général, la variation interne dépend de la nature des données d'entrée. Cette nature est souvent traduite mathématiquement par une représentation probabiliste avec plusieurs distributions basées sur des données expérimentales. Par ailleurs, une incertitude épistémique dépend du manque de connaissances ou d'informations incomplètes.

3.8 Conclusion

Dans ce travail, un nouveau système de notation des vulnérabilités est introduit spécifique aux ICSs appelé ICVSS (Industrial Control Vulnerability Scoring System). Nous avons présenté les faiblesses de la version 2 du CVSS classique. Ensuite, nous avons proposé des adaptations pour bien capter les caractéristiques des ICSs. le système de notation ICVSS offre non seulement des informations plus utiles sur la vulnérabilité pour les ingénieurs de SAF, mais aussi des informations plus claires, riches et plus précises par rapport au CVSS. De plus, il aide les ingénieurs de SAF et SAC de parler le même langage pour une meilleure intégration de la SAF et la SEC.
Dans le chapitre suivant, nous allons utiliser la logique floue pour améliorer notre système de score. La logique floue permet d'avoir plus de précision lors de l'évaluation des vulnérabilités.

Chapitre 4

ICVSS-Floue : Méthodologie de notation des vulnérabilités des ICSs basée sur la logique floue

Contents

4.1 Introduction

Nous pouvons noter plusieurs similitudes entre la SAF et la SEC en termes d'évaluation des risques. Ce que l'on appelle un danger dans la SAF est une menace dans la SEC. Cependant, l'approche de l'analyse et évaluation des risques est très différente. En effet, contrairement aux méthodes d'évaluation des risques utilisées en matière de SAF, l'évaluation des risques en matière de la SEC comporte plusieurs paramètres subjectifs tels que les motivations et les compétences de l'attaquant. Cela empêche l'utilisation des méthodes probabilistes quantitatives comme des méthodes d'évaluation des risques des cyberattaques (Braband and Schäbe, 2019). En outre, le manque de données expérimentales et la difficulté de modéliser les facteurs humains compliquent encore toute modélisation mathématique. En effet, nous ne pouvons pas utiliser les données expérimentales de la même façon qu'on les utilise dans les méthodes de la SAF, car le paysage des menaces change tout le temps et les attaquants cherchent toujours de nouvelles techniques pour pirater les systèmes informatiques. Si une nouvelle vulnérabilité est connue ou publiée, l'évaluation des risques doit être mise à jour pour pouvoir estimer les nouveaux risques. Il est donc très important d'évaluer les niveaux de risque et de classer ces vulnérabilités selon un ordre de priorité en fonction de leur degré de criticité. Cela permet par la suite de traiter les menaces par ordre de leur gravité sur le système étudié.

Dans ce chapitre, nous nous focalisons sur la modélisation qui inclut les incertitudes du raisonnement humains. La théorie des ensembles flous et la logique floue fournissent un cadre mathématique le plus approprié (Celikyilmaz and Türksen, 2009) pour modéliser les incertitudes. La différence entre la théorie des ensembles traditionnels et la théorie des ensembles flous réside dans la nature de l'appartenance des éléments. La logique floue introduit donc une notion de degré d'appartenance avec des valeurs comprises entre 0 et 1, ce qui permet de modéliser à la fois le flou et les ambiguïtés du modèle (Zadeh, 1999). En général, un système flou est un système dont les variables peuvent prendre des états qui sont des termes ou des variables linguistiques plutôt que des valeurs numériques. Par exemple, nous pouvons définir la mesure de la température avec de termes linguistiques comme : "Faible", "Moyen", "Élevé", etc. En fait, l'utilisation de variables linguistiques rend les modèles de logique floue plus proches du raisonnement humain (Celikyilmaz and Türksen, 2009). De plus, leur intégration dans les CVSS - qui inclut déjà des paramètres linguistiques-aide les experts ou les ingénieurs à modéliser les incertitudes liées aux choix des paramètres lors l'évaluation des risques. Dans un premier temps , nous allons nous focaliser sur une seule métrique de Vecteur d'accès (AV) pour monter l'utilité de la logique floue. Le vecteur comporte deux sous métriques comme suit (voir le chapitre trois pour plus de détails) : le moyen physique (PM) et la couche d'accès (AL). Cette dernière sous métrique est conçue pour mesurer quelle couche pourrait être exploitée, selon l'endroit où se trouve la vulnérabilité ciblée. Trois valeurs sont possibles pour cette sous-métrique :
- **La première valeur** est attribuée lorsque la vulnérabilité se trouve dans la valeur du réseau type le WAN (Wide Area Network) et le MAN (Metropolitan Area Network).
- Ensuite **la deuxième valeur** est divisée en 4 niveaux selon le modèle CIM (Computer Integrated Manufacturing model). En fait, le CIM a été conçu pour être la réponse à la recherche de performance en créant une segmentation verticale du réseau. Le CIM représente 4 niveaux de décision de l'entreprise, allant du niveau Capteur/Actionneur, qui nécessite un transfert efficace et en temps réel (quelques millisecondes), mais avec peu d'informations (données binaires), au niveau gestion des opérations commerciales qui nécessite de transmettre de grands volumes d'informations. Les fabricants des automates programmables ont créé des réseaux et des bus adaptés aux besoins.
- Des bus de capteurs et d'actionneurs simples ;
- Des bus d'appareils : ce niveau de réseaux comprend la communication entre : robots, axes, etc ;
- Des bus de terrain : les bus de terrain ou réseaux de communication comprennent la communication entre les unités de traitement (automates, superviseurs, commandes numériques, ... ,etc.).
- Les réseaux industriels locaux, pour l'établissement de la communication entre le système automatisé et le monde informatique.

Aujourd'hui, il existe plusieurs types de bus de terrain (voir la figure 4.1). Nous citons les bus de terrain les plus connus : PROFIBUS, AS-I, MODBUS, CAN-Bus que l'on peut encore trouver sur certaines applications et des réseaux plus développés tels que PROFINET, MODBUS-TCP, EtherCAT, CC-link, Ethernet-IP, Powerlink, ... Ces protocoles sont distribués sur les 4 niveaux du modèle CIM.

Sur la figure 4.1(Wollschlaeger et al., 2017), nous montrons la connexion entre ces niveaux. Pour exploiter une vulnérabilité, les attaquants doivent compromettre les niveaux supérieurs pour atteindre les niveaux inférieurs où se trouve cette vulnérabilité. Pour cette raison, nous accordons de moins en moins de valeur, lorsque la vulnérabilité est de plus

en plus proche du bus des capteurs et des actionneurs. Cela signifie que plus la vulnérabilité est plus proche de niveau terrain plus la vulnérabilité est difficile à atteindre.

La troisième valeur de cette sous-métrique est Physique. Cette valeur est attribuée lorsque l'attaquant a besoin d'un accès physique pour exploiter la vulnérabilité. Cela inclut également l'exploitation physique des vulnérabilités des capteurs et les actionneurs (comme la vulnérabilité des canaux secondaires).

La figure 4.2 montre le lien entre ces niveaux. Nous utilisons la logique floue pour modéliser la connaissance de l'expert et aussi l'incertitude des différentes métriques. Cette méthodologie permet d'évaluer les vulnérabilités en fonction de leur proximité avec le niveau de Capteur/Actionneur (la valeur Physique) ou, à l'inverse, de leur proximité avec le monde externe (réseau Internet). Par exemple, les deux protocoles AS-i et Modbus-TCP sont considérés tous les deux comme un réseau local (LAN) lorsque nous utilisons le ICVSS classique . Mais, dans le cas du système de notation des vulnérabilités floue, nous pouvons différencier entre les deux protocoles de communication. En effet, le protocole AS-i est plus proche de la valeur Physique (Ph) que la valeur Réseaux (N), contrairement au protocole Modbus-TCP qui est considéré comme plus proche de la valeur réseau (N) plutôt que la valeur physique (Ph). Nous pouvons attribuer les valeurs suivantes :

- le protocole AS-i est 70% (LAN) et 30% est (Ph).
- le protocole modbus-TCP est est 70% (LAN) et 30% est (N).

Cela permet de donner plus de flexibilité et de précision pour l'évaluation des vulnérabilités.

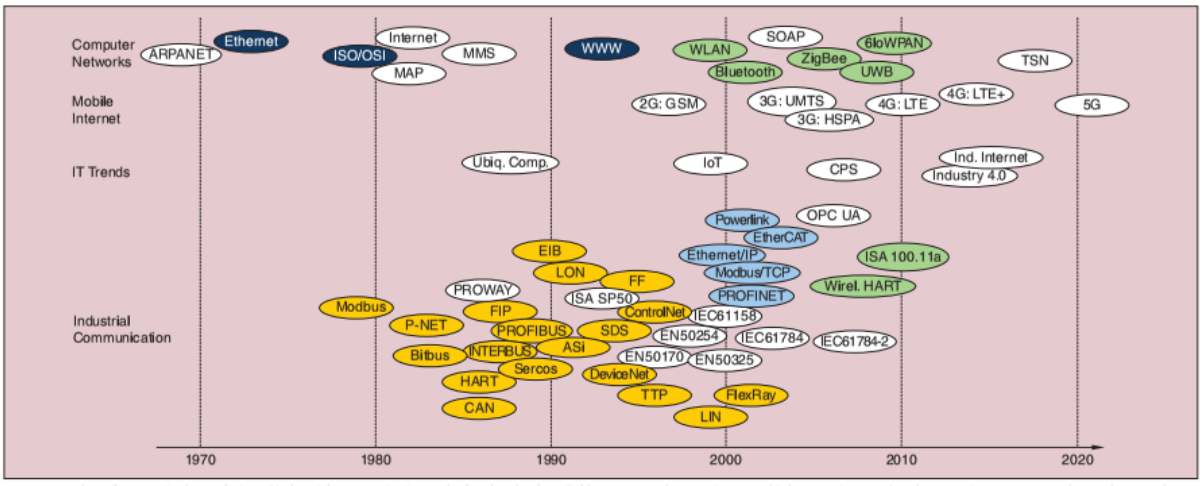


FIGURE 4.1 – Protocoles de communication dans les ICS et les secteurs technologiques associés (Wollschlaeger et al., 2017).

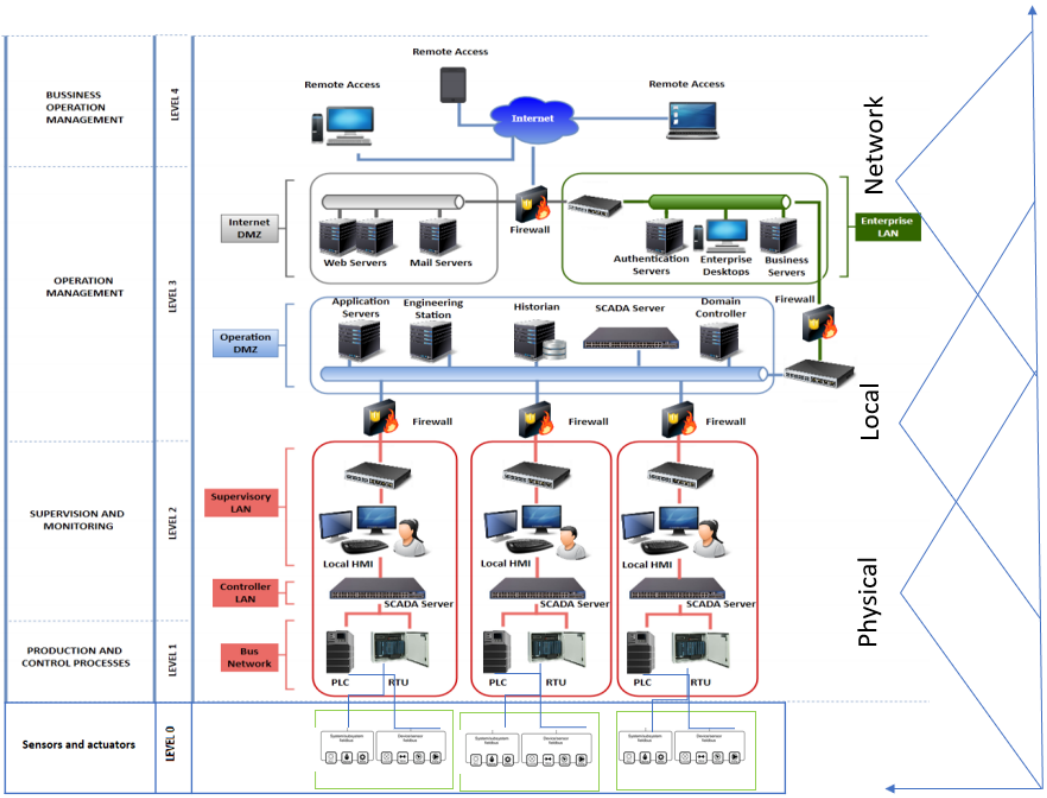


FIGURE 4.2 – Sous-métrique de la couche d'accès (AL)

4.2 Logique floue

4.2.1 Introduction

Les humains peuvent souvent gérer différents types de situations complexes en utilisant des informations, dont beaucoup sont subjectives, imprécises et incertaines.

Parmi les nombreuses formes d'incertitude, comme le montre la figure 4.3, deux groupes d'incertitude nous apparaissent importants si l'on considère les alternatives au niveau des protocoles de communication : l'Imprécision (Vagueness) et l'ambiguïté. L'imprécision est généralement définie comme la difficulté de faire des distinctions claires et précises dans le cas du manque d'informations détaillées (Sauter, 2007) (Celikyilmaz and Türksen, 2009). D'autre part, l'ambiguïté est définie comme des relations où il n'y a pas de choix clair entre plusieurs alternatives. Les ensembles flous permettent de traiter ces différents types d'incertitude. (Celikyilmaz and Türksen, 2009). Le concept de modélisation dite "Floue" trouve son origine dans la théorie des ensembles flous proposée en 1965 par Zadeh (Zadeh, 1965b), comme un moyen de traiter l'incertitude, basée sur l'idée de définir des ensembles pouvant contenir des éléments de manière progressive. Cette théorie a introduit une façon de formaliser les méthodes raisonnement humaines, en utilisant des bases de règles et des variables linguistiques pour la représentation de la connaissance (Zadeh, 1973). La plupart des applications développées dans les années 1980 et 1990 étaient basées sur une approche "basée sur la connaissance" qui reposait sur l'expertise d'un opérateur pour un problème donné de complexité limitée. Lorsque nous voulions passer à des problèmes plus complexes, il était difficile d'écrire (même pour un expert) des bases de règles volumineuses et l'approche basée sur la connaissance n'était plus appropriée. Pour faire face à ce problème, nous proposons une approche largement utilisée dans la théorie du contrôle appelée théorie de Takagi-Sugeno (TS).

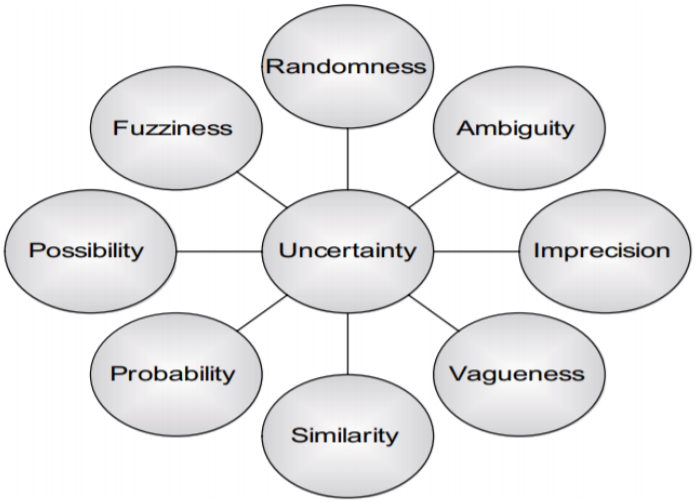


FIGURE 4.3 – Différents types d'incertitudes (Celikyilmaz and Türksen, 2009).

4.2.2 Théorie de Takagi-Sugeno

L'algorithme de logique flou permet de modéliser les incertitudes de l'expert lors la prise de la décision sur le choix des métriques. Deux types d'algorithmes flous sont les plus connus à savoir Mamdani et Takagi segeno. Le modèle TS comme le modèle de Mamdani (Mamdani, 1977), est construit sur une base de règles "Si...Alors...", dans lequel si la prémisse est toujours exprimée linguistiquement, la conséquence utilise des variables numériques plutôt que des variables linguistiques. La conséquence peut être exprimée, par exemple, sous forme de constante, de polynôme selon les variables associées à l'antécédent. L'utilisation de l'algorithme flou de Mamdani augmente le nombre des règles floues qui explosent d'une manière exponentielle avec le nombre de métriques. Cependant, l'algorithme de Takagi Segeno permet non seulement d'utiliser la puissance de la logique floue pour modéliser les incertitudes, mais aussi d'automatiser la génération de règles floues en utilisant les équations de base, temporelles et environnementales du CVSS dans l'étape que l'appelle : la defuzzification.

Dans la théorie Takagi-Sugeno, la sortie du modèle est obtenue à partir d'une combinaison d'opérations d'inférence et de défuzzification (Galichet, 2001). La sortie finale est calculée comme la moyenne des sorties correspondant aux règles, pondérées par le degré de réalisation normalisé, selon l'expression (Takagi and Sugeno, 1985).Dans ce cas, par une fonction d'appartenance (multivariable) de la forme (voir la figure 4.4) :

$$\mu(x) : \Re^p \rightarrow [0,1] \tag{4.1}$$

la proposition de l'antécédent "x est A_i" est normalement exprimée comme une combinaison logique de propositions simples avec des sous-ensembles flous unidimensionnels définis pour les composantes individuelles du vecteur x, généralement sous la forme conjonctive suivante :

$$\mathrm{R}_i : \textbf{si } x_i \; est \; \mathrm{A}_{i1} \textbf{ et } x_2 \; est \; \mathrm{A}_{i2} \textbf{ et } ... \textbf{ et } x_p \; est \; \mathrm{A}_{ip} \textbf{ Alors } y_i = f_i(x), i = 1, ..., r \tag{4.2}$$

où R_i désigne la i-ème règle. r est le nombre de règles contenues dans l'ensemble de règles. $x \in \Re^p$ représente les valeurs des métriques (antécédent) A_i est le sous-ensemble flou de l'antécédent de la i-ème règle. Les vecteurs d'entrée sont définis comme $x = [x_1 x_2, ..., x_n]^{\mathrm{T}}$, ou x_i représente les variables linguistiques floues.

$$T(x_i) = A_i^1, A_i^2, ..., A_i^{m_i} \tag{4.3}$$

où $i = 1,2,..,n,,$ A_i^j $(j = 1,2...m_i)$ représente les j-ème valeur de la variable linguistique x_i, qui est un ensemble flou défini sur le domaine U_i .

La fonction d'appartenance associée de A_i^j est $\mu_{A_i^j}(x_i)$, $i = 1,2,...,n$; $j = 1,2,...,m_i$

$$\alpha_i = \mu_{A_1^j}(x_1) \cap \mu_{A_2^j}(x_2) \cap ... \cap \mu_{A_n^j}(x_n) \tag{4.4}$$

ou

$$\alpha_i = \mu_{A_1^j}(x_1)\, \mu_{A_2^j}(x_2) ... \mu_{A_n^j}(x_n) \tag{4.5}$$

La defuzzification du modèle flou de TS est donnée par (Takagi and Sugeno, 1985) :

$$\sum \text{TS} = \frac{\sum_{j=i}^{m} \alpha_i y_i}{\sum_{j=i}^{m} \alpha_i} \tag{4.6}$$

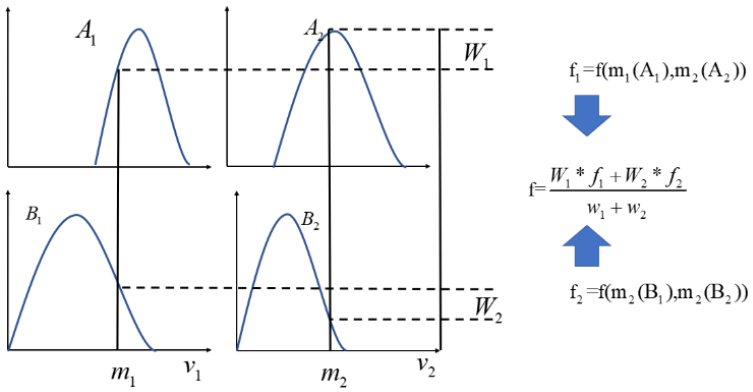


FIGURE 4.4 – Defuzzification de Takagi Segino

4.3 ICVSS basé sur le Modèle Takagi Segino (TS)

L'algorithme proposé 4.6 comporte deux couches. La première couche traite les sous-métriques, en utilisant la fonction Max ou Min pour calculer la sortie (les métriques). Ces métriques élémentaires sont injectées dans la deuxième couche qui utilise les équations d'ICVSS pour calculer le score final (voir les figures 4.7 et 4.6).

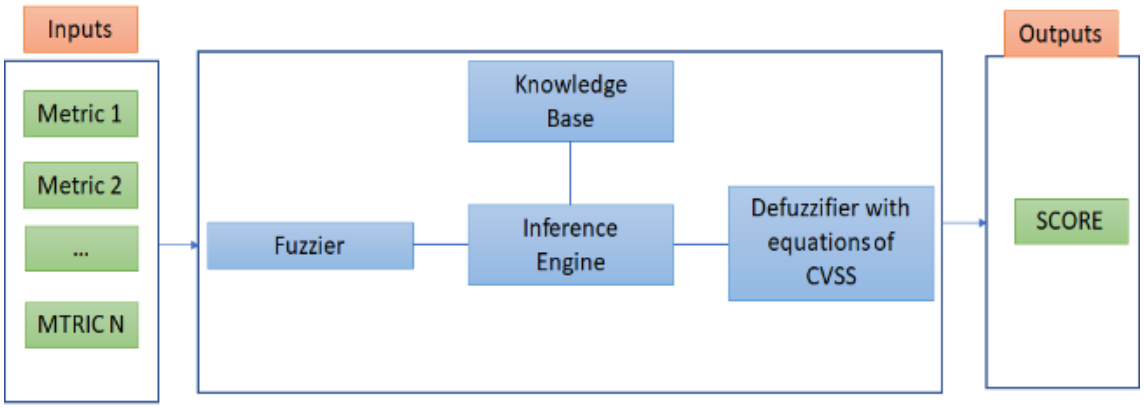


FIGURE 4.5 – Concepts de la logique floue.

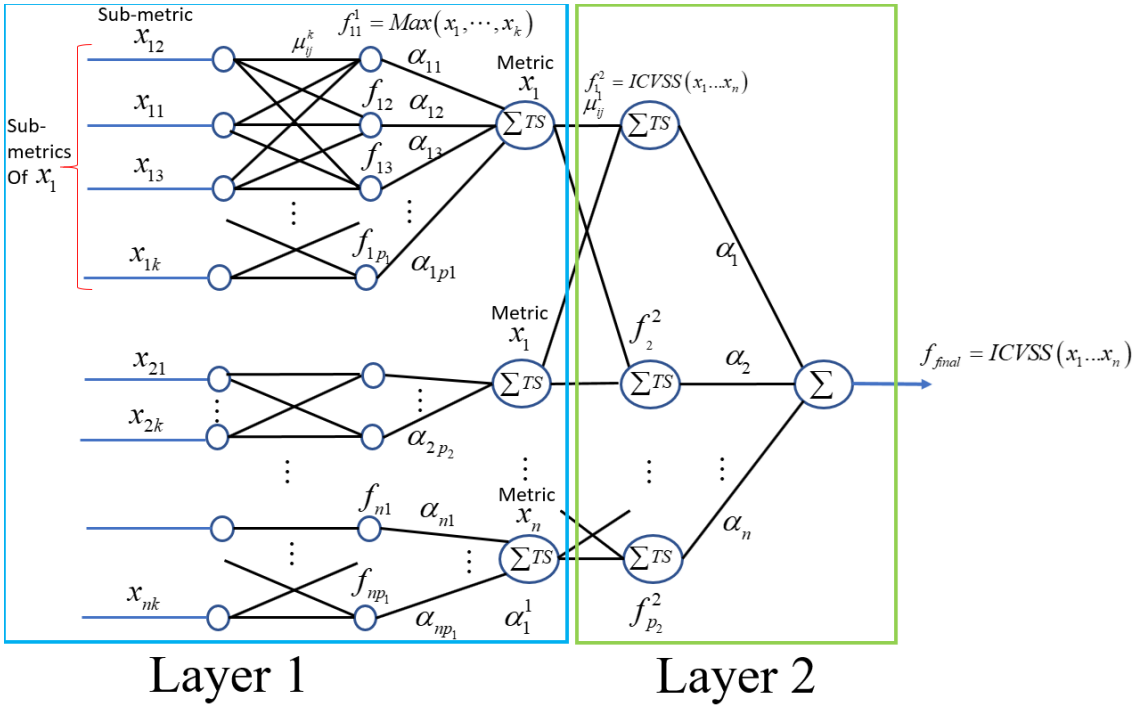


FIGURE 4.6 – ICVSS basé sur l'algorithme de Takagi-Sugeno

Dans l'équation (4.6), nous remplaçons $f_i(x)$ par la fonction $Max(x_i)$ ou $Min(x_i)$ dans le cas de la couche des sub-métriques, ce qui permet d'avoir le pire cas entre les sous métriques (pour plus de détails voir la fonction & dans chapitre 3). Par contre, nous remplaçons $f_i(x)$ par les équations base, temporelles, environnementales, dans le cas de la couche métrique (Voir les figures 4.6 et 4.7). Les équations de la defuzzification sont données dans les équations (3.10) , (3.5), (3.6).

Les fonctions d'appartenances de type triangle sont utilisées de telle manière que les sommets des fonctions d'appartenance correspondent aux valeurs de sub-métrique de la version 2 du CVSS, et le chevauchement entre les fonctions d'appartenance (Voir la figure 4.8a, 4.8b, 4.9a, 4.9b) donne :

$$\sum_{j=i}^{m} \alpha_i(x) = 1 \tag{4.7}$$

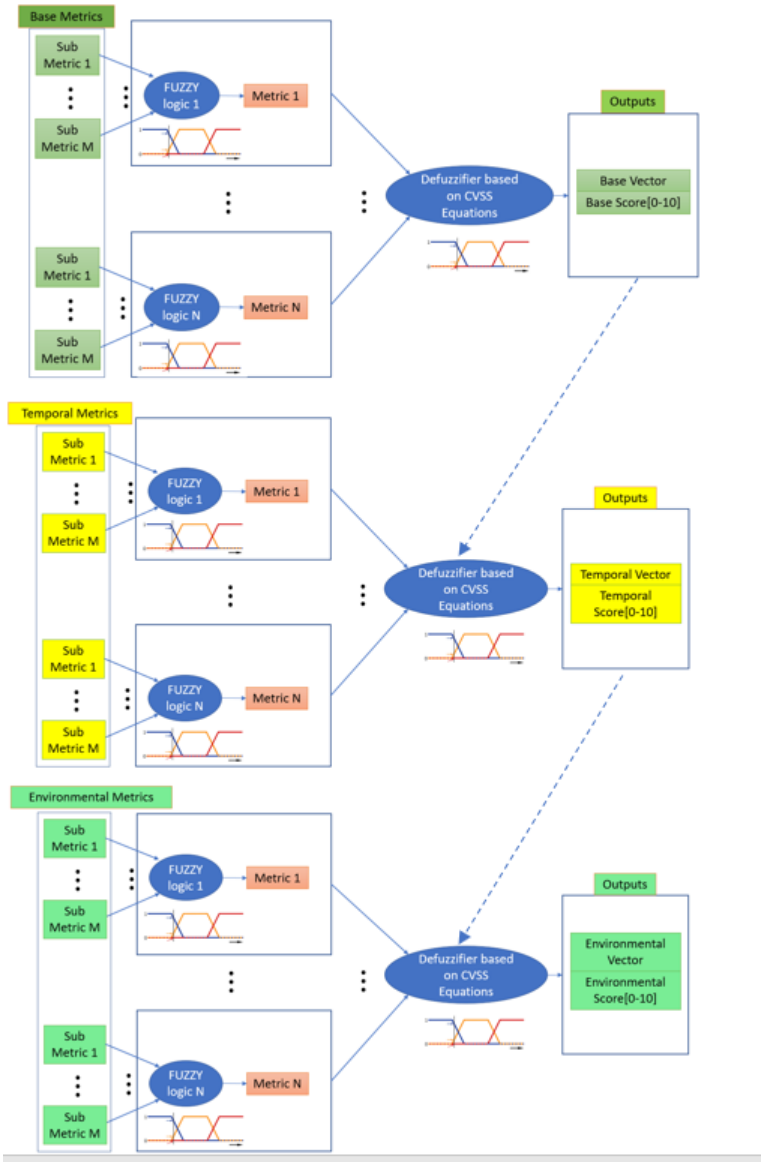
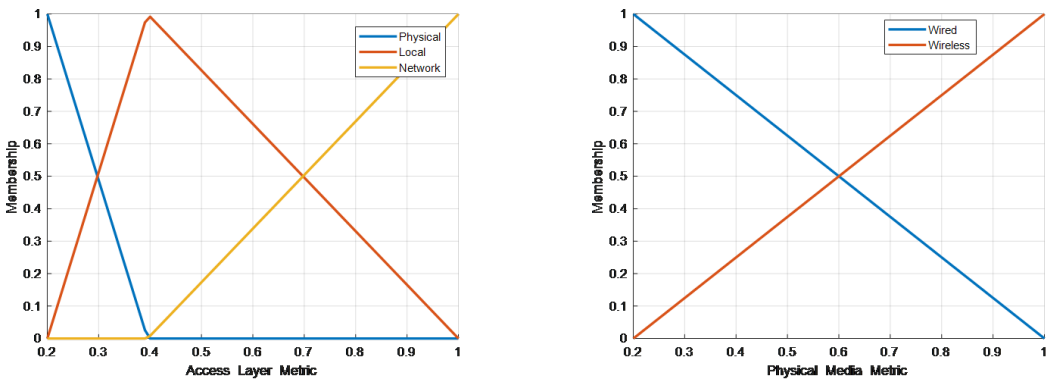
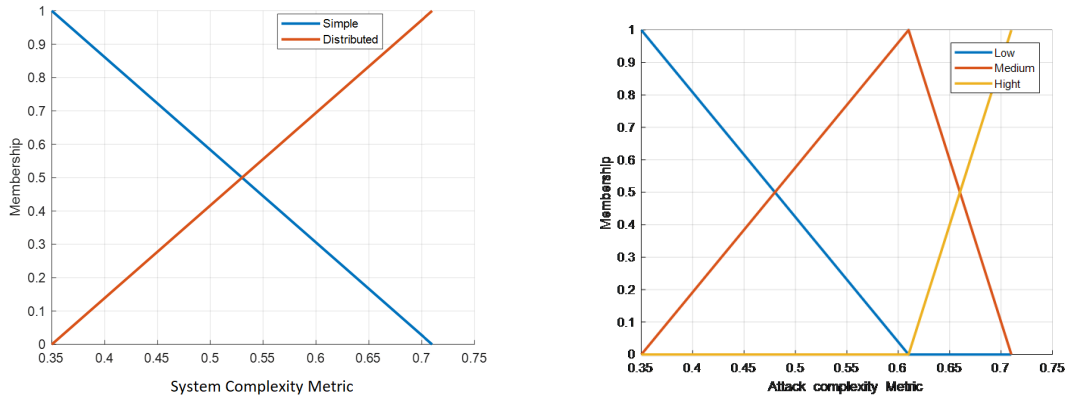


FIGURE 4.7 – Méthodologie floue ICVSS



(a) (b)

FIGURE 4.8 – Fonctions d'appartenance de : (a) couche d'accès (AL) , (b) moyen physique (PM)



(a) (b)

FIGURE 4.9 – Fonctions d'appartenance de : (a) complexité du système (SC), (b) complexité attaque (AC)

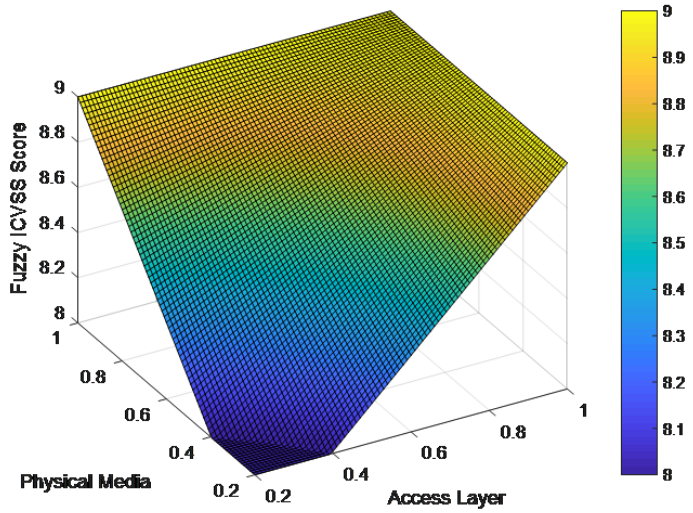


FIGURE 4.10 – Variation du score ICVSS flou par rapport à la couche d'accès (AM) et au moyen physique (PM)

Nous remarquons que le score final est proportionnel à la métrique de la couche d'accès (AC) et au moyen physique (PM) (voir la figure 4.10). Cela signifie que la gravité des risques est proportionnelle au degré de connectivité avec le monde extérieur (lorsque l'installation est plus connectée au monde extérieur plus le risque augmente).

4.3.1 Cas d'étude : Centrale électrique à eau bouillante

Dans cette section, nous proposons un cas d'étude pour démontrer comment notre système de notation floue nous donne plus de flexibilité dans l'évaluation des vulnérabilités.

Pour ce faire, nous appliquons l'approche proposée sur la centrale électrique d'eau bouillante (Boiling Water Power Plant) BWPP (Tan et al., 2005). L'architecture de cette centrale est décrite à la figure 4.11. Comme indiqué, cette architecture se compose de trois couches de réseaux : un réseau d'entreprise contenant des stations de travail, des

serveurs d'application, un réseau de contrôle comprenant des contrôleurs, des serveurs de contrôle et une IHM et un réseau physique contenant différents capteurs : un capteur pour mesurer le niveau d'eau ; un capteur pour lire la pression de la vapeur à l'intérieur du réservoir ; et un capteur pour lire l'électricité produite. Le réseau communique aussi avec des actionneurs suivants : vanne de combustible, vanne de vapeur et vanne d'alimentation d'eau.

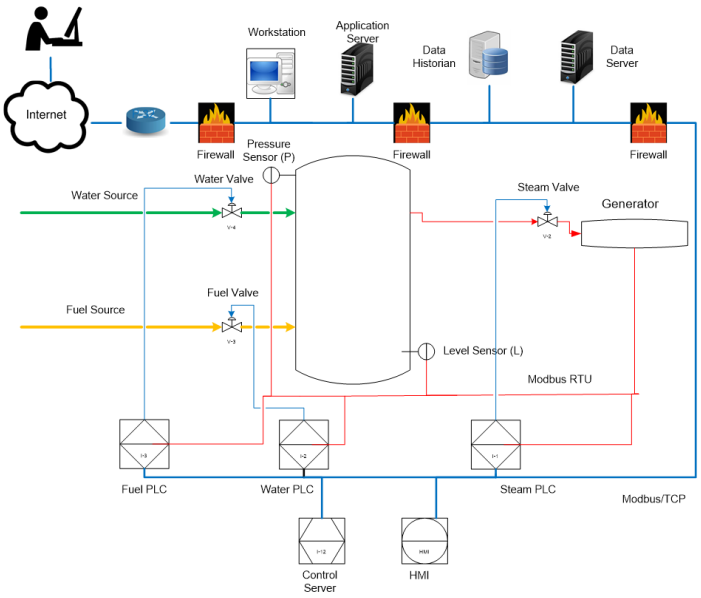


FIGURE 4.11 – Architecture 1 : The boiling water power plant with demilitarized zone (DMZ)

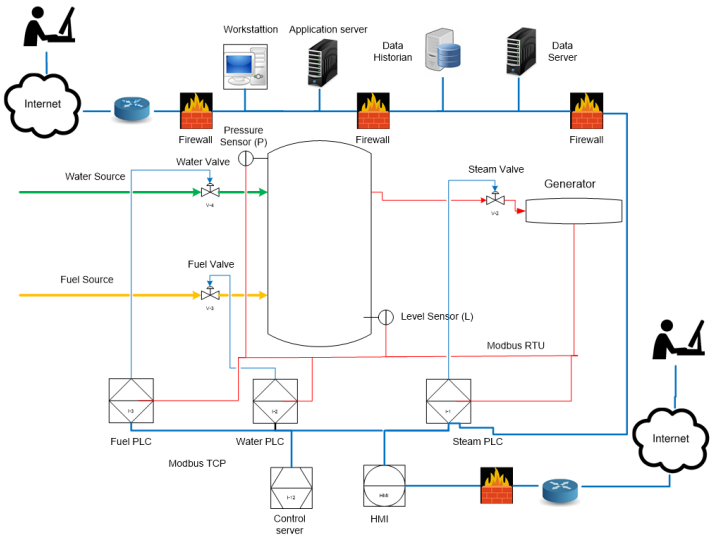


FIGURE 4.12 – Architecture 2 : The boiling water power plant without demilitarized zone (DMZ)

Nous discutons les vulnérabilités qui affectent le réseau de communication dans lequel le protocole Modbus TCP/RTU est utilisé. Dans ce cas, les attaques par injection ou par fabrication pourraient être lancées en créant complètement de nouveaux paquets à envoyer entre les automates et l'IHM.

Dans un premier temps, dans le cas de la version CVSS, le vecteur d'accès métrique est égal à valeur Local (L) dans les deux cas ; la vulnérabilité du Modbus/RTU ou du Modbus/TCP est la même dans les deux architectures.

CVSS = AV : L /AC : L/ C : N/ I :C / A :C / E : ND/RL :ND/RC :ND/CDP :H/TD :ND/CR :ND /IR :ND/AR :ND = 8.0.

Tandis que, en cas d'ICVSS flou, nous savions déjà que Modbus/RTU est plus proche de la métrique physique (70 % physique et 30 % local) que Modbus/TCP (30 % physique et 70 % local).

Vulnérabilité de Modbus/RTU par rapport à l'architecture (1) :

Les figures 4.13, 4.14, 4.15 illustrent le choix des métriques de bases, temporelles, environnementales qui permet d'avoir le score de ICVSS floue.

Critères	Sous-critères	Notation					Quantification
Groupe d'exploitabilité							
Vecteur d'accès (AV)	Physical Media (PM)	Phy (0,2)	W (0,395)	WL (1,0)			0,25
		0%	**100%**	**0%**			
	Couche d'accès (AL) :	P (0,2)	L (0,395)	N (1,0)			
		70%	**30%**	**0%**			
Complexité d'accès (AC)	Complexité d'attaque (ATC)	H (0,35)	M (0.61)	L (0,71)			0,71
		0%	**0%**	**100%**			
	Complexié du System (SC)	S (0,35)	D (0,71)				
		100%	**0%**				
	Cryptographie (C)	N (0,71)	C (0,35)				
		100%	**0%**				
Authentication (Au)	Authentication (Au)	N (0,704)	S (0,56)	M (0,45)			0,704
		100%					
Groupe d'impact							
Impact de confidentialité (C)	Impact de confidentialité (C)	N (0)	P (0,275)	C (0,660)			0
		100%					
Impact d'intégrité (I)	Impact d'intégrité (I)	N (0)	P (0,275)	C (0,660)			0,66
				100%			
Impact de disponibilité (A)	Impact de disponibilité (A)	N (0)	P (0,275)	C (0,660)			0,66
				100%			
Système de SAF (SS)	Système de SAF (SS)	N (0,9)	SS (0,01)				0,9
		100%					

FIGURE 4.13 – Métriques de base pour Modbus/RTU de l'architecture (1)

Critères	Sous-critères	Notation					Quantification
Eploitabilité (E)	Accès au système (SA)	ND (1,0)	OS (1,0)	P (0,85)			(1,0)
		100%	**0%**	0%			
	Maturité (M)	H (1,0)	F (0,95)	PoC (0,9)	U (0,85)	ND (1,0)	0,9
		0%	**0%**	**0%**	**0%**	**100%**	
Niveau de correction (RL)	Niveau de correction (RL)	OF(0,87)	TF (0,9)	W(0,95)		U (1,0) ND (1,0)	1
		0%	**0%**	**0%**		**0%** **100%**	
Niveau de confiance (RC)	Niveau de confiance (RC)	UC(0,9)	UR (0,95)	C(0,95)		ND (1,0)	1
		0%	**0%**	**0%**		**100%**	

FIGURE 4.14 – Métriques temporelles pour Modbus/RTU de l'architecture (1)

Critères	Sous-critères	Notation					Quantification
Dommage collatéral potentiel (CDP)	Impact fonctionnel (FI)	LoV (0,5)	LoC (0,3)	Dos (0,4)			0,5
		100%					
	Impact de sûreté (SI)	N (0,0)	L (0,1)	LM (0,3)	MH (0,4)	H (0,5)	0,5
		0%	**0%**	**0%**	**0%**	**100%**	
Nombre de cibles impactée (TD)	Nombre de cibles impactée (TD)	N(0,0)	L (0,25)	M(0,75)		H (1,0) ND (1,0)	1
		0%	**0%**	**0%**		**0%** **100%**	
Exigences de Confidentialité (RC)	Exigences de Confidentialité (CR)	L(0,5)	M (1,0)	H(1,51)		ND (1,0)	1
		0%	**0%**	**0%**		**100%**	
Exigences d'Intégrité (IR)	Exigences d'Intégrité (IR)	L(0,5)	M (1,0)	H(1,51)		ND (1,0)	1
		0%	**0%**	**0%**		**100%**	
Exigences de Disponibilié (AR)	Exigences de Disponibilié (AR)	L(0,5)	(Ctrl)	H(1,51)		ND (1,0)	1
		0%	**0%**	**0%**		**100%**	

FIGURE 4.15 – Métriques environnementaux pour Modbus/RTU de l'architecture (1)

la représentation du vecteur de cette exemple est donné comme suit :

Fuzzy ICVSS = AV{PM :{100%W} & AL : {70%Ph ;30%L}/AC{SC :100%S&ATC :{100%L} /Au :{100%N}/C :{100%N}/I :{100%C}/A :{100%C}/SS :{100%N}/E :{100%ND}/ RL :{100%ND}/RC :{100%ND}/CDP{FI :{100%LoV}&SI :{100%H}} TD :{100%H}/CR :{100%ND}/IR :{100%ND} /AR :{100%ND}=7.9.

Où & : est une fonction choisie grâce à l'expertise de l'utilisateur. Dans notre cas, nous utilisons la fonction maximum ou minimum -selon la métrique- pour obtenir le résultat entre les sous-métriques. Et { } est le vecteur des sous-métriques. % représente le niveau de la fonction d'appartenance.

Vulnérabilité Modbus/TCP par rapport à l'architecture (1) :

Comme protocole Modbus/TCP est plus proche aux couches en dessous par rapport Modbus/RTU . Nous devons changer les poids des sous-métriques (dans ce cas 30% pour la valeur Phy et 70% pour la valeur locale). Donc, nous modifions que la sous-métrique (AL) et le reste des métriques restent sans changement. Les figures 4.16, 4.17, 4.18 illustrent le choix des métriques de bases, temporelles, environnementales qui permet d'avoir le score de ICVSS floue final.

Critères	Sous-critères	Notation					Quantification
Groupe d'exploitabilité							
Vecteur d'accès (AV)	Physical Media (PM)	Phy (0,2)	W (0,395)	WL (1,0)			0,3365
		0%	**100%**	**0%**			
	Couche d'accès (AL) :	P (0,2)	L (0,395)	N (1,0)			
		30%	**70%**	**0%**			
Complexité d'accès (AC)	Complexité d'attaque (ATC)	H (0,35)	M (0.61)	L (0,71)			0,71
		0%	**0%**	**100%**			
	Complexié du System (SC)	S (0,35)	D (0,71)				
		100%	**0%**				
	Cryptographie (C)	N (0,71)	C (0,35)				
		100%	**0%**				
Authentication (Au)	Authentication (Au)	N (0,704)	S (0,56)	M (0,45)			0,704
		100%					
Groupe d'impact							
Impact de confidentialité (C)	Impact de confidentialité (C)	N (0)	P (0,275)	C (0,660)			0
		100%					
Impact d'intégrité (I)	Impact d'intégrité (I)	N (0)	P (0,275)	C (0,660)			0,66
				100%			
Impact de disponibilité (A)	Impact de disponibilité (A)	N (0)	P (0,275)	C (0,660)			0,66
				100%			
Système de SAF (SS)	Système de SAF (SS)	N (0,9)	SS (0,01)				0,9
		100%					

FIGURE 4.16 – Métriques de base pour Modbus/TCP de l'architecture (1)

Critères	Sous-critères	Notation						Quantification
Eploitabilité (E)	Accès au système (SA)	ND (1,0)	OS (0,85)	P (1,0)				(1,0)
		100%	**0%**	**0%**				
	Maturité (M)	H (1,0)	F (0,95)	PoC (0,9)	U (0,85)	ND (1,0)		0,9
		0%	**0%**	**0%**	**0%**	**100%**		
Niveau de correction (RL)	Niveau de correction (RL)	OF(0,87)	TF (0,9)	W(0,95)		U (1,0)	ND (1,0)	1
							100%	
Niveau de confiance (RC)	Niveau de confiance (RC)	UC(0,9)	UR (0,95)	C(0,95)		ND (1,0)		1
		0%	**0%**	**0%**		**100%**		

FIGURE 4.17 – Métriques temporelles pour Modbus/TCP de l'architecture (1)

Critères	Sous-critères	Notation						Quantification
Dommage collatéral potentiel (CDP)	Impact fonctionnel (FI)	LoV (0,5)	LoC (0,3)	Dos (0,4)				0,5
		100%						
	Impact de sûreté (SI)	N (0,0)	L (0,1)	LM (0,3)	MH (0,4)	H (0,5)		0,5
		0%	**0%**	**0%**	**0%**	**100%**		
Nombre de cibles impactée (TD)	Nombre de cibles impactée (TD)	N(0,0)	L (0,25)	M(0,75)		H (1,0)	ND (1,0)	1
		0%	**0%**	**0%**		**0%**	**100%**	
Exigences de Confidentialité (RC)	Exigences de Confidentialité (CR)	L(0,5)	M (1,0)	H(1,51)		ND (1,0)		1
		0%	**0%**	**0%**		**100%**		
Exigences d'Intégrité (IR)	Exigences d'Intégrité (IR)	L(0,5)	M (1,0)	H(1,51)		ND (1,0)		1
		0%	**0%**	**0%**		**100%**		
Exigences de Disponibilié (AR)	Exigences de Disponibilié (AR)	L(0,5)	M (1,0)	H(1,51)		ND (1,0)		1
		0%	**0%**	**0%**		**100%**		

FIGURE 4.18 – Métriques environnementaux pour Modbus/RTU de l'architecture (1)

Fuzzy ICVSS = AV{PM :{100%W} & AL : {30%Ph ;70%L}}/AC{SC :100}
%S&ATC :{100%L}}/Au :{100%N}/C :{100%N}
/I :{100%C}/A :{100%C}/SS :{100%N}/E :{100%ND}/
RL :{100%ND}/RC :{100%ND}/CDP{FI :{100%LoV}&SI :{100%H}
/TD :{100%H}/CR :{100%ND}/IR :{100%ND}/AR :{100%ND}
=8.15.

Nous remarquons qu'il y a changement de valeurs au niveau la métrique (AV) qui passe de 0.33 à 0.57 (voir les tableaux 4.13 et 4.16). Cela dû à la pondération engendrée par les fonctions d'appartenance (voir l'équation 4.6).

Dans un deuxième temps, dans cette nouvelle architecture, l'IHM est connectée à Internet. Nous partons sur un principe que plus l'installation est connectée au monde extérieur (Internet par exemple plus le risque augmente). Dans notre système score nous devons ressentir cette augmentation du risque à travers la sous-métrique couche d'accès (AL). En effet, cette augmentation de risque n'est pas quantifiable dans le cas du CVSS classique. Par exemple, dans le cas de la version CVSS, le vecteur d'accès métrique est égal à celui du réseau local dans les deux cas de vulnérabilité en Modbus/RTU ou Modbus/TCP. À l'inverse, dans le cas de la version ICVSS floue, nous savons que cette architecture est plus ouverte à l'extérieur, car il y a un seul pare-feu contre trois dans le premier cas, ce qui rend les vulnérabilités de Modbus/RTU et Modbus/TCP plus accessibles aux attaques. Par conséquent, nous avons dû modifier la valeur métrique de Modbus/RTU ou Modbus/TCP par rapport le premier cas de l'architecture (1), par exemple : 50 % physique et 50 % local pour Modbus/RTU et 90 % local et 10 % réseau pour le Modbus/TCP. Nous rappelons que le choix des valeurs pondérations (les fonctions d'appartenance) doit être fait par un expert. Cela est l'inconvénient major de cette méthodologie. Mais, par contre méthodologie donne plus de flexibilité à l'expert pour faire son choix, car il n'est pas limité un nombre binaire de choix .

Vulnérabilité de Modbus/RTU par rapport à l'architecture (2) :

Les figures 4.19, 4.20, 4.21 illustrent le choix des métriques de bases, temporelles, environnementales qui permet d'avoir le score de ICVSS floue de l'architecture (2).

Critères	Sous-critères	Notation					Quantification
Groupe d'exploitabilité							
Vecteur d'accès (AV)	**Physical Media (PM)**	Phy (0,2)	W (0,395)	WL (1,0)			0,29
		0%	**100%**	**0%**			
	Couche d'accès (AL) :	P (0,2)	L (0,395)	N (1,0)			
		50%	**50%**	**0%**			
Complexité d'accès (AC)	**Complexité d'attaque (ATC)**	H (0,35)	M (0.61)	L (0,71)			0,71
		0%	**0%**	**100%**			
	Complexié du System (SC)	S (0,35)	D (0,71)				
		100%	**0%**				
	Cryptographie (C)	N (0,71)	C (0,35)				
		100%	**0%**				
Authentication (Au)	**Authentication (Au)**	N (0,704)	S (0,56)	M (0,45)			0,704
		100%					
Groupe d'impact							
Impact de confidentialité (C)	**Impact de confidentialité (C)**	N (0)	P (0,275)	C (0,660)			0
		100%					
Impact d'intégrité (I)	**Impact d'intégrité (I)**	N (0)	P (0,275)	C (0,660)			0,66
				100%			
Impact de disponibilité (A)	**Impact de disponibilité (A)**	N (0)	P (0,275)	C (0,660)			0,66
				100%			
Système de SAF (SS)	**Système de SAF (SS)**	N (0,9)	SS (0,01)				0,9
		100%					

FIGURE 4.19 – Métriques de base pour Modbus/RTU de l'architecture (2)

Critères	Sous-critères	Notation					Quantification
Eploitabilité (E)	**Accès au système (SA)**	ND (1,0)	OS (1,0)	P (0,85)			(1,0)
		100%	**0%**	0%			
	Maturité (M)	H (1,0)	F (0,95)	PoC (0,9)	U (0,85)	ND (1,0)	0,9
		0%	**0%**	**0%**	**0%**	**100%**	
Niveau de correction (RL)	**Niveau de correction (RL)**	OF(0,87)	TF (0,9)	W(0,95)		U (1,0) / ND (1,0)	1
		0%	**0%**	**0%**		**0%** / **100%**	
Niveau de confiance (RC)	**Niveau de confiance (RC)**	UC(0,9)	UR (0,95)	C(0,95)		ND (1,0)	1
		0%	**0%**	**0%**		**100%**	

FIGURE 4.20 – Métriques temporelles Modbus/RTU de l'architecture (2)

Critères	Sous-critères	Notation					Quantification
Dommage collatéral potentiel (CDP)	**Impact fonctionnel (FI)**	LoV (0,5)	LoC (0,3)	Dos (0,4)			0,5
		100%					
	Impact de sûreté (SI)	N (0,0)	L (0,1)	LM (0,3)	MH (0,4)	H (0,5)	0,5
		0%	**0%**	**0%**	**0%**	**100%**	
Nombre de cibles impactée (TD)	**Nombre de cibles impactée (TD)**	N(0,0)	L (0,25)	M(0,75)		H (1,0) / ND (1,0)	1
						X	
Exigences de Confidentialité (RC)	**Exigences de Confidentialité (CR)**	L(0,5)	M (1,0)	H(1,51)		ND (1,0)	1
						100%	
Exigences d'Intégrité (IR)	**Exigences d'Intégrité (IR)**	L(0,5)	M (1,0)	H(1,51)		ND (1,0)	1
						100%	
Exigences de Disponibilié (AR)	**Exigences de Disponibilié (AR)**	L(0,5)	M (1,0)	H(1,51)		ND (1,0)	1
		0%	**0%**	**0%**		**100%**	

FIGURE 4.21 – Métriques environnementaux pour Modbus/RTU de l'architecture (2)

Fuzzy ICVSS =
AV{PM :{100%W} & AL : {50%Ph;50%L}}/
AC{SC :100%S&ATC :{100%L}/Au :{100%N}
/C :{100%N}/I :{100%C}/A :{100%C}/SS :{100%N}/
E :{100%ND}/RL :{100%ND}/RC :{100%ND}/
CDP{FI :{100%LoV}&SI :{100%H}/TD :{100%H}/CR :{100%ND}/
IR :{100%ND}/AR :{100%ND}= 8.0 .

Vulnérabilité de Modbus/TCP par rapport à l'architecture (2) :

Les figures 4.19, 4.20, 4.21 illustrent le choix des métriques de bases, temporelles, environnementales qui permet d'avoir le score de ICVSS floue de l'architecture (2).

Critères	Sous-critères	Notation					Quantification
Groupe d'exploitabilité							
Vecteur d'accès (AV)	Physical Media (PM)	Phy (0,2)	W (0,395)	WL (1,0)			0,93
		0%	**100%**	**0%**			
	Couche d'accès (AL) :	P (0,2)	L (0,395)	N (1,0)			
		0%	**10%**	**90%**			
Complexité d'accès (AC)	Complexité d'attaque (ATC)	H (0,35)	M (0.61)	L (0,71)			0,71
		0%	**0%**	**100%**			
	Complexié du System (SC)	S (0,35)	D (0,71)				
		100%	**0%**				
	Cryptographie (C)	N (0,71)	C (0,35)				
		100%	**0%**				
Authentication (Au)	Authentication (Au)	N (0,704)	S (0,56)	M (0,45)			0,704
		100%					
Groupe d'impact							
Impact de confidentialité (C)	Impact de confidentialité (C)	N (0)	P (0,275)	C (0,660)			0
		100%					
Impact d'intégrité (I)	Impact d'intégrité (I)	N (0)	P (0,275)	C (0,660)			0,66
				100%			
Impact de disponibilité (A)	Impact de disponibilité (A)	N (0)	P (0,275)	C (0,660)			0,66
				100%			
Système de SAF (SS)	Système de SAF (SS)	N (0,9)	SS (0,01)				0,9
		100%					

FIGURE 4.22 – Métriques de base pour Modbus/TCP de l'architecture (2)

Critères	Sous-critères	Notation						Quantification
Eploitabilité (E)	Accès au système (SA)	ND (1,0)	OS (0,85)	P (1,0)				(1,0)
		100%	**0%**	**0%**				
	Maturité (M)	H (1,0)	F (0,95)	PoC (0,9)	U (0,85)	ND (1,0)		0,9
		0%	**0%**	**0%**	**0%**	**100%**		
Niveau de correction (RL)	Niveau de correction (RL)	OF(0,87)	TF (0,9)	W(0,95)		U (1,0)	ND (1,0)	1
							100%	
Niveau de confiance (RC)	Niveau de confiance (RC)	UC(0,9)	UR (0,95)	C(0,95)		ND (1,0)		1
		0%	**0%**	**0%**		**100%**		

FIGURE 4.23 – Métriques temporelles pour Modbus/TCP de l'architecture (2)

Critères	Sous-critères	Notation						Quantification
Dommage collatéral potentiel (CDP)	Impact fonctionnel (FI)	LoV (0,5)	LoC (0,3)	Dos (0,4)				0,5
		100%						
	Impact de sûreté (SI)	N (0,0)	L (0,1)	LM (0,3)	MH (0,4)	H (0,5)		0,5
		0%	**0%**	**0%**	**0%**	**100%**		
Nombre de cibles impactée (TD)	Nombre de cibles impactée (TD)	N(0,0)	L (0,25)	M(0,75)		H (1,0)	ND (1,0)	1
							X	
Exigences de Confidentialité (RC)	Exigences de Confidentialité (CR)	L(0,5)	M (1,0)	H(1,51)		ND (1,0)		1
						100%		
Exigences d'Intégrité (IR)	Exigences d'Intégrité (IR)	L(0,5)	M (1,0)	H(1,51)		ND (1,0)		1
						100%		
Exigences de Disponibilié (AR)	Exigences de Disponibilié (AR)	L(0,5)	M (1,0)	H(1,51)		ND (1,0)		1
		0%	**0%**	**0%**		**100%**		

FIGURE 4.24 – Métriques environnementaux pour Modbus/TCP de l'architecture (2)

Fuzzy ICVSS = AV{PM :{100%W} & AL : {70%Ph;30%N}/
AC{SC :100%S&ATC :{100%L}/Au :{100%N}
/C :{100%N}/I :{100%C}/A :{100%C}/
SS :{100%N}/E :{100%ND}/RL :{100%ND}/RC :{100%ND}/
CDP{FI :{100%LoV}&SI :{100%H}/
TD :{100%H}/CR :{100%ND}/IR :{100%ND}/AR :{100%ND}= 9.5.

Nous remarquons que système de notation ICVSS flou permet de donner plus de flexibilité à l'expert pour choisir des valeurs plus adaptées à son installation c-.à.d l'évaluateur peut avoir des valeurs proportionnelles (l'évaluation qualitative/quantitative) au lieu d'avoir des valeurs binaires grâce aux fonctions d'appartenance. Par exemple, dans ce cas particulier nous pouvons classer les différents protocoles selon leur niveau dans le modèle CIM. Cela permet d'adapter le score en fonction de la proximité de la vulnérabilité au monde extérieur (connectivité au monde extérieur) . Tandis que la version 2 de CVSS

donne à toutes les vulnérabilités du réseau local la même valeur malgré le changement d'architecture dans le second cas.

En revanche, le changement au niveau du score final n'est pas significatif , lorsqu'on passe du score de 7.9 à 8.0 pour l'architecture (1) et de 8.15 à 9.5 pour l'architecture (2) cela est dû au fait que nous agissons sur une seule métrique. Mais, nous avons pu constater le changement des valeurs de la métrique couche d'accès (AL). En conséquence, si nous modifions plusieurs métriques nous allons noter un grand changement de score final. Enfin, l'inconvénient major de cette méthode est sa subjectivité, car elle dépend beaucoup plus des connaissances et l'expérience de l'évaluateur.

4.3.2 Conclusion

Dans ce travail, une nouveau système de notation de la vulnérabilité dans les ICSs appelée Fuzzy ICVSS est introduite. Utilisation de l'ICVSS flou est non seulement permet d' offrir des informations plus utiles sur la vulnérabilité (un vecteur qualitatif, une valeur quantitative), mais aussi sa capacité de modéliser les incertitudes liées à la prise de la décision par l'expert. Dans le chapitre suivant, nous allons travailler plus sur la démarche globale qui conduit à une intégration de sécurité-innocuité (SAF) avec la sécurité-immunité (SEC) en utilisant toujours système de notation ICVSS.

Chapitre 5

Méthode d'intégration des risques de sécurité-innocuité et la sécurité-immunité

Contents

5.1 Introduction

Dans ce chapitre, une nouvelle approche de co-analyse et de co-évaluation de la SAF et de la SEC appelée l'AMDVEC & ER (Analyse des Modes de Défaillance et de Vulnérabilité, de leurs Effets et de leur Criticité & Évaluation des Risques) est proposée. En fait, l'AMDVEC & ER est un cas d'utilisation qui montre l'efficacité de notre méthodologie pour laquelle nous avons pu réutiliser la méthode AMDEC et la méthode ICVSS, connues comme des techniques largement utilisées dans le domaine de la sécurité-innocuité (SAF) et de la sécurité immunité (SEC) respectivement. Cela permet d'effectuer une co-analyse des dangers et des menaces à la fois pour évaluer leurs risques mutuels. De plus, la solution proposée est conforme aux normes IEC 60812 pour la SAF et IEC 62443 pour la SEC.

Nous présenterons dans un premier temps les principaux standards prenant en compte la sécurité innocuité et la sécurité immunité ainsi que certaines approches émergentes intégrant ces deux aspects. Puis, nous décrirons le concept de l'AMDVEC qui nous sert de référence pour l'analyse des éléments critiques en sécurité.

5.2 Normes de la SAF et la SEC dans le domaine des ICSs

Nous allons donné dans cette section les principaux standards de la sécurité-innocuité et la sécurité-immunité ainsi que les standards communs utilisés dans l'industrie.

5.2.1 Standards de la sécurité innocuité (SAF)

Nous évoquons les standards génériques IEC 61508 de la SAF, qui sont divisés en plusieurs branches selon le domaine (e.g., IEC 61513 pour l'industrie du nucléaire, IEC 61511 pour l'industrie du procédé et ISO 26262 pour industrie de transport). Ensuite, nous abordons le standard générique CEI 60812 :

- **IEC 61508 :** C'est un standard pour SAF et tous les systèmes électriques/électroniques/électroniques programmables (ISO, 2010). Le standard couvre tous les aspects importants concernant l'utilisation d'équipement électrique ou électronique et sa relation avec la SAF. La stratégie de la norme IEC 61508 est de dériver les exigences de la SAF d'une analyse des dangers et des risques et de concevoir le système de manière à répondre à ces exigences, en tenant compte de toutes les causes possibles de défaillance (Soerby, 2003). La norme prend en compte toutes les phases d'un cycle de vie de la SAF, en accompagnant le cycle de vie du produit tout au long de sa conception initiale, sa conception détaillée, sa réalisation, son exploitation, sa maintenance et son démantèlement. La figure 5.1 illustre le processus global de sécurité associé à cette norme. La norme CEI 61508 spécifie un ensemble de méthodes, mesures et procédures qui doivent être respectées pour revendiquer un certain niveau d'intégrité de sûreté (Safety Integrity Level SIL). La norme ne traite pas directement des exigences en matière de sécurité, mais reconnaît que si une action malveillante ou non autorisée est identifiée dans l'analyse des dangers, une analyse des menaces à la sécurité doit être effectuée.

- **Norme CEI 60812 :** C'est un standard qui explique l'Analyse des Modes de Défaillance, de leurs Effets et de leur Criticité (AMDEC). L'objectif de l'AMDEC est de déterminer comment les composants ou les processus, ne pourraient pas accomplir leur fonction nominale, et ensuite, comment pouvoir identifier les mesures correctives nécessaires. La norme est applicable aux matériels, aux logiciels, aux pro-

cessus, y compris les actions humaines, et à leurs interfaces, quelle que soit leur combinaison. Dans la section 5.3, nous allons voir plus de détails son utilisation.

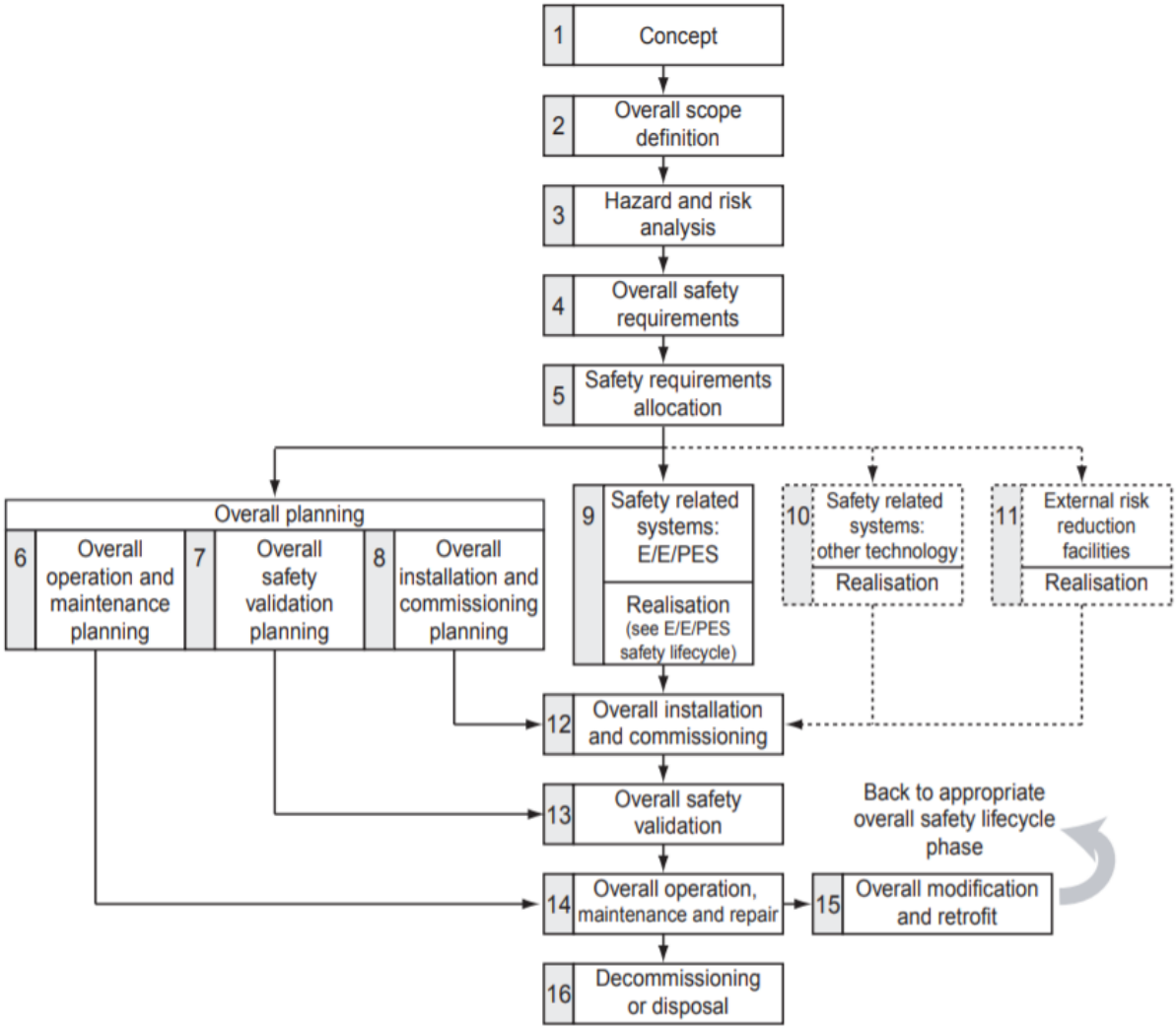


FIGURE 5.1 – Cycle de vie global de la sécurité-innocuité de la CEI 61508 (Brun et al., 2013) (Lundteigen, 2009).

5.2.2 Standards de la sécurité-immunité (SEC)

La sécurité-immunité des systèmes d'information traditionnels est généralement basée sur le principe de la C-I-A (Confidentiality, Integrity, Availability) par ordre de priorité. Cependant, pour les systèmes de contrôle industriel (ICSs) la priorité est généralement inversée en fonction des spécificités du système considéré (Rekik et al., 2018). Par exemple, dans les systèmes ferroviaires, le plus important est la circulation des trains. Cela signifie que la préoccupation de SEC est tout d'abord l'Intégrité (I), puis la disponibilité (A) et enfin la confidentialité (C). En effet, l'absence d'intégrité entraîne des impacts catastrophiques comme des collisions des trains, alors que l'absence de disponibilité provoque l'arrêt du système ferroviaire. La perte de confidentialité est une menace moins immédiate, mais elle pourrait entraîner la fuite d'informations opérationnelles sensibles. De plus, les normes et les méthodologies élaborées pour les systèmes informatiques traditionnels ne peuvent pas être appliquées directement. Cette question a retenu l'attention

non seulement des chercheurs, mais aussi des autorités publiques et des comités de normalisation au cours des dernières années.

Plusieurs normes de sécurité de l'information ont été proposées pour traiter les questions de sécurité dans le cas particulier de l'ICS, tels que ISO/IEC 27000 (ISO, 2016), ISO/IEC 15408 Common Criteria (ISO, 2009), ISA/IEC 62443 (ISA, 2016b), EN 50159 (for Electrotechnical, 2010), RFC 2196 (Fraser, 2003), ETSI TS 102 165 ((ETSI), 2007), des normes allemandes comme DIN VDE V 0831-102 (for Standardization (DIN), 2013) et DIN VDE V 0831-104 (for Standardization (DIN), 2015), normes américaines comme FIPS PUB 199 (Pub, 2004), FIPS PUB 200 (PUB, 2006) et NIST Special Publications (PS) comme PS 800-37 (Initiative et al., 2014), PS 800-53 rév. 4 (Force and Initiative, 2013), etc. Une étude approfondie sur les normes et directives de sécurité pour l'ICS est disponible dans (Knowles et al., 2015).
Nous présentons dans cette section certaines normes de sécurité parmi les plus connues pour la conception et l'évaluation de la sécurité-immunité.

Norme ISA/IEC 62443

De ces normes de sécurité, la norme ISA/IEC 62443 est parmi les plus importantes pour ICS. Le comité ISA99, qui est en charge de produire des spécifications, a fait de grands travaux pour rassembler de nombreuses normes et recommandations et ensuite créer un ensemble complet de documents uniformes et cohérents et largement applicables dans presque tous les secteurs industriels. Ceci est le fait que ces spécifications ont été reconnues à l'échelle mondiale grâce à l'adoption par la CEI de la série ISA/IEC 62443 qui constitue un ensemble unique et définitif de normes internationales pour la cybersécurité de l'ICS.

La norme ISA/IEC-62443 (ISA, 2016a) propose des directives pour renforcer la sécurité électronique et contribuer à atténuer le risque de compromis d'informations confidentielles, de dégradation ou de défaillance de l'équipement (matériel et logiciel) des systèmes sous contrôle. De plus, la norme ISA/IEC-62443 permet de renforcer la disponibilité, l'intégrité et la confidentialité des composants ou des systèmes utilisés pour l'automatisation et le contrôle industriels.

Les composants de la série 62443 sont illustrées dans la figure 5.2. Les composantes sont classées en quatre groupes, correspondant à l'objectif principal et au destinataire.

1. **Groupe général :** groupe qui comprend des éléments concernant des aspects communs à toute la série.

    - **Norme 62443-1-1 : Terminologie et concepts :** présente les concepts et les modèles utilisés dans toute la série.Le public visé comprend toute personne qui souhaite se familiariser avec les concepts fondamentaux constituant la base de la série. La première édition de cette norme a été publiée en 2007.
    - **62443-1-2 : Glossaire principal :** est un rapport technique qui comporte un glossaire principal des termes et abréviations utilisés dans la série.
    - **Norme 62443-1-3 : Métriques de conformité de SEC du système :** présente une série de mesures quantitatives dérivées des exigences fondamentales, des exigences du système et des exigences connexes. Cet élément n'est disponible que sous forme de brouillon.

- **Norme 62443-1-4 : Cycle de vie de la sécurité et cas d'utilisation :** fournira une description plus détaillée du cycle de vie de la sécurité du ICS, ainsi le rapport montre plusieurs cas d'utilisation. Le travail sur ce rapport n'a pas encore commencé.

2. **Politiques et procédures :** Les composantes de ce groupe focalisent sur les politiques et procédures relatives à la sécurité du ICS.

   - **Norme 62443-2-1 : Exigences relatives à un système de gestion de la sécurité des ICSs :** définit ce qu'il faut faire pour mettre en œuvre un système efficace de gestion de la cybersécurité du ICS. Le public ciblé comprend les utilisateurs finaux et les propriétaires de biens qui ont la responsabilité de la conception et de la mise en œuvre d'un tel programme. La première édition de cette norme a été publiée en 2009 et le comité ISA99 est en train d'élaborer une deuxième édition mise à jour qui s'alignera mieux sur la série de normes ISO-27000 sur la cybersécurité des systèmes IT.
   - **Norme 62443-2-2** fournira des orientations spécifiques sur ce qui est nécessaire pour exploiter un système efficace de gestion de la cybersécurité du ICS. Le public visé comprend les utilisateurs finaux.
   - **Norme 62443-2-3** fournira des directives sur la gestion des mises à jour et des correctives pour ICS. Le public visé comprend toute personne qui a la responsabilité de la conception et de la mise en oeuvre de gestion des correctifs. Ce rapport a été approuvé et publié par l'ISA et la CEI en 2015.
   - **Norme 62443-2-4** établit les spécifications pour les fournisseurs du ICS. Le public principal contient les fournisseurs de solutions de systèmes de contrôle. Cette norme a été élaborée par le groupe de travail WG10 du comité technique TC65 de la CEI et sera officiellement adoptée par l'ISA dans le cadre de la série ISA-62443.

3. **Spécifications du système :** Les éléments du troisième groupe traitent des exigences au niveau du système.

   - **Norme 62443-3-1 :** décrit l'application de nombreuses technologies de sécurité sur un environnement du ICS. La deuxième édition a été publiée en 2007, et le comité ISA99 travaille actuellement sur la troisième édition.
   - **Norme 62443-3-2 :** traite l'évaluation des risques de sécurité et de la conception du système pour ICS. Cette norme s'adresse principalement aux propriétaires d'actifs ou aux utilisateurs finaux.
   - **Norme 62443-3-3 :** décrit les spécifications fondamentales en matière de sécurité des systèmes et les niveaux d'assurance de la sécurité. Cette norme a été publiée par l'ISA et la CEI en 2013.

4. **Exigences des composantes :** Le quatrième et dernier groupe comprennent des éléments qui proposent des informations sur les spécifications plus précises et détaillées associées au développement de produit.

   - **Norme 62443-4-1** décrit les spécifications dérivées applicables au développement des produits. Elle s'adresse principalement aux fournisseurs de solutions de systèmes de contrôle.

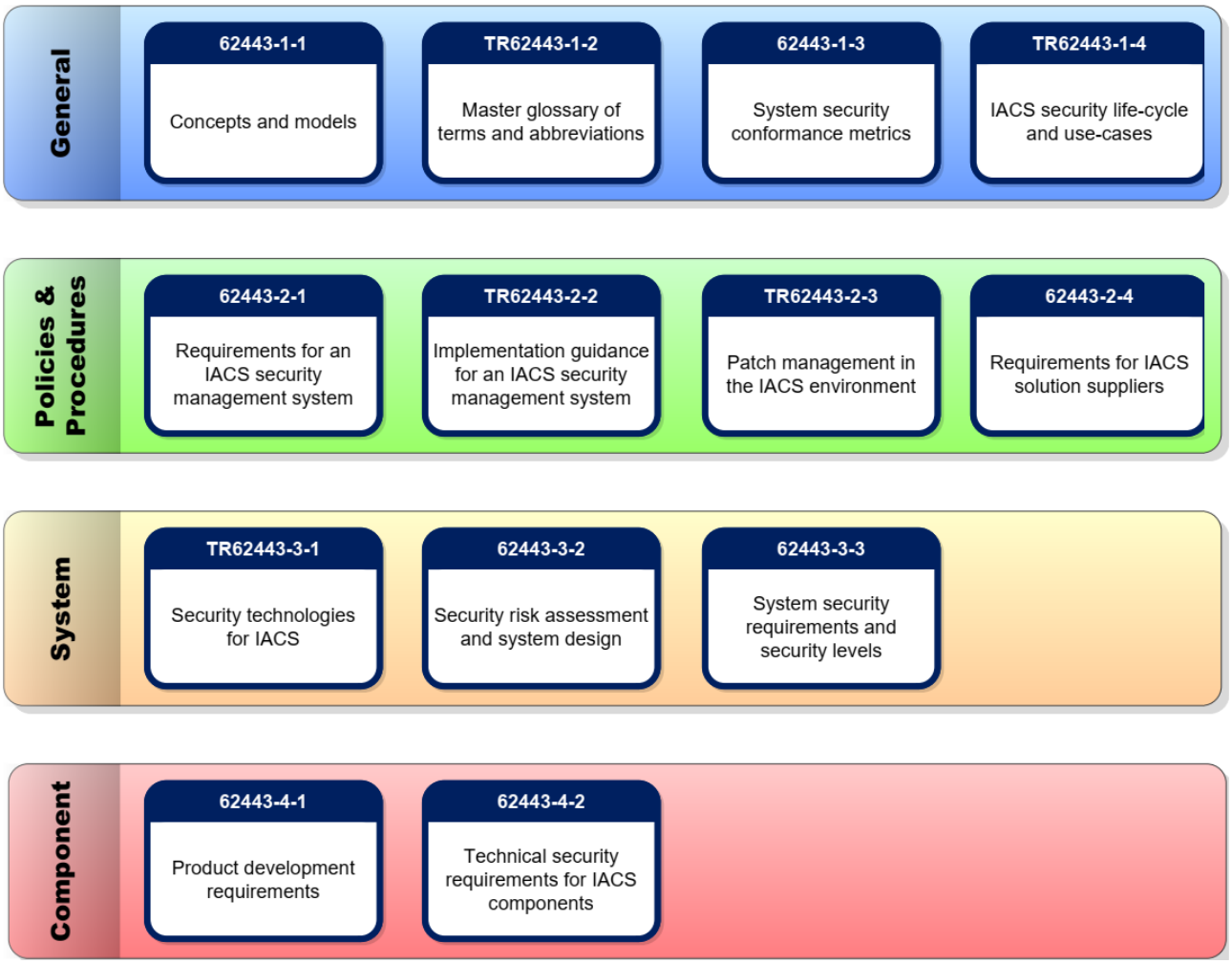


FIGURE 5.2 – Composantes de ISA/IEC 62443 (Niemann, 2017).

- **Norme 62443-4-2** contient des ensembles de spécifications dérivées qui fournissent les spécifications du système avec les sous-systèmes et les composants du système. Le public principal comporte les fournisseurs de solutions de systèmes de contrôle.

La méthode d'évaluation des risques de sécurité proposée par la norme ISA/IEC-62443 comporte 13 étapes, comme le montre la figure 5.3. L'identification du SuC (System Under Consideration) est la première étape de la méthodologie. Elle consiste en une phase de spécification fonctionnelle en conception qui vise à identifier les équipements physiques et informatiques du système. Les étapes 2 et 3 évaluent les menaces et les vulnérabilités. Une fois que les menaces potentielles et les vulnérabilités du système sont identifiées, leurs impacts directs et leurs conséquences sur l'ensemble du système doivent être analysés à l'étape 4. Ensuite, la probabilité de chaque menace identifiée doit être déterminée à l'étape 5. L'étape 6 consiste à calculer le risque non atténué dans une matrice de risques en utilisant les taux de probabilité et l'impact . À l'étape 7, le risque créé par chaque menace identifiée doit être évalué en fonction de la matrice des risques. À l'étape 8, il faut déterminer les contre-mesures à adopter pour limiter les risques jugés intolérables. Ensuite, les probabilités et les risques devraient être réévalués afin de mesurer l'efficacité des mesures proposées. Si certains risques sont encore jugés inacceptables, il faudrait alors envisager un ensemble de contre-mesures supplémentaires, puis reprendre les étapes 9

et 10 jusqu'à ce que tous les risques deviennent tolérables. Au final (étape 12), l'évaluation des risques de sécurité devrait être finalisée par une phase de documentation.

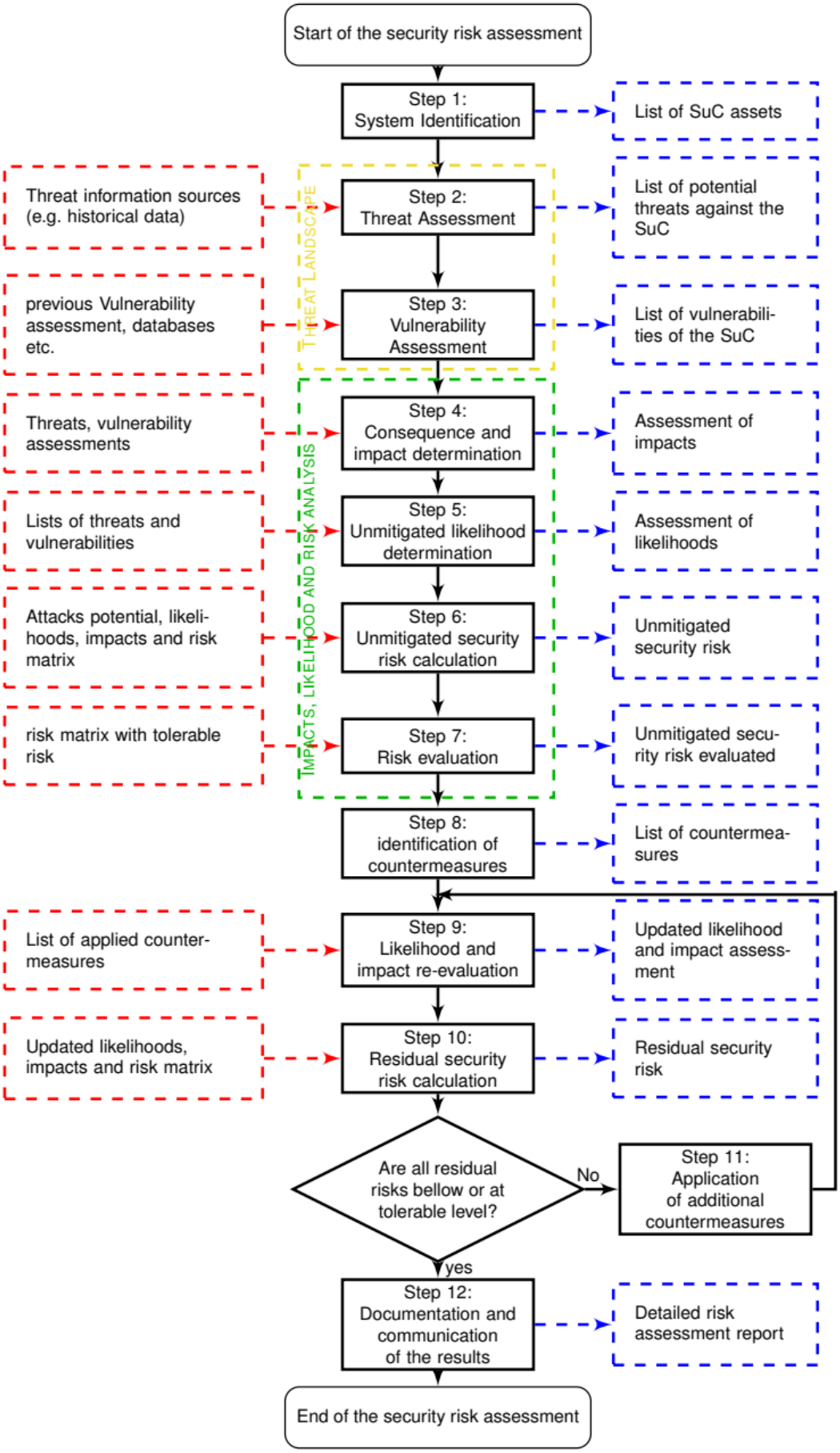


FIGURE 5.3 – Méthode d'évaluation des risques de sécurité ISA/IEC-62443 (Rekik et al., 2018).

Le standard propose aussi des orientations pour renforcer la connectivité des systèmes de sécurité-innocuité instrumentés (Safety Instrumented System SIS), la partie 2-4 de la norme précise des mesures de sécurité telles que :

- Garantir l'intégrité des communications par le câblage ou la séparation logique des communications liées à la sûreté des autres communications de contrôle du réseau ;
- Isoler le SIS des connexions de la couche 3 (couche réseau) ;
- Empêcher la connexion de données entre le système de contrôle distribué et le SIS ;
- Restreindre les fonctions autorisées du poste de travail technique (utilisé à des fins de maintenance) et son interaction avec le SIS.

Norme CEI 62645

Elle s'intitule *Centrales nucléaires - Systèmes d'instrumentation et de contrôle - Exigences pour les programmes de sécurité-immunité*. Publiée en 2014, cette norme a été déclinée pour le nucléaire. Elle fournira des conseils pour l'élaboration et la gestion de programmes efficaces de sécurité informatique pour les systèmes d'instrumentation et de contrôle (I&C) dans les centrales nucléaires. La norme définit une approche graduelle de la cyber-sécurité en attribuant un niveau de sécurité à chaque système I&C en fonction de l'impact d'une attaque sur la sûreté et la performance. Les systèmes d'I&C sont regroupés en zones de sécurité (Pietre-Cambacedes et al., 2013; ISO, 2012).

Autres normes

Les normes de sécurité suivantes concernent les systèmes IT en général et ne tiennent donc pas en compte les contraintes des ICSs. En dépit de cela, ces normes sont utilisées par les ingénieurs de sécurité de l'informatique industrielle.

- **Critères communs / CEI 15408 :** est une norme internationale qui établit les concepts et les principes généraux de l'évaluation de la sécurité des IT et précise le modèle général d'évaluation. Il définit des niveaux d'assurance appliqués à la gestion de la sécurité et des critères en relation avec chaque niveau d'assurance.
- **Norme ISO/IEC 27001 :** est une norme internationale pour les systèmes de gestion de la sécurité de l'information (Information Security Management Systems ISMS)(ISO, 2013). Il fournit un modèle de cycle de vie pour l'établissement, la mise en œuvre, l'exploitation, la surveillance, l'examen, le maintien et l'amélioration d'une organisation. Ce modèle de cycle de vie, appelé " Planifier, réaliser, vérifier, agir " (Plan-Do-Check-Act PDCA) est illustré dans la figure 5.4 montre les principales actions du processus du ISMS qui considère les exigences de sécurité de l'information comme des entrées et des résultats de sécurité de l'information qui répondent à ces exigences comme des sorties.

  Cette norme est le premier document d'une série de normes dont ISO/IEC 27005 (iso,), qui traitent spécifiquement de la gestion des risques liés à la sécurité de l'information. Elle fournit un processus structuré, systématique et rigoureux pour toute la démarche en partant de l'analyse des risques jusqu'à l'élaboration du plan de traitement des risques. Ce processus est illustré à la figure 5.5. Malheureusement, ces normes ne mentionnent pas la sécurité-innocuité du système.

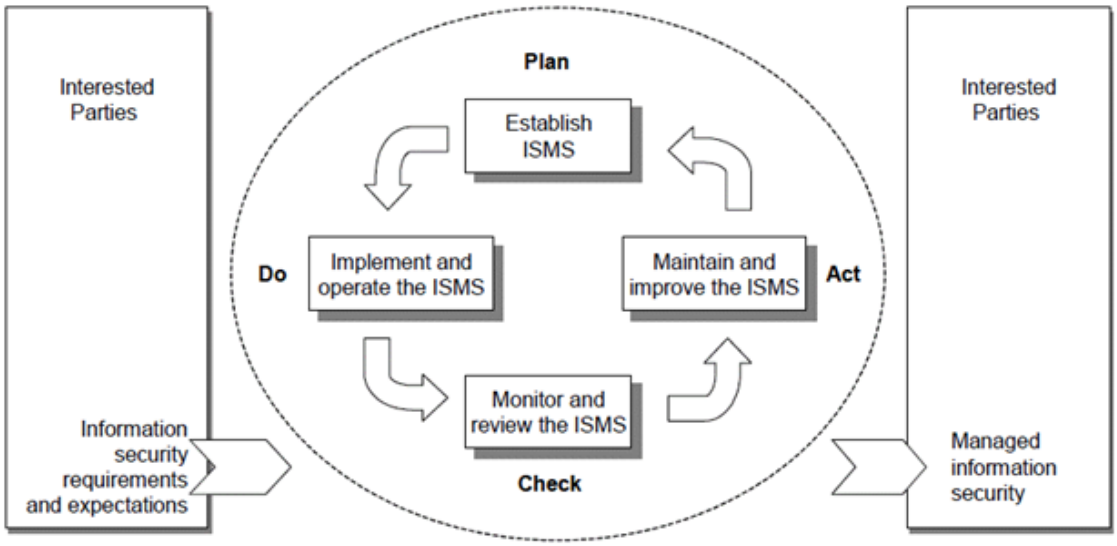


FIGURE 5.4 – Modèle PDCA appliqué aux processus du ISMS (Raspotnig et al., 2012).

- **EBIOS :** La méthodologie *EBIOS* a été formalisée et adoptée par l'Agence Nationale de Sécurité des Systèmes d'Information (ANSSI). Cette méthodologie a été mise à jour afin d'être conforme à la norme ISO/CEI 27005 et propose un moyen d'évaluer les risques. Elle consiste à identifier les équipements à protéger et à effectuer une analyse des risques pour chaque équipement en identifiant les scénarii d'attaque possibles, et en proposant des mesures de sécurité-immunité.

5.2.3 Initiatives relatives aux normes de la sécurité-innocuité et de la sécurité-immunité

Dans cette section, nous décrivons certaines initiatives de normalisation émergentes qui tiennent compte de la coordination de la sécurité-innocuité et de la sécurité-immunité des ICSs.

- **ISA-99 WG7 :** est un groupe de travail établi au sein du comité de l'ISA-99 qui traite des problématiques liées à la sécurité-innocuité et à la sécurité-immunité des systèmes d'automatisation, de contrôle et de commande industriels. Le but de ce groupe de travail est de prolonger le cycle de vie actuel de la sûreté afin d'examiner les aspects de la cybersécurité à différentes étapes du cycle de vie des procédés industriels (c'est-à-dire la conception, la mise en œuvre, la mise en service et l'entretien) afin de garantir la fiabilité et la sûreté du système ou du processus.

- **IEC TC65 AHG1 :** est un groupe de travail ad-hoc de la CEI, qui a l'intention de développer un "cadre de travail pour coordonner la sécurité-innocuité et la sécurité-immunité". Il est rattaché au même comité technique que celui qui élabore les normes CEI 61508 et CEI 62443, ce qui crée une occasion prometteuse pour les experts de la sécurité-innocuité et de la cybersécurité qui participent à leur élaboration de se réunir et d'élaborer effectivement le cadre visé.

- **CEI 62859 :** est une future norme dérivée de la norme CEI 62645 qui s'intitule "Centrales nucléaires - Systèmes d'instrumentation et de contrôle - Exigences pour coordonner la sûreté et la cybersécurité" (Nuclear power plants – instrumentation

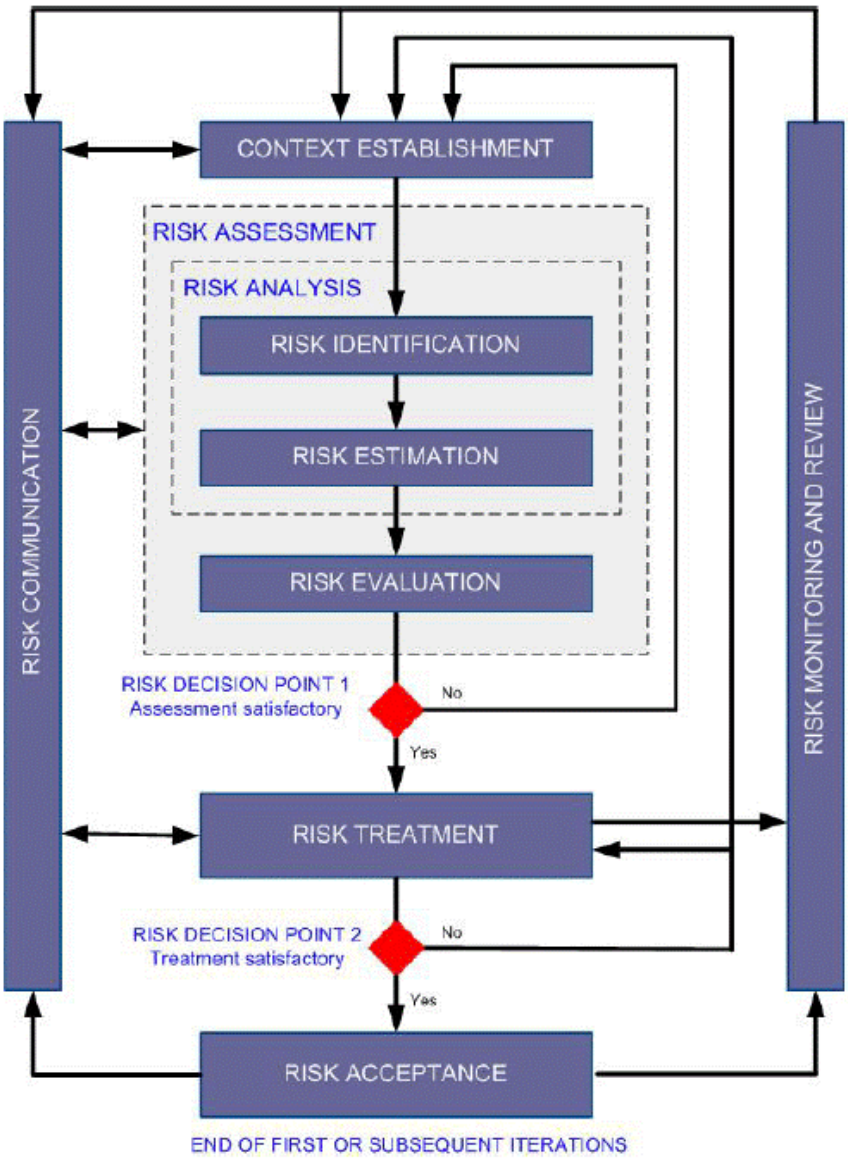


FIGURE 5.5 – Processus de gestion des risques pour la sécurité de l'information de la norme ISO/CEI 27005(iso,).

and control systems – requirements for coordinating safety and cyber security). Elle vise à établir des exigences et des recommandations qui optimisent et coordonnent la conception et les efforts opérationnels en matière de sûreté et de cybersécurité ; à améliorer l'identification et la résolution des conflits potentiels entre ces aspects tout au long du cycle de vie du système I&C ; à aider ; à identifier et à exploiter les synergies potentielles entre sécurité innocuité et sécurité immunité (Pietre-Cambacedes et al., 2013). Bien que cette norme concerne le domaine nucléaire, de nombreux autres secteurs industriels ont manifesté un intérêt concret pour la coordination entre sécurité innocuité et cybersécurité. On peut citer, par exemple, les initiatives dans l'industrie aérospatiale à travers le projet SESAR (Bieber et al., 2012) et dans la gestion du contrôle du trafic aérien (Raspotnig et al., 2012).

- **DO-326/ED-202**, elle est publiée pour la première fois en 2010 et révisée en 2014 ; Il s'agit d'une norme dans le domaine de l'avionique intitulée "Spécification du

processus de sécurité de navigabilité". Elle vise à compléter les lignes directrices actuelles en matière de certification aéronautique afin d'établir un lien entre les menaces à la sécurité de l'information et la sécurité-innocuité des aéronefs. Les versions successives de ce document ont abordé le positionnement du processus d'évaluation de la sécurité-immunité par rapport à la phase de développement du système et au processus d'évaluation de la sécurité-innocuité de différentes façons. Premièrement, dans sa première version publiée (2010), les activités de sécurité ont été intégrées dans les activités de sécurité avec un échange bidirectionnel et avec la phase de développement du système. Au cours d'un projet de révision en 2013 (DO-326A Draft), les activités de sécurité-innocuité ont été découplées des activités de sécurité-immunité toutefois avec des boucles mutuelles entre les deux. Finalement, à la révision publiée en 2014 (DO-326A), les activités de sécurité-innocuité ont encore été éloignées des activités de sécurité-immunité avec un seul bouclage de la sécurité-innocuité à la sécurité-immunité.

Nous avons vu qu'il existait des normes relatives à la sécurité innocuité, d'autres construites pour la sécurité immunité, et des travaux en cours intégrant les deux aspects.

À partir de ces informations, dans la suite, nous proposons une nouvelle approche de co-analyse et de co-évaluation de la SAF et de SEC appelée AMDVEC & ER (Analyse des Modes de Défaillance et de Vulnérabilité, de leurs Effets et de leur Criticité & Évaluation des Risques). Elle est construite en partant de l'analyse des risques (AMDEC) proposée dans la norme IEC 60812, que nous avons adapté à l'étude des menaces.

La méthodologie globale d'évaluation est structurée en suivant la démarche de la norme IEC 62442.

5.3 Analyse des modes de défaillance, de leurs effets et de leur criticité

5.3.1 Concept de l'AMDEC

L'approche de base pour réaliser une AMDEC est décrite dans la norme CEI 60812. Sur la base de cette description, l'organigramme (voir la figure 5.6) résume les étapes importantes. Le système est divisé en composants, et les modes de défaillance de chaque composant sont identifiés. Pour chaque mode de défaillance, les effets, la gravité, les conséquences finales sur le système et les causes potentiels sont examinés. Ensuite, la fréquence ou la probabilité des modes de défaillance sont estimées.

La chaîne de cause-effet analysée avec une AMDEC est présentée à la figure 5.7. Chaque mode de défaillance a une cause, et chaque effet de défaillance est associé à un mode de défaillance. Un effet de défaillance conduit à un scénario non souhaité. La gravité décrit l'importance du scénario. La fréquence est liée à la cause et à l'effet de la défaillance. Elle décrit la probabilité de l'événement. Les étapes de la méthode selon la norme IEC 60812 sont :

- **Cause de la défaillance :** pourquoi la composante est-elle tombée en panne ?
- **Mode de défaillance :** la manière dont la composante est défaillante.
- **Effet de panne :** conséquence d'un mode de défaillance du fonctionnement, de la fonction ou de l'état de la composante.

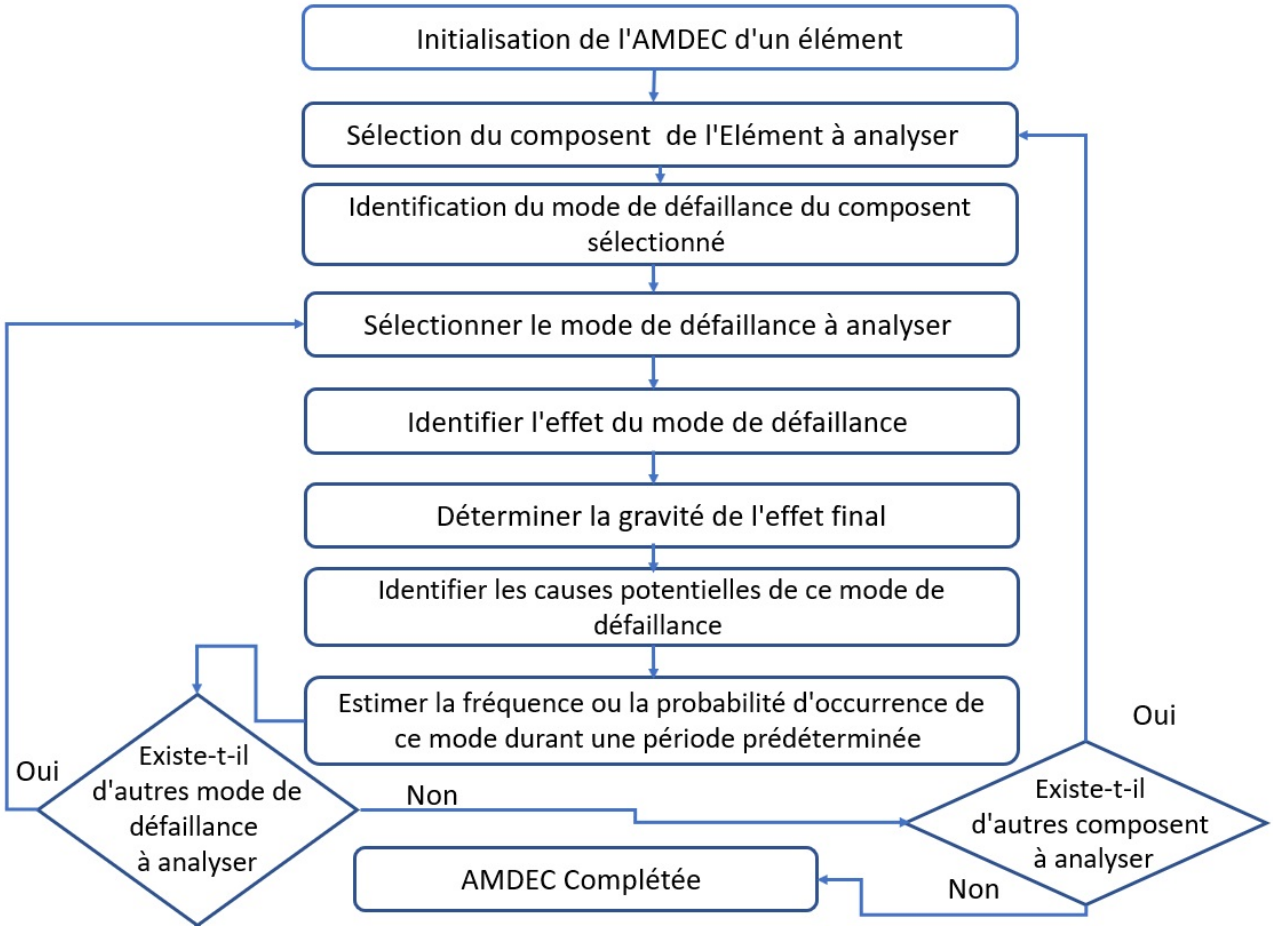


FIGURE 5.6 – AMDEC - diagramme d'analyse (Schmittner et al., 2014a)

- **Gravité de la défaillance :** importance de l'effet du mode de défaillance sur le fonctionnement de la composante.
- **Criticité des défaillances :** combinaison de la gravité d'un effet et de la fréquence de son apparition ou d'autres attributs d'une défaillance comme mesure de la nécessité d'y remédier et de l'atténuer.

5.3.2 Analyse des menaces

À partir de l'AMDEC, (Schmittner et al., 2014a) proposent une chaîne de cause-effet pour la sécurité-immunité dans l'analyse. Ils divisent les événements critiques pour la sécurité en étapes similaires à l'AMDEC. Les éléments suggérés d'une chaîne de cause-effet en matière de SEC sont les suivants :

1. **Vulnérabilités :** La condition préalable essentielle à la réussite d'une attaque sur un système est la vulnérabilité. Dans le cas de l'AMDEC, la vulnérabilité est comparable à une cause de défaillance (pour plus de détails sur les vulnérabilité, voir le chapitre 1).

2. **Agent de menace :** Les agents de menace représentent l'élément actif qui tente d'exploiter la vulnérabilité. Les exemples d'agents de menace possibles sont les pirates, les criminels informatiques, les terroristes, l'espionnage industriel ou les initiés (pour plus de détails sur l'agent de menace, voir le chapitre 1).

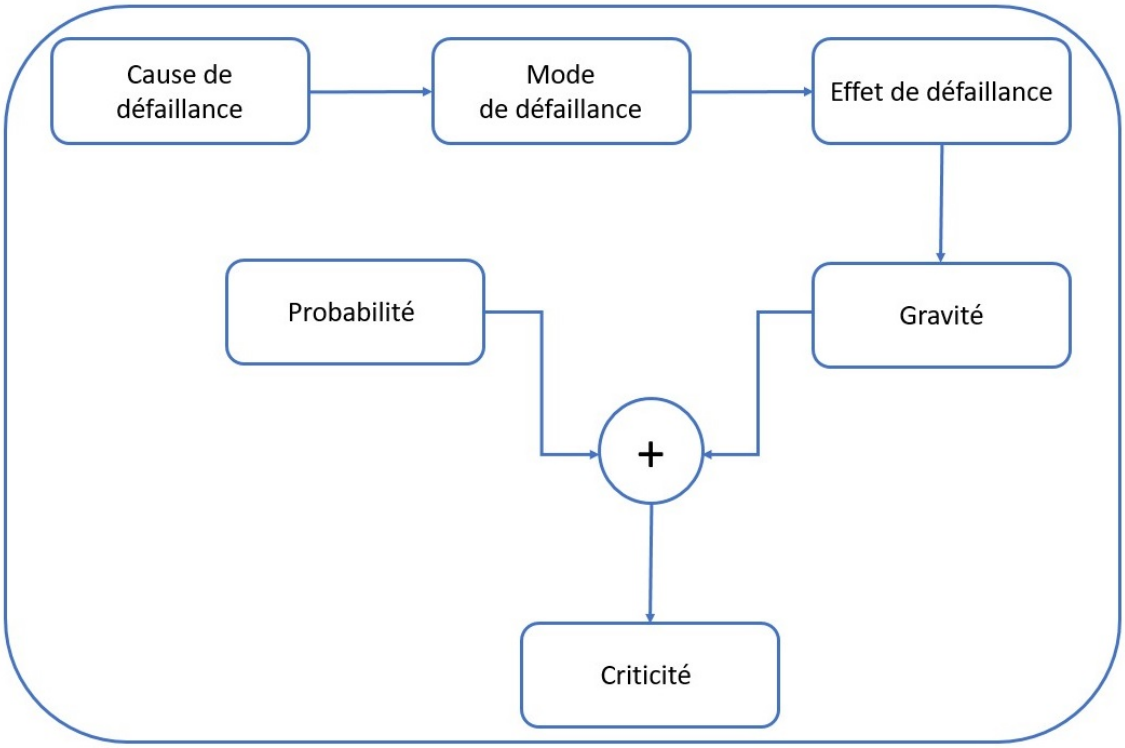


FIGURE 5.7 – AMDEC-Chaîne de cause-effet (Schmittner et al., 2014a)

3. **Mode de menace :** Il est similaire au mode de défaillance de la SAF et décrit la manière dont la SEC échoue. Le mode de menace représente la manière dont les vulnérabilités sont exploitées. Les vulnérabilités peuvent être exploitées de diverses manières, chacune ayant des effets et des conditions préalables différents. Les modes de menace potentiels dépendent du système et des capacités de l'agent de menace. Les modes de menace peuvent être simples comme le brouillage d'une connexion ou des opérations complexes comme l'exploitation d'une vulnérabilité d'injection, qui nécessite l'accès au système d'entrée et l'envoi d'une trame d'entrée formulé avec précision. En général, cela peut être mis en relation avec une violation d'un attribut de SEC. Selon le système, chaque mode de menace peut affecter la fiabilité (fiabilité, disponibilité, maintenabilité et la SAF) ou non.

4. **Effet de menace :** Toute comme l'effet de défaillance (SAF), l'effet de menace (SEC) est la conséquence en termes de fonctionnement, ou d'état. Alors que le mode de menace caractérise l'attribut de sécurité violé, l'effet de menace décrit l'attribut de qualité du système violé (Laprie, 1985). Les attributs violés ne sont pas limités à la sécurité. Tous les attributs de sûreté de fonctionnement peuvent être affectés. L'attribut qui est effectivement violé dans un cas particulier dépend du système, de son environnement et de son état de fonctionnement.

5. **Probabilité d'attaque :** Afin d'évaluer la criticité d'une attaque de sécurité, la gravité et la probabilité de l'attaque doivent être évaluées. Si la gravité peut être évaluée avec l'aide d'experts du domaine, la probabilité est définie différemment pour la SAF et la SEC.
   Dans le cas de la SAF, un événement défaillance d'une composante est décrit par la probabilité de défaillance du matériel ou du logiciel. Par contre, dans le cas de la SEC, un événement d'attaque sur une composante est décrit par la probabilité

que l'agent de menace accomplisse l'effet de la menace. Cela dépend non seulement de l'agent de menace lui-même, mais aussi des propriétés du système et de son environnement. Si un système n'est pas connecté à un réseau public et situé dans une zone restreinte, une attaque réussie est relativement improbable. En plus de la probabilité technique d'une attaque, chaque agent de menace a des facteurs de motivation et des capacités différents. Les capacités sont un terme général qui désigne les ressources financières , les connaissances et compétences ou d'autres ressources éventuellement que l'agent de menace utilise pour exploiter la vulnérabilité. Pour simplifier le problème et avoir une étude plus objective dans ce manuscrit, nous partons de l'hypothèse que tous les attaquants ont des motivations similaires de causer le plus de dégâts possibles .

5.3.3 Analyse des Modes de Défaillance, de Vulnérabilité, de leurs Effets, de leur Criticité et Évaluation des Risques (AMDVEC & ER)

Avec les composants individuels d'une chaîne de cause à effets de la SEC décrits dans les sections précédentes, nous sommes en mesure de générer une chaîne de cause à effets qui combine la SAF et la SEC. L'approche combinée inclut les causes à un effet négatif sur les attributs de la sûreté de fonctionnement (voir la figure 5.8).

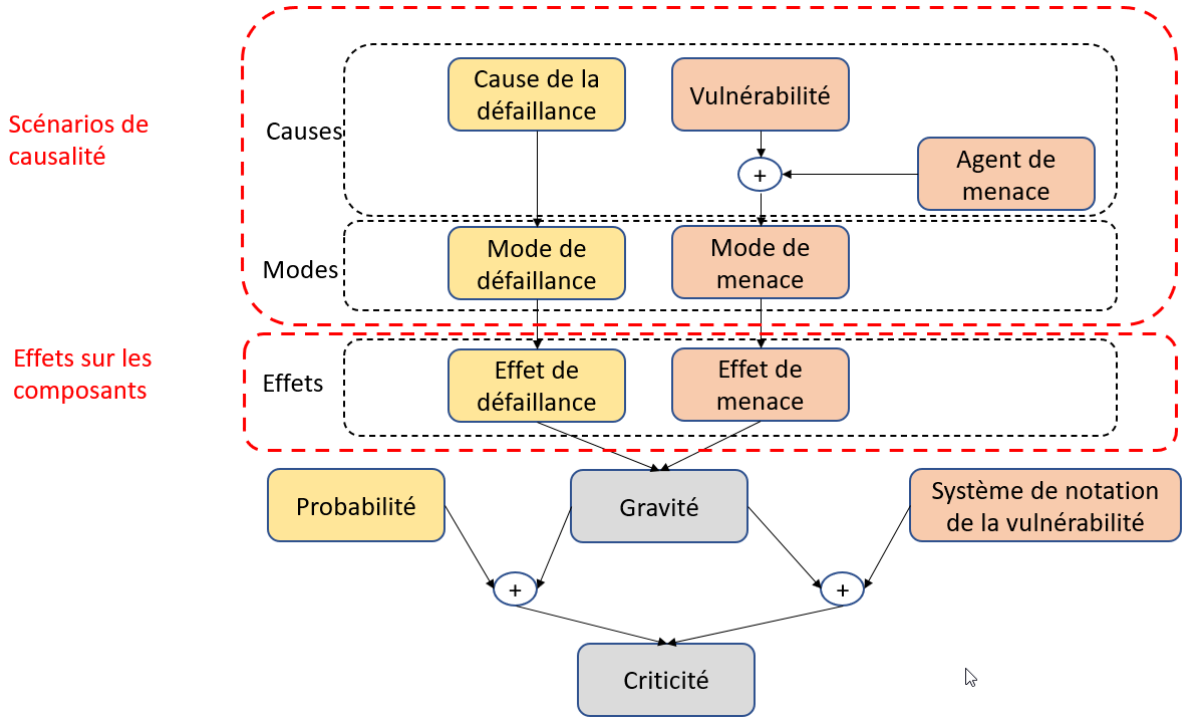


FIGURE 5.8 – Chaîne de cause-effet d'AMDVEC

5.4 Méthodologie d'évaluation des risques

L'organigramme étendu d'un AMDEC, dans la figure 5.8, inclut la sécurité dans l'analyse. Il existe différentes façons dont les propriétés de SEC ou de SAF d'un système peuvent influencer les risques. Par conséquent, bien que l'examen des modes de défaillance (ou de menace d'un élément ou une composante) soit séparé, l'analyse des effets et des causes

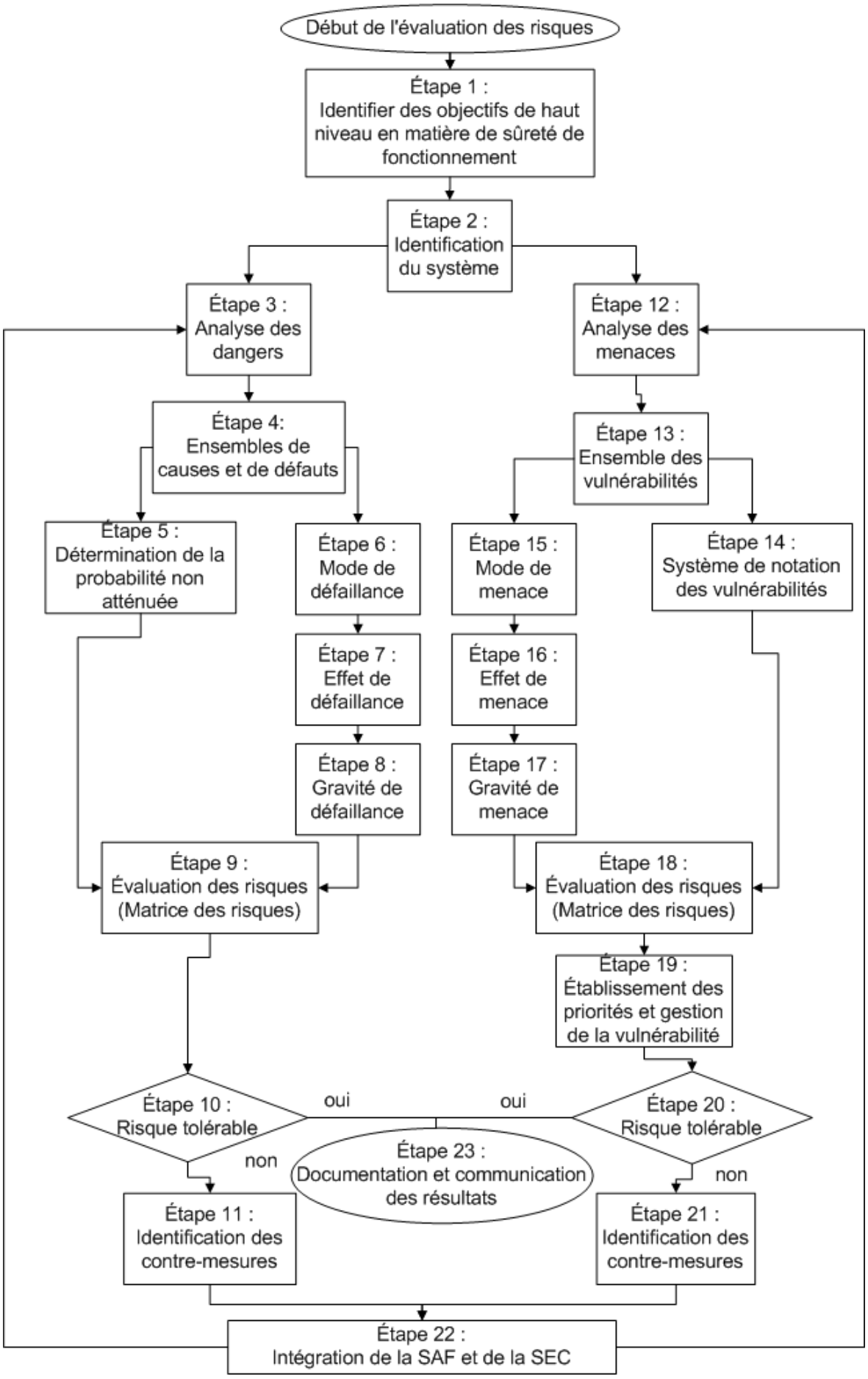


FIGURE 5.9 – Méthodologie d'évaluation des risques basée sur les normes ISA/IEC-62443 et IEC-60812 (AMDVEC & ER)

quant à elle combine les deux points de vue. De plus, la solution proposée doit être conforme aux normes de la SAF et de la SEC des systèmes industriels. À partir de la norme CEI 60812 de la SAF et la norme ISA/CEI 62443 de la SEC, nous proposons une nouvelle méthodologie d'évaluations des risques (voir la figure 5.9). Cette méthodologie est composée de 23 étapes :

- La première étape consiste à identifier les objectifs de haut niveau en matière de SAF et /ou SAF, parfois aussi appelés objectifs ou buts de SAF et / ou SEC. Par exemple, les objectifs de sécurité comprennent tous les actifs de sécurité pertinents (par exemple : des données, des fonctionnalités ou des ressources critiques) et les politiques de sécurité (par exemple, *seul le personnel autorisé peut modifier les paramètres de fonctionnement des composants*).

- L'étape 2 est l'identification du système qui doit être étudié. Elle implique une phase de spécification fonctionnelle et de conception, qui vise à identifier les équipements physiques et informatiques du système.

- Les étapes 3, 4, 12, 13 et 14 traitent du paysage des périls du système par le biais d'une analyse des dangers et / ou des menaces. Les défaillances et vulnérabilités potentielles du système sont identifiées.

- Ensuite, la probabilité de défaillance et le score de vulnérabilité identifiée doivent être déterminés aux étapes 5 et 14 respectivement.

- Dans les étapes 6 et 7 pour la SAF et dans les étapes 15 et 16 pour la SEC, le mode et l'effet sont déterminés, en identifiant l'effet par lequel la défaillance ou l'exploitation de la vulnérabilité est observée. Et pour chaque mode, les procédures de détection et les actions correctives requises doivent être spécifiées.

- Une fois que le mode et l'effet de la défaillance ou/et de la vulnérabilité sont identifiés, leurs impacts directs et leurs conséquences en cascade (la gravité) sur l'ensemble du système doivent être étudiés aux étapes 8 (pour la SAF) et 17 (pour la SEC).

- Les étapes 9 et 18 consistent à calculer les matrices des risques de la SAF et la SEC en utilisant la probabilité (dans le cas de la SAF) ou le système de notation de la vulnérabilité (dans le cas de la SEC) et la gravité déterminée.

- Aux étapes 11 et 21, les contre-mesures doivent être mises en œuvre pour atténuer les risques intolérables. Ensuite, le score ou la probabilité doit être réévalué pour mesurer l'efficacité des mesures proposées. Si certains risques sont considérés comme inacceptables, un ensemble de contre-mesures supplémentaires doivent être proposées.

- À l'étape 22, l'alignement entre la SAF et la SEC doit être effectué.

- Les étapes 3 à 22 doivent être répétées jusqu'à ce que tous les risques deviennent tolérables.

- Enfin, le processus d'évaluation des risques doit se clôturer par une phase de documentation (étape 23) .

Pour appliquer la méthodologie proposée, nous allons nous focaliser sur les risques cyberattaques notamment sur les étapes 14,15,16 et 18 de la figure 5.9. Dans la suite, nous allons détailler ci-dessous chacune de ces étapes :

- **Étape 14 : système de notation de la vulnérabilité :** dans le cas de la SEC, la probabilité d'un accident peut être comparée au degré d'accessibilité de l'attaquant pour exploiter une faiblesse du système. Dans notre cas, le potentiel d'attaque décrit les ressources techniques et intellectuelles accumulées qui sont nécessaires pour monter avec succès une certaine attaque.
  Pour avoir une approche similaire à l'AMDEC, il nous faut séparer la probabilité et la gravité d'une attaque dans le système de notation de la vulnérabilité que nous avons défini dans le chapitre 3. En effet, dans le calcul de ICVSS, nous avons trois composantes : les métriques d'exploitabilités, les métriques d'impact et celles environnementales. Dans le cadre de l'approche proposée, nous souhaitons avoir une métrique proche de la probabilité d'une attaque, que nous avons notée *système de notation de la vulnérabilité* sur la figure 5.9. Nous avons donc séparé les métriques et retenu que les métriques d'exploitabilité (AV, AC, Au) et les métriques temporelles (E, RL, RC) (voir la figure 5.10). Les autres métriques (les métriques d'impact (C-I-A) et environnementales (TD, CPD, CR,IR,IR)) sont utilisées pour évaluer la gravité de la menace que nous allons détailler dans la section 5.5.

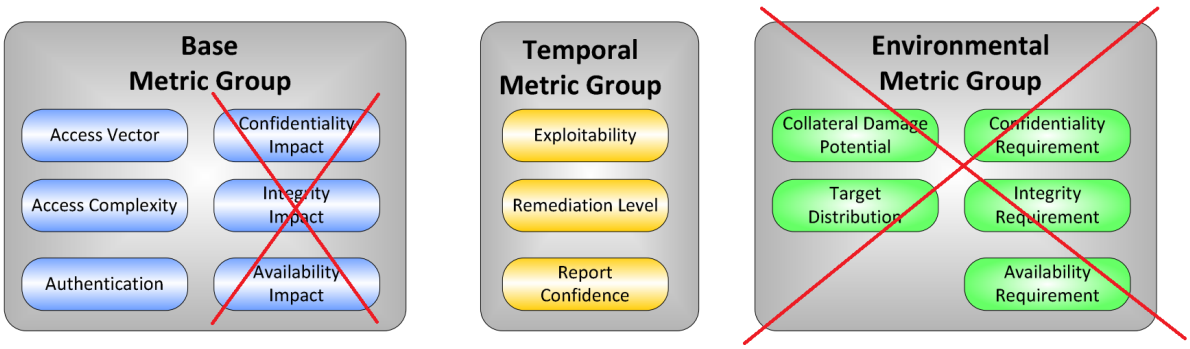


FIGURE 5.10 – Métriques utilisées pour noter la vulnérabilité

Afin que nous soyons cohérents avec l'approche AMDEC, nous allons définir cinq niveaux de criticité sur le système de score notation de la vulnérabilité (voir le tableau 5.1). La nouvelle équation du système de notation est définie comme suit :

$$\mathrm{BS} = \mathrm{ES} = 20 \times \mathrm{AV} \times \mathrm{AC} \times \mathrm{A}u \tag{5.1}$$

$$Score_{final} = RoundToDecimal(\mathrm{BS} \times \mathrm{E} \times \mathrm{RL} \times \mathrm{RC}) \tag{5.2}$$

le nouveau score entre 0,0 et 10 est reparti cette fois sur cinq valeurs quantitatives (voir le tableau 5.1).

- **Étape 15 : Mode de menace :**

  Pour définir les modes de menaces, nous proposons une extension aux ICS du modèle commun STRID (Spoofing, Tampering Repudiation, Information, disclosure, Denial of service and Elevation of privilege) (Hernan et al., 2006). Elle est décrite dans le tableau 5.2 qui présente les effets génériques conduits par les vulnérabilités exploitées. Pour une classification des modes de menace et de défaillance, l'approche décrite dans (Powell and Stroud, 2003) pourrait être aussi utilisée. Différentes propriétés des modes de défaillance sont décrites et triées.

Notation	Score de ICVSS
Très faible	0.0 - 1,9
Faible	1.9 - 3.9
Medium	4.0 - 6.9
Élevé	7.0 - 7,9
Très Élevé	7.9 - 10

TABLEAU 5.1 – Échelle quantitative et qualitative du score

Mode de menace	**Description**	**Attribut de sécurité violé (effet générique)**
Usurpation d'identité	Accéder à un système déguisé en autre acteur	Authenticité
Falsification des données de contrôle des actionneurs	Modification non autorisée des données envoyées aux actionneurs	Integrité
Falsification des données des capteurs	Modification non autorisée des données envoyées aux capteurs	Intégrité
Falsification des données sur envoyées au système de supervision	Modification non autorisée des données envoyées aux systèmes de supervision	Intégrité
Répudiation	pouvoir nier qu'un événement a eu lieu	Non-répudiation
Divulgation des informations	Accès aux données restreintes	Confidentialité
Élévation du privilège	Les acteurs peuvent effectuer des actions avec un niveau d'autorité supérieur.	Authenticité
Déni de service (DoS)	Restreindre ou empêcher l'accès à un niveau d'autorité de service ou de fonction.	Disponibilité

TABLEAU 5.2 – Modes de menaces

- **Étape 16 : Effet de la menace :**

  Est une étape descriptive de l'effet de la menace , similaire à la présentation de l'effet de la défaillance (étape 7).

- **Étape 17 : Gravité de la menace :**

  Selon notre méthodologie, il y a une similarité entre l'impact et la gravité et aussi entre le système de notation de la vulnérabilité avec la probabilité. Pour l'étape 17, l'approche retenue est de bâtir une évaluation de la gravité qui aboutira une analyse de risque similaire de sécurité-innocuité (voir la figure 5.11). Nous examinons les impacts directs des menaces potentielles identifiées et leurs conséquences qui en résultent. Dans section 5.5, nous allons donner plus de détails sur les étapes de calcul de la gravité dans le cas de la cybersécurité.

- **Étape 18 : Évaluation des risques de la SEC :** Les matrices de risque sont utilisées pour déterminer le niveau de risque (Probabilité x Gravité) et pour décider si le

Probabilité	Niveau du risque			
Certain	Inacceptable	Inacceptable	Inacceptable	Inacceptable
Probablement	Médium	Inacceptable	Inacceptable	Inacceptable
Eventuellement	Acceptable	Médium	Inacceptable	Inacceptable
Peu probable	Acceptable	Acceptable	Médium	Inacceptable
Rare	Acceptable	Acceptable	Acceptable	Médium
	Insignifiant	Médium	Critique	Catastrophique
	Gravité			

FIGURE 5.11 – Matrice des risques de la SAF

risque est acceptable ou non. Dans les systèmes industriels, un risque est considéré comme non acceptable lorsque sa valeur est élevée ou critique, et acceptable si sa valeur est faible ou négligeable (Rekik et al., 2018). Par contre, dans le cas de la SEC, nous remplaçons la probabilité par le système de notation ICVSS (voir la figure 5.12). Les matrices de risques seront également utilisées pour identifier des solutions d'atténuation. En effet, les contre-mesures seront appliquées de manière à réduire la gravité des défauts ou des vulnérabilités. Ainsi, si un danger ou une menace présente un risque inacceptable, nous devons pousser diagonalement à travers la matrice des risques (voir figures 5.11,5.12) jusqu'à la partie acceptable la plus proche, en suivant la méthodologie de la figure 5.9. Dans une évaluation des risques, les impacts sur le système doivent être évalués sans aucune contre-mesure supplémentaire afin de voir les conséquences réelles (Rekik et al., 2018).

Donc, à partir du système de notation de la vulnérabilité, et la gravité, on peut évaluer le risque par la matrice de sécurité (voir la figure 5.12)

System de notation	Niveau du risque			
Très élevé	Inacceptable	Inacceptable	Inacceptable	Inacceptable
Elevé	Médium	Inacceptable	Inacceptable	Inacceptable
Médium	Acceptable	Médium	Inacceptable	Inacceptable
Faible	Acceptable	Acceptable	Médium	Inacceptable
Très faible	Acceptable	Acceptable	Acceptable	Médium
	Insignifiant	Médium	Critique	Catastrophique
	Gravité			

FIGURE 5.12 – Matrice des risques de la SEC

Dans la section suivante, nous allons présenter les métriques et les paramètres que nous allons utiliser pour évaluer et calculer la gravité de la menace (G) à l'étape 18.

5.5 Gravité de la menace (G)

D'abord, la gravité doit inclure les impacts directs des menaces et des vulnérabilités potentielles identifiées et leurs conséquences sur l'ensemble du système. Le calcul de la gravité dépend de plusieurs types d'impacts, à savoir un impact sur la sécurité-innocuité, sur la sécurité-immunité et un impact financier. Elle dépend aussi des autres métriques que nous avons vues dans le système de notation présenté dans le chapitre 3, comme nombre de cibles impactées (TD), couverture par le Système de SAF (SS). Enfin, nous

avons ajouté d'autre métriques comme la détectabilité de la menace(D) - très utilisé dans les méthodes de l'AMDEC - et la Sévérité de la Zone (SZ).

5.5.1 Détermination de l'impact

Les impacts identifiés peuvent toucher un ou plusieurs aspects en fonction de la zone touchée qui doit être prise en compte. Nous définissons trois types d'impact : *impact de la SEC, impact financier et impact de la SAF.*

La méthodologie (Wolf and Scheibel, 2012) attribue les conséquences de chaque type d'impact (tableau 5.3), en fonction de leur niveau de gravité. Une échelle de puissance décimale a été utilisée pour évaluer la gravité. En somme, l'impact total est déterminé comme suit :

$$I_{mpact} = I_{mpact_{\mathrm{SEC}}} + I_{mpact_{\mathrm{SAF}}} + I_{mpact_{\mathrm{F}inancière}} \tag{5.3}$$

Ci-après, nous présentons les trois types d'impact évoqués :

Impact de la sécurité-immunité (SEC)

L'impact de la SEC représente l'impact de la confidentialité, l'intégrité et la disponibilité. Par ailleurs, nous souhaitons donner plus d'importance à la disponibilité et à l'intégrité par rapport à la confidentialité, puisque dans le cas des ICSs, la disponibilité (A) et l'intégrité (I) sont plus importantes que la confidentialité (C). En effet, Les métriques (CR, IR, AR) permettent aux utilisateurs d'ajuster l'impact en fonction de l'importance des paramètres de la sécurité C-I-A. Les valeurs possibles des exigences de sécurités (CR,IR, AR) sont : "faible L= 0.5", "moyen M=1.0", "élevé H = 1.5", "non Défini=1.0". Nous avons choisi la valeur "élevé H = 1.5" pour disponibilité (A) et l'intégrité (I) et la valeur 1.0 pour la confidentialité (C),

En conséquence, nous définissons l'impact de la SEC comme suit :

$$I_{mpact_{\mathrm{SEC}}} = (\mathrm{C}_{impact} + 1,5 \times \mathrm{I}_{impact} + 1,5 \times \mathrm{A}_{impact})/4 \tag{5.4}$$

Par contre, les trois valeurs de C-I-A définies dans la chapitre 3 sont remplacées par les valeurs de puissance décimale suivantes :
Aucune ou insignifiante (0) ; Partielle : (1000) ; Complète (10000)

Impact de la sécurité-innocuité (SAF)

Les niveaux d'intégrité de la SAF (SIL) sont une classification discrète et systématique, qui varie de SIL 1 (pour le niveau de sécurité le plus faible) à SIL 4 (pour le niveau de sécurité le plus élevé). Selon la norme appliquée, l'intégrité de la sécurité (et donc le SIL) est un concept applicable aux systèmes électriques/électroniques/programmables (E/E/PE) (pour la CEI 61508 ((61508, 2005))) ou aux systèmes instrumentés (SIS) liés à la SAF (pour la CEI 61511 (61511, 2004)). Dans le tableau 5.3, les valeurs du niveau d'intégrité de la SAF et les proportions correspondantes (Wolf and Scheibel, 2012) sont données.

Impact financier

L'impact financier est le moins important parmi les impacts évoqués (SAF et SEC). Le tableau 5.4 résume les niveaux de criticité financiers avec leurs facteurs de criticité correspondants (Rekik et al., 2018).

Échelle abrégée des blessures	Référence SIL [IEC61508]	Facteur de réduction du risque
S1	Pas de blessures	10-100
S2	Blessures légères et modérées	100-1000
S3	Sévère et mortel; blessures (survie probable).	1000-10000
S4	En danger de mort; blessures (survie incertaine); blessures mortelles.	10000-100000

TABLEAU 5.3 – Mesures du niveau d'intégrité de la sécurité-innocuité et les proportions correspondantes

Niveau de Criticité	Référence	Facteur de Réduction du risque
S1	Aucun dommage financier ou tolérable	1-10
S2	Dommage financier indésirable et/ou l'incident peut avoir une l'impact sur l'image publique de l'entreprise	10-100
S3	Un dommage financier important, mais qui ne menace pas encore l'existence et/ou l'incident peut avoir un impact sérieux sur l'image publique de l'entreprise	100-1000
S4	L'existence d'un dommage financier menaçant et/ou l'incident entraînera des poursuites contre l'entreprise, ce qui aura un impact grave sur l'image publique de l'entreprise	1000-10000

TABLEAU 5.4 – Niveaux d'impact financier

5.5.2 Autres métriques

Nombre de cibles impactées (Target Distribution- TD)

Cette métrique appartient au groupe environnemental du système de notation de la vulnérabilité vu au chapitre 3. Elle mesure la proportion de systèmes vulnérables. Il s'agit d'un indicateur spécifique à l'environnement qui permet d'évaluer approximativement le pourcentage de systèmes qui pourraient être affectés par la vulnérabilité. Les valeurs possibles pour cette métrique sont :

- *Aucune (N = 0) :* le système cible n'existe pas, ou bien les cibles sont si spécialisées qu'elles n'existent que dans un cadre de laboratoire. En fait, 0% de l'environnement est menacé.
- *Faible (Low/L = 0.25) :* Les cibles existent dans l'environnement, mais à petite échelle. Entre 1 % et 25 % de l'environnement total est menacé.
- *Moyenne (Medium /M = 0.75) :* Les cibles existent dans l'environnement, mais à une échelle moyenne. Entre 26% et 75 % de l'environnement total est menacé.

- *Élevé (High /H = 1.00) :* Les cibles existent dans l'environnement à une échelle considérable. Entre 76 % et 100 % de l'environnement total est considéré comme menacé.

- *(Non défini / ND= 1.00) :* L'attribution de cette valeur n'influence pas le score final.

Détection (D)

Il s'agit d'une métrique de l'efficacité des contrôles (inspection, alerte/avertissement) - très utilisée dans la démarche AMDEC - pour prévenir ou détecter la cause ou le mode de défaillance avant que la défaillance cause des dégâts. Trois valeurs sont possibles pour cette métrique :
Aucune ou insignifiante (0) ; Partielle : (0.275) ; Complète (0.66)

Couverture par le système de SAF (SS)

Cette métrique présente le degré de couverture par le système de SAF (SS) lorsque une vulnérabilité est exploitée. Trois valeurs sont possibles :
Aucune ou insignifiante (0) ; Partielle : (0.275) ; Complète (0.66)

Sévérité de la zone (SZ)

Il s'agit d'une métrique qui permet de mesurer la sévérité et le danger de la zone lorsqu'une vulnérabilité est exploitée. En fait, dans la même infrastructure nous pouvons la segmenter en plusieurs zones selon le danger qui représente le point de vue SAF. Par exemple, une zone qui contient des produits explosifs. Deux valeurs sont possibles :
Normale : 1, Critique : 1,5

5.5.3 Calcul de la Gravité (G)

Après avoir résumé les métriques qui interviennent sur les différents types d'impact, nous pouvons écrire finalement l'équation globale de la gravité (G) comme suit :

$$\mathrm{G} = (\mathrm{I}impact_{\mathrm{SAF}} + \mathrm{I}impact_{\mathrm{SEC}} + \mathrm{I}impact_{\mathrm{Financière}}) \times (1 - \mathrm{D}) \times (1 - \mathrm{SS}) \times (\mathrm{SZ}) \times (\mathrm{TD}) \quad (5.5)$$

La valeur calculée reflète la gravité de la menace. Le tableau 5.5 résume les niveaux de gravité avec leurs facteurs correspondants.

Valeur de la gravité	Niveau de gravité
0 -99	Insignifiant
99 - 1000	Médium
1001 - 9999	Critique
>= 10 000	Catastrophique

TABLEAU 5.5 – Niveau de gravité

Pour illustrer notre méthodologie, nous allons l'appliquer sur un cas d'étude.

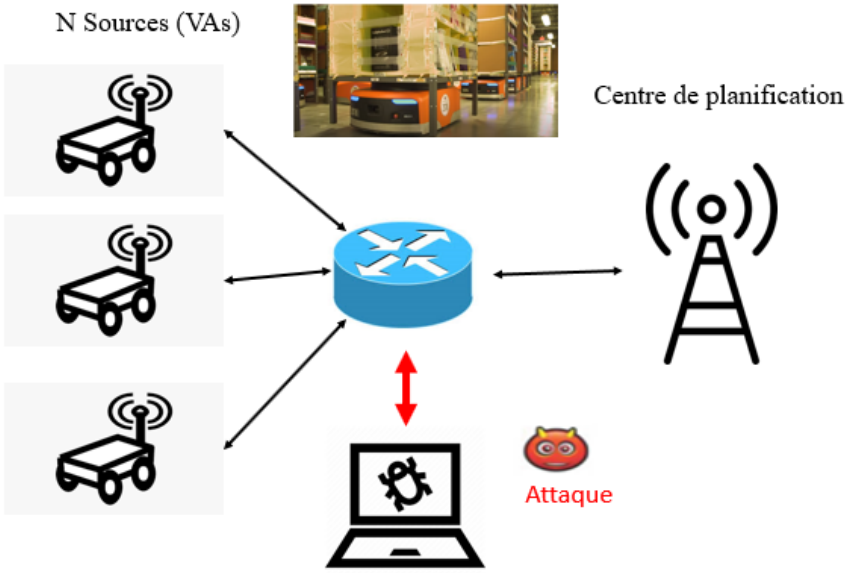


FIGURE 5.13 – Cas d'étude : réseaux sans fil des robots mobiles

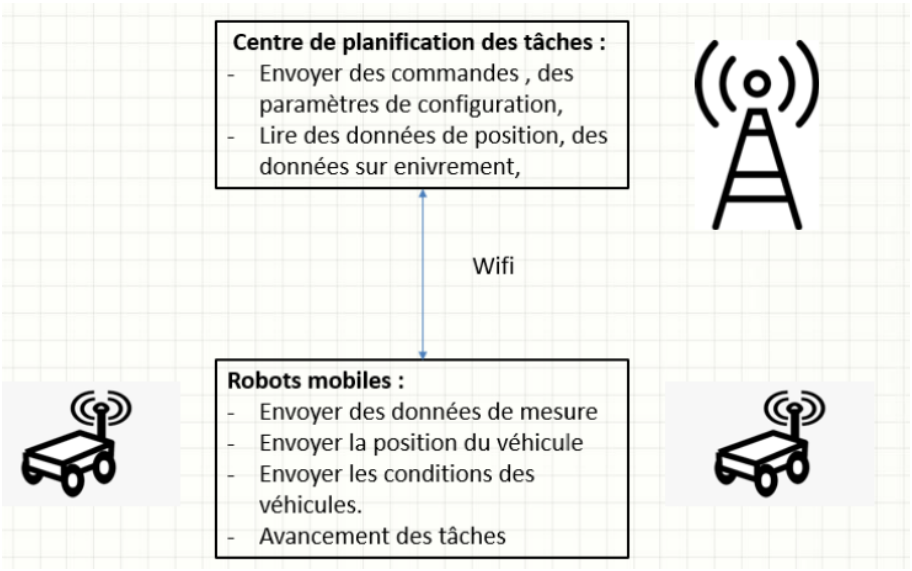


FIGURE 5.14 – Communication bidirectionnelle entre les robots et la station

5.6 Cas d'étude : Réseau des robots mobiles

Nous allons appliquer notre méthodologie à un système industriel constitué d'un réseau de robots mobiles sans fil qui collaborent entre eux pour mener à bien les missions demandées. Les robots reçoivent des commandes d'un centre de planification des tâches en temps réel. La communication est assurée par un routeur qui assure l'échange bidirectionnel de données entre les robots et la station de planification (voir les Figures 5.13 5.14) via un protocole TCP.

5.6.1 Protocole TCP (Transmission Control Protocol)

Le TCP est un protocole de transport fiable. Les données échangées sont segmentées et peuvent être envoyées ou reçues par paquets individuels. L'émetteur envoie plusieurs

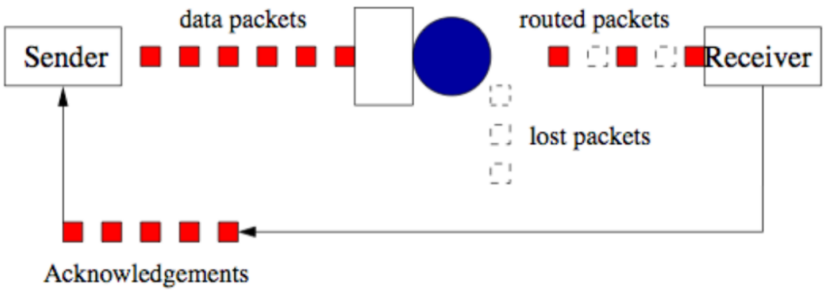


FIGURE 5.15 – Pertes des paquets au niveau du routeur (Hollot et al., 2002)

paquets et il attend l'acquittement lors de leur réception(Figure 5.15).

5.6.2 Phénomène de congestion

Lorsque le trafic requis est très supérieur à la capacité du réseau, un phénomène se produit que l'on appelle la congestion. En réalité, la congestion ou la saturation du réseau entraîne des retards dans la transmission des données et au pire leur éventuelle perte. Le protocole TCP met donc en place un mécanisme de contrôle de la congestion qui permet à chaque émetteur la possibilité de "sonder" le réseau afin de mieux ajuster son débit à la charge disponible. D'une façon globale, le contrôle de la congestion vise à régulariser le trafic produit par les différents émetteurs en relation avec la capacité du réseau. Le protocole TCP surveille l'apparition d'une perte pour détecter un problème de congestion au sein du réseau. Ce retour d'information est possible par le biais du système d'accusé de réception qui permettra à l'émetteur de "se tenir au courant des paquets demandés" par le récepteur . La solution proposée par le TCP revient donc à modifier la taille de la fenêtre de transmission en tenant compte de la capacité et la charge du réseau (la fenêtre de congestion). Elle détermine le nombre maximum de paquets que l'expéditeur peut transmettre avant de recevoir un accusé de réception. Sa taille, que l'on note W, augmente lorsque de nouvelles données sont acquittées et diminue lorsque des données doivent être retransmises.

5.6.3 Différentes types de menaces

Il existe différentes attaques sur un unique réseau de robots. Chacune d'entre elles affectant différents paramètres du réseau. Nous pouvons établir une liste de quelques-unes des attaques potentielles :
- L'attaque par trou de ver : dans ce cas, l'attaquant fait passer des messages à travers le trou de ver afin de pouvoir récupérer des informations sur le réseau (routage, données...) ;
- L'attaque par usurpation d'identité : elle vise à falsifier les informations d'identité. Cela pourrait conduire à l'isolement de certains nœuds, à échanger de fausses données de routage et à la violation de l'intégrité et la confidentialité ;
- L'attaque par déni de service (Denial of Service - DoS) : elle consiste à envoyer volontairement des trames afin de saturer et de paralyser le réseau. Dans ce cas d'étude, nous nous focalisons principalement sur les attaques de type (DoS).

Topologie utilisée

Pour répondre à notre problématique de recherche, nous prenons dans un premier temps en considération une topologie simple constituée de *N* émetteurs, d'un routeur et d'un récepteur (figure 5.16). Par conséquent, nous avons N sources TCP avec le même

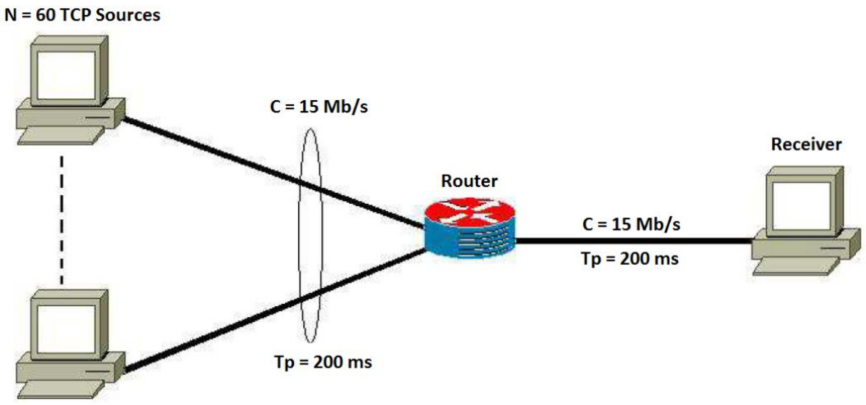


FIGURE 5.16 – Topologie du réseau utilisé (Ariba et al., 2008)

temps de propagation connectées à un nœud de destination via le routeur. Nous nous basons sur (Ariba et al., 2008), pour choisir les paramètres du réseau :
- la capacité du lien (C) = 3750 paquets/s ;
- le retard de propagation : (Tp) = 0.2s ;
- le nombre de sessions TCP (N) = 60.
Nous employons le modèle présenté dans l'article (Ariba et al., 2008). Le modèle d'états dynamique du changement de la fenêtre de congestion W(t) d'une N source TCP et la longueur la file d'attente du tampon q(t), sont donnés comme suit :

$$\begin{cases} \dot{\mathrm{W}}(t) = \frac{1}{\mathrm{R}(t)} - \frac{\mathrm{W}(t)\mathrm{W}(t-\mathrm{R}(t))}{2\mathrm{R}(t-\mathrm{R}(t))} p(t-\mathrm{R}(t)) \\ \dot{q}(t) = \frac{\mathrm{W}(t)}{\mathrm{R}(t)}\mathrm{N} - \mathrm{C} + d(t) \end{cases} \tag{5.6}$$

Avec :
- W : La taille de la fenêtre de congestion (paquets) ;
- q : La taille de la file d'attente (paquets) ;
- R : RTT (Round-trip-time, [seconds]) ;
- p : La probabilité d'éjection de paquets ;
- C : La capacité du lien ;
- Tp : Le retard de propagation ;
- N : Le nombre de sessions TCP ;
- d(t) : représente un signal modélisant le trafic anormal ou une attaque qui paralyse le buffer du routeur. La figure 5.17 représente le résultat de la simulation du modèle 5.6. En bleu le trafic normal et en rouge le trafic subissant une série d'attaques sur le routeur qui consiste à injecter de faux paquets formant des rampes, afin de saturer le routeur. Nous supposons que le réseau va saturer à partir de 200 paquets par seconde pour rendre le réseau paralysé.
Nous émettons quelques hypothèses sur le choix des métriques pour ce cas d'étude. Nous supposons que :

- l'attaquant réussi à exploiter une vulnérabilité dans le système d'exploitation du routeur.

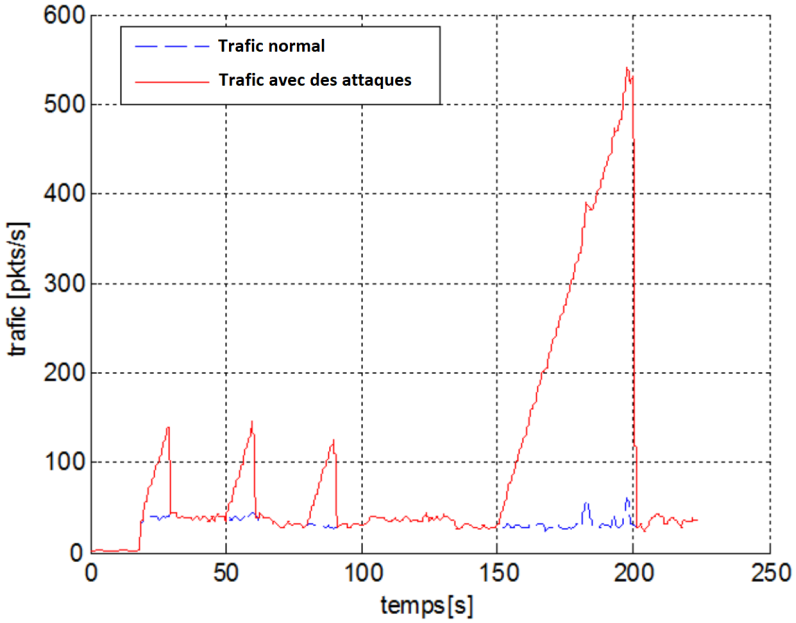


FIGURE 5.17 – Trafic normal vs trafic avec une attaque DoS de type rampe (CHEMALI et al., 2017)

- le nombre de cibles impactés est non défini (TD = 1.0).
- la criticité de la zone est normale (SZ =1.0).
- il y a un risque de collision entre les robots et les personnes. La menace peut causer des blessures (survie probable, voir le niveau SIL= S3 du tableau 5.3). L'impact de la SAF est *critique (SIL= S3)*. Nous avons estimé que la valeur est égale à 1000.
- l'impact financier est insignifiant (égale à la valeur 10.0)

L'attaque Dos va impacter la disponibilité (A = complète (10000), sans impacter l'intégrité (I= Aucun (0.0)) ou la confidentialité ((I= Aucun (0.0)), car il s'agit d'un arrêt de service. Le système n'est pas doté d'un système de SAF (SS = Aucun (0.0)). L'attaque n'est pas détectable (il n'y a pas un système de détection D = Aucun (0.0)).

La figure 5.18 présente en détail le choix des métriques pour le calcul de la gravité (G). L'application de la partie évaluation de la gravité de la menace du DoS en suivant les étapes présentées dans l'organigramme de la figure 5.9.

En utilisant les tableaux 5.3 et 5.4 et l'équation 5.4, nous pouvons calculer la gravité comme suit :

$$G = [SAF_{Impact} + SEC_{Impact} + Financière_{Impact}] \times (1 - D) \times (1 - SS) \times (SZ) \times (TD) \quad (5.7)$$

$G = [1000 + ((10000 * 1.5 + 0.0 * 1.5 + 0.0 * 1)/4 + 10] \times (1 - 0)(1 - 0) \times 1.0 \times 1.0 = 4760$
La valeur calculée correspond au niveau gravité critique (voir tableau 5.5).

Calcul du score ICVSS du vulnérabilité Dos du routeur

D'après l'architecture du réseau de communication des robots mobiles, nous allons construire le vecteur notation ICVSS comme suit :

- Le réseau de communication est un réseau sans fil (WL=1.0) ;

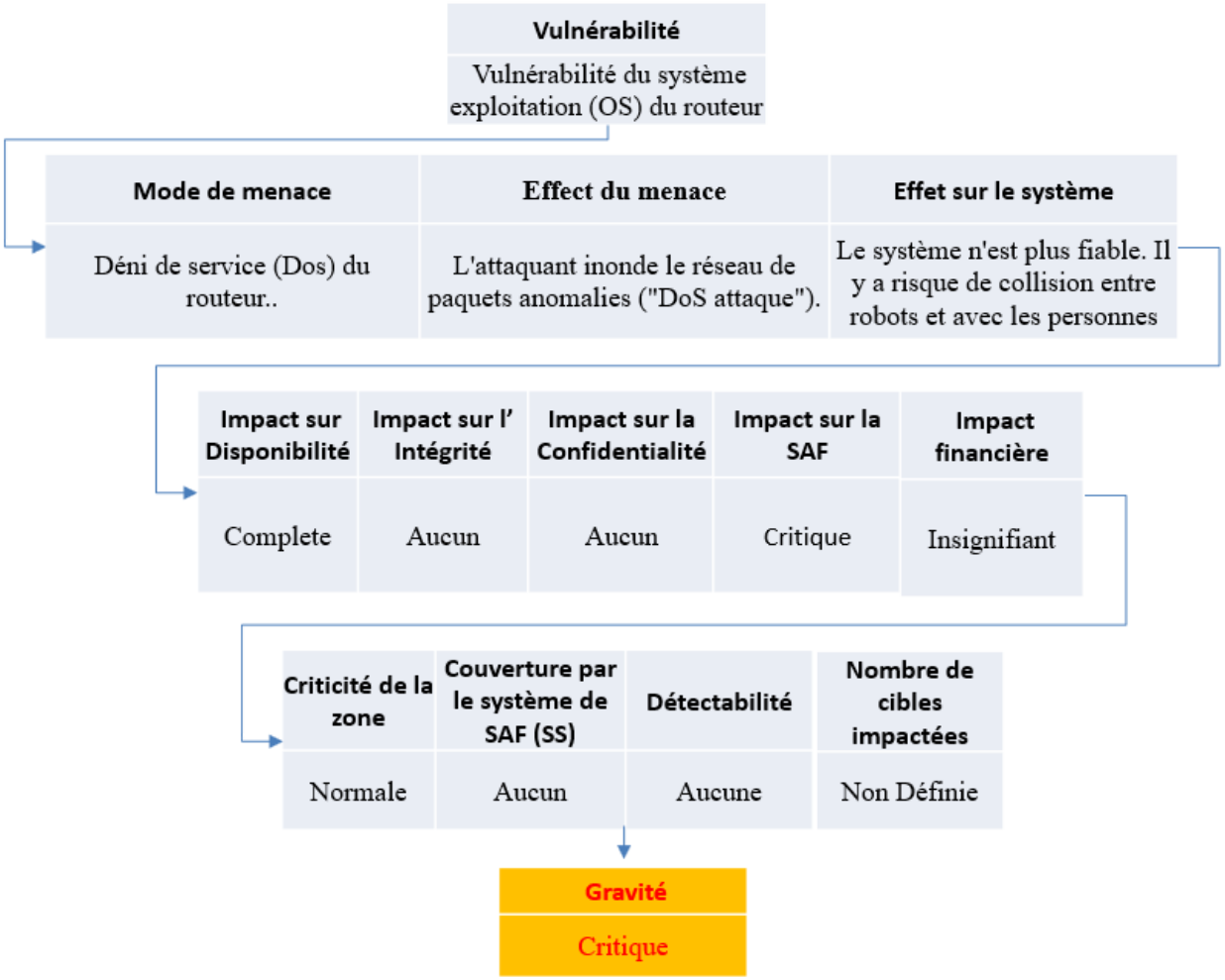


FIGURE 5.18 – Étapes de calcul la gravité du menace Dos

- Le réseau de communication est un réseau local (A=0.646) ;
- Nous supposons que la complexité de l'attaque est facile (L=0.71) ;
- Il n'y a pas un système de chiffrement (cryptage) de la communication ;
- Nombre d'authentification nécessaire pour se connecter au réseau est unique (Au=0.56) ;
- Les métriques de : Maturité (M), Accès au système (SA), Niveau de correction (RL), Niveau de confiance (RC) sont supposées non définies.

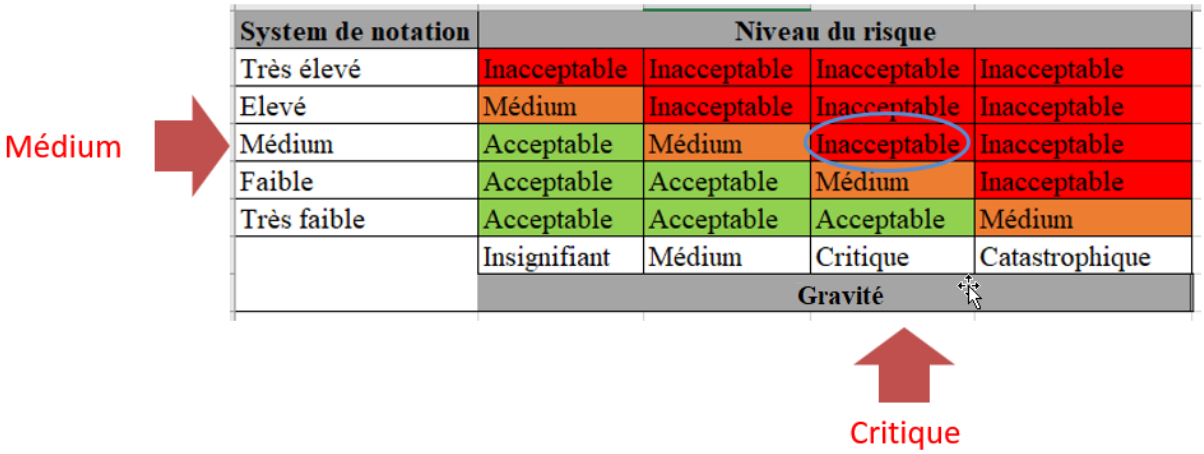
La figure 5.19 montre les métriques qui permettent d'évaluer la vulnérabilité DoS du routeur. Le vecteur et score correspondant est donné par :
ICVSS = AV{PM : W&AL : Adj}/AC{SC : S&ATC : L&C : N}/Au : N/RL : ND/RC : ND = 6,8
Par la suite, nous pouvons obtenir la valeur *Médium* comme une valeur qualitative de la criticité de la vulnérabilité à partir du tableau 5.1.

5.6.4 Calcul de la criticité

L'utilisation de la matrice du risque 5.12 donne un risque inacceptable (voir la figure 5.20). Pour cette raison, nous devons pousser la criticalité vers la zone verte (risque acceptable).

	Criterion	Notation
Access Vector, AV	Physical Media (PM):	Wireless (WL) : 1.0
	Access Layer (AL) :	Adjacent Network (A): 0.646
Access Complexity, AC	System complexity [SC]	Simple (S) : 0.35
	Attack complexity [ATC]	Low (L): 0.71
	Cryptography [C] :	Non (N) : 0.71
	Authentication, Au	Single (S): 0.56
Exploitability €	System Access [SA]	not defined 1.00
	Maturity [M]	not defined: 1.00
	Remediation lavel [RL]:	not defined: 1.00
	Report Confidence (RC):	not defined: 1.00

FIGURE 5.19 – Vecteur ICVSS du vulnérabilité Dos



System de notation	Niveau du risque			
Très élevé	Inacceptable	Inacceptable	Inacceptable	Inacceptable
Elevé	Médium	Inacceptable	Inacceptable	Inacceptable
Médium	Acceptable	Médium	Inacceptable	Inacceptable
Faible	Acceptable	Acceptable	Médium	Inacceptable
Très faible	Acceptable	Acceptable	Acceptable	Médium
	Insignifiant	Médium	Critique	Catastrophique
	Gravité			

FIGURE 5.20 – Matrice du risque de la SEC

5.6.5 Solution proposée

Nous suggérons une architecture duplex pour renforcer la disponibilité. L'architecture consiste en deux routeurs : un primaire et l'autre secondaire. Chaque routeur utilise un système d'exploitation (OS) différent et avec deux hardwares différents (deux fournisseurs différents). Cette architecture comporte un système de détection d'intrusion IDS (Intrusion Detection System) qui offre la possibilité de surveiller le trafic du réseau (Traffic monitoring) de telle sorte à détecter des activités inhabituelles qui sont considérées comme des intrusions et ainsi permettre d'avoir une action préventive. Elles s'appuient généralement sur deux types de sources d'information : les trames passant par le réseau et les informations recueillies sur les machines. Cela permet de renforcer la Détectabilité (D).

Dans le cas de la détection des anomalies sur le réseau, le système IDS permet de passer du routeur primaire au routeur secondaire pour assurer la disponibilité (A) (voir la figure 5.21). Ainsi, nous recalculons la gravité (G) avec un impact de la *disponibilité (A)* égale à *Aucun (0)*, une *Détectabilité (D)* égale *Complète (0.66)*, *system SAF (SS)* égale *Aucun (0)* (voir la figure 5.22).

Enfin, l'impact de SAF et l'impact financier restent sans modification.

En utilisant l'équation 5.5 nous obtenons :

$$G = [SAF_{Impact} + SEC_{Impact} + Financière_{Impact}] \times (1 - D) \times (1 - SS) \times (SZ) \times TD \quad (5.8)$$

$G = [1000 + (0 \times 1.5 + 0 \times 1.5 + 0\times)/4 + 10] \times (1 - 0.66) \times 1.0 \times 1.0 \times 1.0 = 343.4$

La valeur calculée correspond au niveau d'impact *Médium* (voir tableau 5.5) En analysant la matrice du risque de la solution proposée, nous remarquons que l'architecture duplex

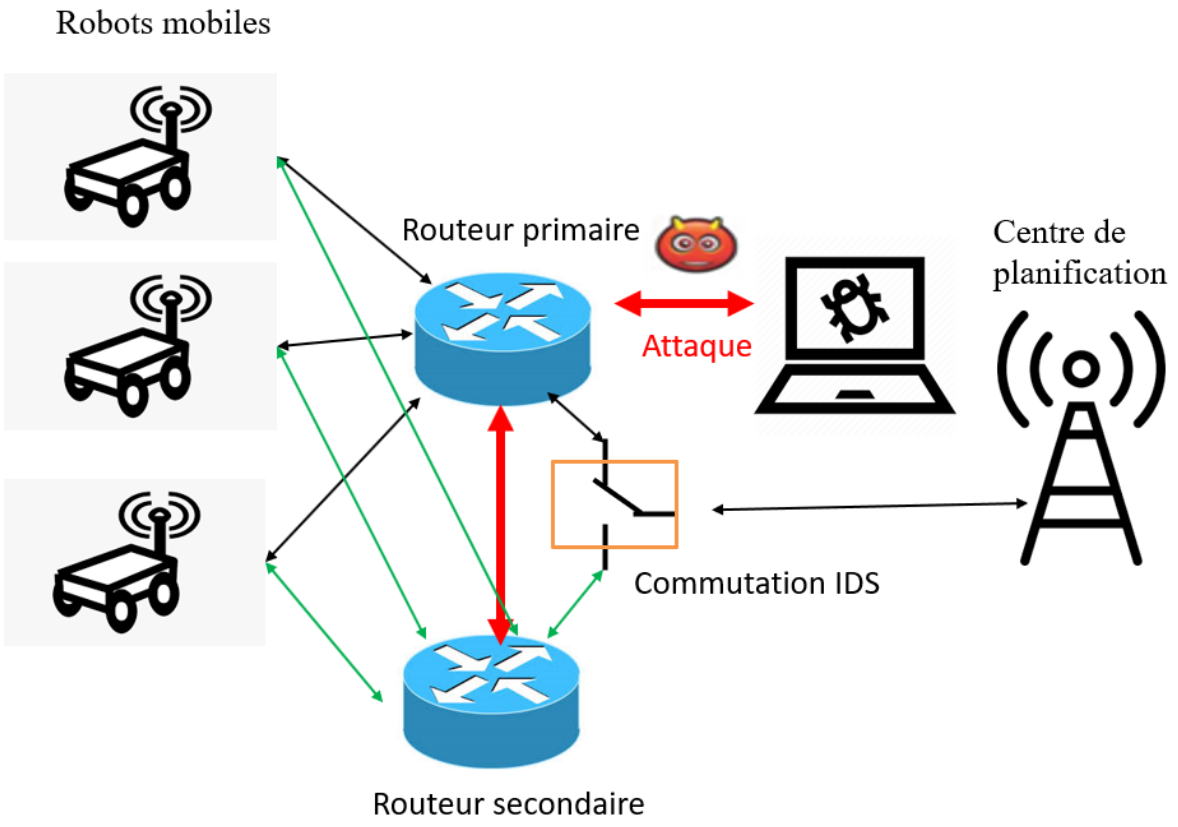


FIGURE 5.21 – Architecture duplex (redondance) pour renforcer la disponibilité

Impact sur Disponibilité	Impact sur l' Intégrité	Impact sur la Confidentialité	Impact sur la SAF	Impact financière	Criticité de la zone	Couverture par le système de SAF (SS)	Détectabilité	Nombre de cibles impactées
Aucun	Aucun	Aucun	Critique	Insignifiant	Normale	Aucun	Complète	Non Définie

Gravité

Medium

Medium

System de notation	Niveau du risque			
Très élevé	Inacceptable	Inacceptable	Inacceptable	Inacceptable
Elevé	Médium	Inacceptable	Inacceptable	Inacceptable
Médium	Acceptable	Médium	Inacceptable	Inacceptable
Faible	Acceptable	Acceptable	Médium	Inacceptable
Très faible	Acceptable	Acceptable	Acceptable	Médium
	Insignifiant	Médium	Critique	Catastrophique
	Gravité			

FIGURE 5.22 – Matrice du risque de l'architecture duplex

avec le système de détection d'intrusion a permis de réduire l'impact de la vulnérabilité. Cependant, l'évaluation du risque donne une valeur égale à *Médium*, ce qui n'est pas suffisant pour avoir un risque acceptable. En conséquence, une autre solution doit être proposée, qui agit sur les métriques du nouveau système de notation (ICVSS) en vue de réduire l'accès à la vulnérabilité et par la suite de réduire indirectement l'exploitabilité de la vulnérabilité.
Dans la section suivante, nous allons essayer de mieux sécuriser le réseau sans fil avec des mécanismes de protection qui compliquent encore la mission de l'attaquant et qui ajoutent des couches supplémentaires à la SEC.

Sécurité des réseaux sans fil

La sécurité vise à éviter les écoutes et les vols inattendus. La sécurité est essentielle pour protéger les communications de données, c'est-à-dire la confidentialité, l'intégrité et la disponibilité doivent être garanties. Les réseaux sans fil sont plus susceptibles d'être attaqués que les réseaux câblés, ce qui accroît les menaces pesant sur le réseau sans fil (A Ochang et al., 2016). En vue de réduire ces menaces, nous allons nous focaliser sur deux métriques : le cryptage (le chiffrement) de la communication et les protocoles l'authentification des robots qui se comportent comme deux couches qui travaillent en parallèle pour complexer l'accès pour les attaquants.

Authentification des robots

Vu que les robots sont considérés comme des utilisateurs du réseau sans fil, l'authentification des utilisateurs est considéré comme un processus d'identification des utilisateurs, généralement basé sur des noms d'utilisateur et des mots de passe. Dans un système de sécurité, l'authentification est différente de l'autorisation, qui est le processus consistant à donner aux utilisateurs l'accès aux objets du système sur la base de leur identité (Manurung, 2020).

Protocoles chiffrement sans fil

Vu que les réseaux sans fil diffusent les trames via l'air, quiconque possède un émetteur-récepteur sans fil peut intercepter les transmissions. Nous pouvons sécuriser les réseaux sans fil en plusieurs étapes, mais la plus importante consiste à mettre en œuvre un protocole de cryptage solide, tel que le Wi-Fi Protected Access II (WPA2) (Gibson, 2017). Les sections suivantes décrivent les principaux protocoles de sécurité disponibles pour les réseaux sans fil :

- **Wired Equivalent Privacy (WEP) :** WEB est un algorithme de chiffrement pour les réseaux sans fil IEEE 802.11. Introduit dans le cadre de la norme 802.11 originale ratifiée en 1997, son intention était de fournir une confidentialité des données comparable à celle d'un réseau câblé traditionnel (Committee et al., 2007). Le WEP reconnaissable à sa clé à 10 ou 26 chiffres hexadécimaux (40 ou 104 bits) a été à une époque largement utilisée et a souvent été le premier choix de sécurité présenté aux utilisateurs par les outils de configuration des routeurs.

- **WPA (Wi-Fi Protected Access) :** Le WPA était un remplacement provisoire du WEP (Wired Equivalent Privacy). Le WEP présente des vulnérabilités connues et son utilisation est à éviter. Le WPA a apporté une solution immédiate aux faiblesses du WEP sans obliger les utilisateurs de mettre à jour leur matériel. Même lorsque le WPA a

remplacé le WEP, ses développeurs ont reconnu que le WPA n'était pas assez solide pour durer pendant une période prolongée (Gibson, 2017). Au lieu de cela, le WPA a amélioré la sécurité sans fil en offrant aux utilisateurs une alternative au WEP avec le matériel existant pendant que les développeurs travaillaient à la création du protocole WPA2, plus solide. Le WPA est sensible aux attaques par craquage de mots de passe. L'attaquant utilise un analyseur de protocole sans fil pour capturer le trafic d'authentification et utilise ensuite une attaque de force brute hors ligne - une technique très connue dans la cryptanalyse pour retrouver un mot de passe ou une clé. Elle effectue des tests, l'un après l'autre, en utilisant toutes les combinaisons possibles- pour découvrir le mot passe (la phrase secrète). Les attaquants utilisent souvent une attaque de dissociation. Cette attaque consiste à retirer effectivement un client d'un réseau sans fil.

- **WPA2 Wi-Fi Protected Access II (WPA2) :** Le WPA2 est le remplacement permanent du WPA. Le WPA2 (également appelé IEEE 802.11i) utilise une cryptographie plus puissante que le WPA. Bien que la norme WPA2 apporte des améliorations significatives en matière de sécurité par rapport aux techniques de cryptage sans fil précédentes, certaines entreprises ont besoin d'une sécurité renforcée.

Attaque de dissociation

Pour comprendre l'attaque de dissociation, il est utile d'assimiler d'abord le fonctionnement normal. Après qu'un client sans fil se soit authentifié auprès d'un point d'accès (PA) sans fil, les deux appareils échangent des trames, ce qui entraîne l'association du client avec le point d'accès. À tout moment, un appareil sans fil peut envoyer une trame de dissociation au point d'accès pour mettre fin à la connexion. Cette trame comprend l'adresse MAC du client sans fil. Lorsque le point d'accès reçoit la trame de dissociation, il libère la mémoire qu'il utilisait pour la connexion. Dans une attaque de dissociation, les attaquants envoient une trame de dissociation au point d'accès avec une adresse MAC de la victime usurpée. Le point d'accès reçoit la trame et coupe la connexion. La victime est maintenant déconnectée du point d'accès et doit repasser par le processus d'authentification pour se reconnecter.

Protocoles d'authentification

Les réseaux sans fil supportent plusieurs protocoles d'authentification différents. Dans notre cas, nous allons mettre en place deux protocoles d'authentification pour avoir une authentification multiple. Afin de toujours complexifier la mission de l'attaquant, les protocoles sont :

- **PAP (Password Authentication Protocol) :** Le protocole d'authentification par mot de passe (PAP) est un protocole d'authentification basé sur un mot de passe et un identifiant. PAP est considéré comme un schéma d'authentification simple qui a une charge de calcul plus faible, mais il est beaucoup plus vulnérable aux attaques.

- **Protocole Authentification Diffie-Hellman :** La méthode Diffie-Hellman (DH) d'authentification des utilisateurs est très difficile à déchiffrer lors d'une simple intrusion (Oracle, 2020). Le client et le serveur possèdent tous deux leur propre clé privée, qui est combinée avec la clé publique pour constituer une clé commune. La clé privée est également appelée clé secrète. Le client et le serveur se servent de la

	Criterion	*Notation*
Access Vector, AV	**Physical Media (PM):**	Wireless (WL) : 1.0
	Access Layer (AL) :	Adjacent Network (A): 0.646
Access Complexity, AC	**System complexity [SC]**	Simple (S) : 0.35
	Attack complexity [ATC]	High (H): 0.35
	Cryptography [C] :	Encrypted (E) : 0.35
	Authentication, Au	Multiple (M): 0.45
Exploitability €	**System Access [SA]**	not defined: 1.00
	Maturity [M]	not defined: 1.00
	Remediation lavel [RL]:	not defined: 1.00
	Report Confidence (RC):	not defined: 1.00

FIGURE 5.23 – Vecteur ICVSS du vulnérabilité Dos avec les améliorations apportées

clé commune pour pouvoir communiquer entre eux. La clé commune est chiffrée à l'aide d'une fonction de cryptage spécifique.

5.6.6 Remarque

Des telles techniques de chiffrement et d'authentification rendent la mission d'un attaquant potentiel plus difficile. En revanche, l'utilisation de ces techniques demande plus de ressources de calcul, qui ne sont pas toujours disponibles dans les systèmes critiques ou dans les systèmes en temps réel. Dans ce manuscrit, nous supposons que les robots et le réseau sont dotés de ressources nécessaires pour implémenter ces algorithmes ou ces techniques.

Calcul du vecteur et du score du ICVSS

Les améliorations de SEC proposées permettent de changer le vecteur de ICVSS par le biais des métriques de cryptage (E), de complexité l'attaque (ATC) et l'authentification (Au). (voir la figure 5.23). La figure montre 5.19 les métriques qui permettent d'évaluer la vulnérabilité DoS du routeur avec les améliorations apportées. Le vecteur et score correspondant est donné par :
ICVSS = AV{PM : W&AL : Adj}/AC{SC : S&ATC : H&C : E}/Au : M/E{SA : ND&M : ND}RL : ND/RC : ND = 3
En utilisant le score calculé et à travers le tableau 5.1, nous pouvons obtenir la valeur qualitative *Faible* de la criticité de la vulnérabilité.

Calcul du criticalité

Après le calcul de la criticité, la matrice du risque de la SEC (voir la figure 5.12) nous a permis d'avoir un risque acceptable (voir la figure 5.24).

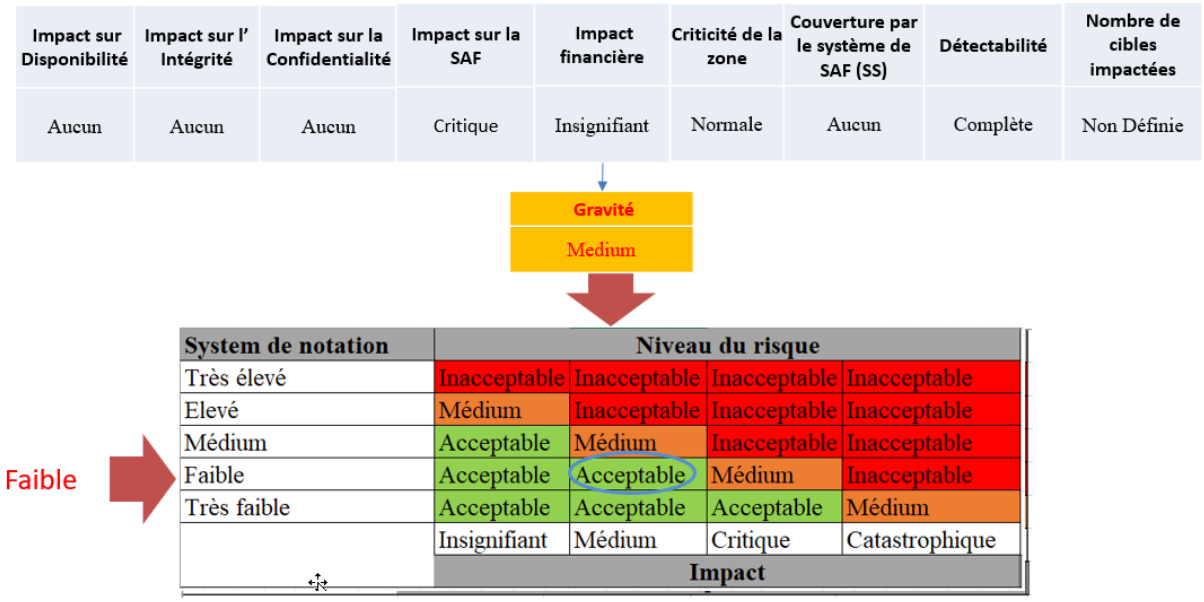


FIGURE 5.24 – Matrice du risque de la SEC

5.7 Conclusion

Nous avons proposé une méthodologie (voir la figure 5.9) pour évaluer les risques qui prennent en considération la dynamique des menaces de la cybersécurité. La méthodologie est utilisable en phase de développement et/ou en phase opérationnelle. Nous nous sommes basés sur un système de notation CVSS. Ce dernier permet de donner une évaluation rapide des risques des vulnérabilités d'une façon quantitative et qualitative. Sa simplicité, sa rapidité et sa dynamique d'évaluation contribuent à sa réputation et il est devenu le système d'évaluation le plus connu dans le domaine de la cybersécurité et dans les organisations comme le NIST. De plus, l'approche facilite la compréhension entre les ingénieurs de la SAF et les ingénieurs de la SEC qui ont besoin de moyens de communication pour harmoniser les efforts des deux équipes. Notre approche permet d'intégrer le principe de score avec une évaluation de SEC orientée vers la SAF, car nous estimons que la vraie problématique réside dans l'influence de SEC sur la SAF pour les systèmes ICSs.

Le défi est d'identifier et de sélectionner les modifications à apporter et les contre-mesures à installer pour les systèmes ICSs. La dynamique rapide des menaces est nécessaire pour rendre la priorisation des vulnérabilités selon leur impact sur la SAF à travers une évaluation quantitative. Notre approche offre aussi une évaluation qualitative sur la vulnérabilité à travers un vecteur des métriques qui doit être associé à chaque évaluation des risques. En effet, ce vecteur permet de donner une carte des faiblesses du système industriel pour chaque menace avec un langage claire (différentes métriques) ce qui facilite la proposition des contre mesures nécessaires.
De plus, notre approche prend en considération les standards de la SAF et la SEC avec l'utilisation IEC60812 et ISA/IEC 62443 respectivement.

Chapitre 6

Conclusion générale et perspectives

Contents

6.1 Synthèse des travaux réalisés

6.1.1 Contribution

Nous avons présenté dans cette thèse, des approches qui prennent en compte l'ensemble des risques et les exigences de SAF et de SEC dans l'analyse et l'évaluation des risques des systèmes industriels. Les recherches dans le cadre de cette thèse ont été menées en quatre étapes principales, chacune apportant une contribution originale :

- L'élaboration d'une étude détaillée des approches existantes, suggérées par les deux communautés universitaires et industrielles, qui combinent les problématiques de la SAF et de la SEC pour l'évaluation conjointe des risques des ICSs. Une analyse critique a été menée afin de classer ces approches et d'identifier leurs lacunes et leurs faiblesses.

- Un système de notation ICVSS spécifique aux ICSs a été proposé qui satisfait plusieurs critères à savoir : quantitative/qualitative, aligne la SAF et SEC dans la même méthodologie, facilite la communication entre les équipes de la SAF et SEC. Nous avons appliqué la méthodologie proposée sur un cas d'étude d'un système à deux réservoirs. Des résultats qualitatifs et quantitatifs ont été obtenus, afin de montrer la capacité de la méthodologie proposée à modéliser les risques des vulnérabilités liées aux ICSs.

- Ensuite, un nouveau système de score appelé fuzzy ICVSS est introduit. L'avantage de ce système est sa capacité de modéliser les incertitudes et les ambiguïtés liées à la décision prise par l'expert.

- Le développement d'une méthodologie AMDEVEC & ER permet d'évaluer les risques des cyberattaques dans une démarche qui aligne et intègre la SAF et SEC en même

temps dans les premières phases de développement ou dans les phases d'exploitation. En effet, la méthodologie hybride des approches très populaires dans le domaine de la sûreté de fonctionnement : l'AMDEC, l'IEC/IEC 62443 et le CVSS. En outre, l'un des avantages majeurs de la méthodologie est sa capacité d'évaluer les systèmes complexes, car elle ne nécessite pas une modélisation fine du système. Enfin, l'AMDVEC & ER peut être utilisée dans différentes phases du cycle de vie du système :

- Dans la phase de conception pour concevoir des systèmes sûrs et sécurisés avec les exigences de SAF et de SEC appropriées. De même, notre méthodologie aide le concepteur à évaluer et à comparer les différentes configurations et mécanismes de protection de la SAF et de SEC avant de converger vers une architecture où les exigences de SAF et de SEC sont assurées ;
- Dans la phase opérationnelle pour évaluer les risques sur les systèmes existants, pour aider à définir de nouveaux mécanismes de SEC sans avoir nuire la SAF. En effet, ICVSS aide les analystes de risques à identifier les vulnérabilités du système (d'une façon permanente), à prévoir les événements indésirables et choisir les contre-mesures et la stratégie de défense appropriées.

6.1.2 Limites

Un inconvénient général de la méthode AMDEC est sa limitation de l'analyse à une cause unique d'un effet. De ce fait, certaines attaques en plusieurs étapes pourraient être négligées (l'aspect séquentiel est négligé). À ce propos, les méthodes séquentielles pourraient être particulièrement pertinentes (si plusieurs systèmes doivent être compromis afin d'atteindre un système cible). Les récentes approches qui combinent les arbres de fautes (FTA) et arbres d'attaque (ATA) pour une analyse combinée pourraient aider un AMDVEC &ER à couvrir ces limitations (Steiner and Liggesmeyer, 2013).

6.1.3 Perspectives

Les extensions suivantes du AMDVEC & ER peuvent être envisagées pour les futurs travaux :

- Les incidences sur la sûreté de fonctionnement ne sont pas exclusives les unes des autres, mais sont étroitement liées. Par exemple, une menace peut modifier les signaux de contrôle en violant leurs intégrités (D) ce qui provoque une défaillance du système qui pourrait en fin de compte affecter la disponibilité (A) du système. Cependant, dans un environnement industriel, il existe d'autres spécifications qui doivent être mentionnées comme : la Détection , l'Isolation et la Reconfiguration des erreurs. En conséquence, nous pourrons ajouter une autre métrique à notre méthodologie qu'on l'appelle la Fonctionnabilité (Fn) (Kumar et al., 2019) . Cette dernière permet de mesurer la capacité du système à reconfigurer (Re), Détecter (De), Isoler (Is) les erreurs provoquées par une éventuelle vulnérabilité ou par une défaillance.

- Utiliser les récentes approches qui combinent les arbres de fautes (FTA) et arbres d'attaque (ATA) pour une analyse combinée pourraient aider un AMDVEC & ER à couvrir ces limitations pour les attaques qui nécessitent plusieurs étapes.

- Continuer le travail sur l'influence de sécurité-innocuité sur sécurité-immunité et vice versa. En effet, à chaque fois qu'on fait des améliorations ou des solutions correctives, nous devons étudier leur impact sur les deux aspects, afin d'assurer les exigences de la sûreté de fonctionnement du système.

Enfin, ce travail s'appuie sur une étroite collaboration entre les experts en SAF et SEC et les aidera à mutualiser leurs efforts pour réduire les risques industriels et construire des systèmes à la fois sûrs et sécurisés.

Annexe A

Acronymes

ACT Attack Contermeasure Trees.

AFT Attacks Faults Tree.

AMDEC Analyse des Modes de Défaillance et de leurs Criticités.

AMDVEC Analyse des Modes de Défaillance et de Vulnérabilité, de leurs Effets et de leur Criticité et Évaluation des Risques.

ASIL Automotive Safety Integrity Level.

ATA Attack Tree Analysis.

AT-BT Attack Tree-Bow Tie.

BDMP Boolean logic Driven Markov Processes.

BLE Bluetooth Low Energy.

BN Bayesian Network.

CEI Commission Electrotechnique Internationale.

CHASSIS Combined Harm Assessment of Safety and Security for Information Systems.

CIM Computer Integrated Manufacturing.

CISA Cybersecurity and Infrastructure Security Agency.

CPS Cyber Physical System.

CVSS Common Vulnerability Scoring System (CVSS).

CYPSec Cyber-Physical Security.

DCS Distributed Control System(s).

D-MILS Distributed Multiple Independent Levels of Security.

DNPSec Distributed Network Protocol Security Framework.

DOA Difficulty Of the Attack.

DoS Denial of Service.

DST Dempster–Shafer Theory.

E/E ELECTRICAL/ ELECTRONIC.

ER Évaluation des Risques.

FMEA Failure Modes and Effects Analysis.

FMVEA Failure Modes, Vulnerabilities and Effect Analysis.

FPBN Fuzzy Probability Bayesian Network.

FT Fault Tree.

FTA Fault Tree Analysis.

GORE Goal-Oriented Requirements Engineering.

GSN Goal Structuring Notation.

GT Goal Tree.

GTST-MLD Goal Tree - Success Tree and Master Logic Diagram.

HARA HAzard and Risk Analysis.

HAZOP HAZard and OPerability.

HEAVENS HEAling Vulnerabilities to ENhance Software Security and Safety.

HMI Human-Machine Interface.

HTTP Hypertext Transfer Protocol.

IACS Industrial Automation Control System.

ICS Industrial Control System.

IDS Intrusion Detection System.

IEC International Electrotechnical Commission.

IED Intelligent Electronic Device.

IEEE Institute of Electrical and Electronics Engineers.

IFDs Diagrammes de Flux d'Information.

IHM Interface Homme-Machine.

IP Internet Protocol.

IS Information System.

ISA International Society of Automation.

ISO International Organization for Standardization.

IT Information Technology.

MBE Model-Based Engineering.

MCS Minimal Cut Sets.

MITM Man In The Middle.

MLD Master Logique Diagramme.

NFR Non-Functional Requirements.

NIAC National Infrastructure Assurance Council.

NIST National Institute of Standards and Technology.

NVD National Vulnérabilité Database.

OPC Open Platform Communications.

OPSEC OPerationnelle SECurity.

OT Opération Technologies.

PAP Password Authentication Protocol.

PERA Purdue Enterprise Reference Architecture.

PHA Process Hazard Analysis.

PLC Programmable Logic Controller.

RTU Remote Terminal Unit (also Remote Telemetry Unit).

SAE Society of Automotive Engineers.

SAHARA Security-Aware HAzard and Risk Analysis.

SCADA Supervisory Control and Data Acquisition.

SeCFTs Security Enhanced Component Fault Trees SeCFTs.

SGM Security Guideword Method.

SHS Stochastic Hybrid System.

SIL Safety Integrity Level.

SIS Safety Instrumented System.

SMC Semi Markov Chain.

SNMP Simple Network Management Protocol.

SPNs Stochastic Petri Nets.

SRA Security Risk Assessment.

ST Success Tree.

STAMP System-Theoretic Accident Model and Processes.

STLSA Systems Theoretic Likelihood and Severity Analysis.

STPA System Theoretic Process Analysis.

STRIDE Spoofing, Tampering Repudiation, Information, disclosure, Denial of service and Elevation of privilege.

SysML Systems Modeling Language.

TCP Transmission Control Protocol.

TVRA Threat Vulnerability and Risk Assessment.

UCE Unité de Contrôle Electronique.

UML Unified Modeling Language.

USB Universal Serial Bus.

WEP Wired Equivalent Privacy.

WPA Wi-Fi Protected Access.

Bibliographie

16, 127, 129

Common vulnerability scoring system sig. https://www.first.org/cvss. Accessed : 2020-10-19. 82

Complete CVSS v1 guide. https://www.first.org/cvss/v1/guide. Accessed : 2019-02-19. 20, 66, 70

Complete CVSS v2 guide. https://www.first.org/cvss/v2/guide. Accessed : 2019-02-19. 15, 83, 84

csrc.nist.gov. https://csrc.nist.gov/glossary/term/cyberspace#:~:text=Definition(s)%3A,and%20embedded%20processors%20and%20controllers. Accessed : 2020-01-21. 32

Explanation of cvss v2 formula and metric valued development. http://www.first.org/cvss/history. Accessed : 2020-10-30. 83, 85

ICS-CERT. https://ics-cert.us-cert.gov/. Accessed : 2019-02-20. 15, 33, 44, 45, 66, 70, 88, 91

NVD - vulnerability metrics. https://nvd.nist.gov/vuln-metrics/cvss. Accessed : 2019-12-20. 66

Symantec security response - severity assessment- symantec corp. https://www.symantec.com/security_response/severityassessment.jsp/. 2019-12-20. 66

Symantec security response - severity assessment- symantec corp. https://www.symantec.com/security_response/severityassessment.jsp. Accessed : 2019-02-19. 66

Symantec, severity assessment, threats, events, vulnerabilities, risks. https://www.symantec.com/content/en/us/about/media/securityintelligence/SSR-Severity-Assesment.pdf. Accessed : 2019-12-20. 66

United states computer emergency readiness team (us-cert). us-cert vulnerability note field descriptions. 2006. http://www.kb.cert.org/vuls/html/fieldhelp. Accessed : 2020-10-21. 71, 73

(2005). Les virus infomatique. *Club de la sécurité des systèmes informatique*. 42

61508, I. (2005). Functional safety of electrical/electronic/programmable electronic safety-related systems. *International Electrotechnical Commission*. 139

61511, I. (2004). Functional safety of electrical/electronic/programmable electronic safety-related systems. *International Electrotechnical Commission*. 139

A Ochang, P., Irving, P., and O Ofem, P. (2016). Research on wireless network security awareness of average users. *International Journal of Wireless and Microwave Technologies*, 6(2) :21–29. 86, 149

Abdo, H., Kaouk, M., Flaus, J.-M., and Masse, F. (2017). A new approach that considers cyber security within industrial risk analysis using a cyber bow-tie analysis. 19

Allodi, L., Banescu, S., Femmer, H., and Beckers, K. (2018). Identifying relevant information cues for vulnerability assessment using cvss. In *Proceedings of the Eighth ACM Conference on Data and Application Security and Privacy*, pages 119–126. 70

Amin, S. (2011). *On cyber security for networked control systems*. PhD thesis, UC Berkeley. 19

Anikin, I. (2017). Using fuzzy logic for vulnerability assessment in telecommunication network. In *2017 International Conference on Industrial Engineering, Applications and Manufacturing (ICIEAM)*, pages 1–4. IEEE. 70

Apvrille, L. and Roudier, Y. (2015). Designing safe and secure embedded and cyber-physical systems with sysml-sec. In *International Conference on Model-Driven Engineering and Software Development*, pages 293–308. Springer. 60, 64

Ariba, Y., Labit, Y., and Gouaisbaut, F. (2008). Network anomaly estimation for tcp/aqm networks using an observer. In *3rd ACM International Workshop on Feedback Control Implementation and Design in Computing Systems and Networks*, pages 3818–3823. Citeseer. 16, 144

Arlat, J., Crouzet, Y., Deswarte, Y., Fabre, J.-C., Laprie, J.-C., and Powell, D. (2006). Tolérance aux fautes. *Les Editions Vuibert, J. Akoka, I. Comyn-Wattiau (Eds)*, pages 241–270. 15, 39

Avizienis, A., Laprie, J.-C., Randell, B., and Landwehr, C. (2004). Basic concepts and taxonomy of dependable and secure computing. *IEEE transactions on dependable and secure computing*, 1(1) :11–33. 15, 36, 37, 38, 41

Balarin, F., Watanabe, Y., Hsieh, H., Lavagno, L., Passerone, C., and Sangiovanni-Vincentelli, A. (2003). Metropolis : An integrated electronic system design environment. *Computer*, 36(4) :45–52. 61

Banerjee, A., Venkatasubramanian, K. K., Mukherjee, T., and Gupta, S. K. S. (2011). Ensuring safety, security, and sustainability of mission-critical cyber–physical systems. *Proceedings of the IEEE*, 100(1) :283–299. 48, 50

Bieber, P., Blanquart, J.-P., Descargues, G., Dulucq, M., Fourastier, Y., Hazane, E., Julien, M., Léonardon, L., and Sarouille, G. (2012). Security and safety assurance for aerospace embedded systems. In *Proceedings of the 6th international conference on embedded real time software and systems (ERTS2), Toulouse, France*. 129

Braband, J. and Schäbe, H. (2019). A SEMI-FORMAL APPROACH TOWARDS LIKELIHOOD EVALUATION IN CYBERSECURITY RISK ASSESSMENT. In *29th European Safety and Reliability Conference (ESREL)*, page 6. 20, 103

Brissaud, F., Barros, A., Berenguer, C., and Charpentier, D. (2009). Reliability study of an intelligent transmitter. In *Proc. 15th ISSAT Int. Conf. Reliability and Quality in Design, San Francisco, United States,*, pages 224–233. 48

Brun, J., Platel, L., and Tea, F. (2013). Cyber security of industrial control system why ics specificity lead to cyber security challenge? *Proceedings of the Computer & Electronics Security Applications Rendez-vous*. 16, 26, 121

Byres, E. J., Franz, M., and Miller, D. (2004). The use of attack trees in assessing vulnerabilities in scada systems. In *Proceedings of the international infrastructure survivability workshop*, pages 3–10. Citeseer. 95

Carcano, A., Fovino, I. N., Masera, M., and Trombetta, A. (2008). Scada malware, a proof of concept. In *International Workshop on Critical Information Infrastructures Security*, pages 211–222. Springer. 96

Celikyilmaz, A. and Türksen, I. B. (2009). Modeling uncertainty with improved fuzzy functions. In *Modeling Uncertainty with Fuzzy Logic*, pages 149–215. Springer. 15, 104, 106, 107

CHEMALI, R., LARRIEU, N., CONDOMINES, J.-P., and MIQUEL, T. (2017). Mise en œuvre d'une méthode de détection d'intrusion dans une flotte de drones. Technical report, Ecole Nationale de l'Aviation Civile. 16, 145

Chen, T. M., Sanchez-Aarnoutse, J. C., and Buford, J. (2011). Petri net modeling of cyber-physical attacks on smart grid. 2(4) :741–749. 58

Chen, Y.-R., Chen, S.-J., Hsiung, P.-A., and Chou, I.-H. (2014). Unified security and safety risk assessment-a case study on nuclear power plant. In *2014 International Conference on Trustworthy Systems and Their Applications*, pages 22–28. IEEE. 53, 63

Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H., and Stoddart, K. (2016). A review of cyber security risk assessment methods for scada systems. *Computers & security*, 56 :1–27. 50

Chung, L., Nixon, B. A., Yu, E., and Mylopoulos, J. (2012). *Non-functional requirements in software engineering*, volume 5. Springer Science & Business Media. 58

Cimatti, A., DeLong, R., Marcantonio, D., and Tonetta, S. (2014). Combining mils with contract-based design for safety and security requirements. In *International Conference on Computer Safety, Reliability, and Security*, pages 264–276. Springer. 61, 64

Commission, I. E. et al. (2003). Iec 62264-1 enterprise-control system integration–part 1 : Models and terminology. *IEC, Genf*. 25

Commission, I. E. et al. (2006a). *Analysis Techniques for System Reliability : Procedure for Failure Mode and Effects Analysis (FMEA)*. International Electrotechnical Commission. 48, 53

Commission, I. E. et al. (2006b). Iec 61025 : Fault tree analysis (fta). *IEC Standards Online*. 62

Committee, I. C. S. L. S. et al. (2007). Ieee standard for information technology-telecommunications and information exchange between systems-local and metropolitan area networks-specific requirements part 11 : Wireless lan medium access control (mac) and physical layer (phy) specifications. *IEEE Std 802.11ˆ*. 149

Corporation, M. (2005). The stride threat model. 53

Cui, J. and Sabaliauskaite, G. (2018). Us^2 : An unified safety and security analysis method for autonomous vehicles. In *Future of Information and Communication Conference*, pages 600–611. Springer. 54, 65

Cui, J., Sabaliauskaite, G., Liew, L. S., Zhou, F., and Zhang, B. (2019). Collaborative analysis framework of safety and security for autonomous vehicles. *IEEE Access*, 7 :148672–148683. 54, 65

Di Maio, F., Mascherona, R., and Zio, E. (2019). Risk analysis of cyber-physical systems by gtst-mld. *IEEE Systems Journal*. 55, 63

D'souza, D. F. and Wills, A. C. (1998). *Objects, components, and frameworks with UML : the catalysis approach*. Addison-Wesley Longman Publishing Co., Inc. 60

Dunjó, J., Fthenakis, V., Vílchez, J. A., and Arnaldos, J. (2010). Hazard and operability (hazop) analysis. a literature review. *Journal of hazardous materials*, 173(1-3) :19–32. 48

Dürrwang, J., Beckers, K., and Kriesten, R. (2017). A lightweight threat analysis approach intertwining safety and security for the automotive domain. In *International Conference on Computer Safety, Reliability, and Security*, pages 305–319. Springer. 54, 64

Dürrwang, J., Braun, J., Rumez, M., Kriesten, R., and Pretschner, A. (2018). Enhancement of automotive penetration testing with threat analyses results. *SAE International Journal of Transportation Cybersecurity and Privacy*, 1(11-01-02-0005) :91–112. 55

Ebeling, C. E. (2004). *An introduction to reliability and maintainability engineering*. Tata McGraw-Hill Education. 48

(ETSI), E. T. S. I. (2007). Telecommunications and internet converged services and protocols for advanced networking (tispan) ; methods and protocols. *Standard*. 122

Fabro, M., Wells, R., Kuipers, D., Nelson, T., and Rohrbaugh, H. (2009). Using Operational Security (OpSec) to Support a Cyber Security Culture in Control Systems Environments. page 31. 27

Falliere, N. (2010). Exploring stuxnet's plc infection process. *Symantec blog entry, http ://www. symantec. com/connect/blogs/exploring-stuxnet-s-plc-infection-process*. 29

Ferson, S. and Ginzburg, L. R. (1996). Different methods are needed to propagate ignorance and variability. 54(2) :133 – 144. 102

Flaus, J.-M. (2018). Cybersécurité des installations industrielles-scada et industrial iot. 15, 17, 24, 25, 26, 31

for Electrotechnical, E. C. (2010). En50159 : Railway applications - communication, signalling and processing systems-safety-related communication in transmission systems. *Standard*. 122

for Standardization (DIN), G. I. (2013). Vde v 0831-102 :2013-12 : Electric signalling systems for railways - part 102 : Protection profile for technical functions in railway signalling. *pre Standard*. 122

for Standardization (DIN), G. I. (2015). Vde v 0831-104 :2015-10 : Electric signalling systems for railways - part 104 : It security guideline based on iec 62443. *Pre-Standard*. 122

Force, J. T. and Initiative, T. (2013). Security and privacy controls for federal information systems and organizations. *NIST Special Publication*, 800(53) :8–13. 122

Fovino, I. N., Carcano, A., Masera, M., and Trombetta, A. (2009). Design and implementation of a secure modbus protocol. In *International conference on critical infrastructure protection*, pages 83–96. Springer. 96

Francesco Di Maio, Roberto Mascherano, W. W. (2019). Ssimulation-based goal tree success tree for the risk analysis of cyber physical systems. In *29th European Safety and Reliability Conference (ESREL 2019)*, pages 4122–4129. ESREL. 56

Fraser, B. (2003). Rfc 2196. site security handbook. 1997. *URL : http ://www. faqs. org/rfcs/rfc2196. html*. 122

Friedberg, I., McLaughlin, K., Smith, P., Laverty, D., and Sezer, S. (2017). Stpa-safesec : Safety and security analysis for cyber-physical systems. *Journal of Information Security and Applications*, 34 :183–196. 57

Galichet, S. (2001). *Contrôle flou : de l'interpolation numérique au codage de l'expertise*. PhD thesis. 107

Gallon, L. and Bascou, J. J. (2011). Using cvss in attack graphs. In *2011 Sixth International Conference on Availability, Reliability and Security*, pages 59–66. IEEE. 70

Gibson, D. (2017). *CompTIA Security+ : Get Certified Get Ahead : SY0-501 Study Guide*. YCDA, LLC. 88, 149, 150

Gross, M. J. (2011). A declaration of cyber-war. *Vanity Fair*, 53(4). 29

Grunske, L., Colvin, R., and Winter, K. (2007). Probabilistic model-checking support for fmea. In *Fourth International Conference on the Quantitative Evaluation of Systems (QEST 2007)*, pages 119–128. IEEE. 48

Hernan, S., Lambert, S., Ostwald, T., and Shostack, A. (2006). Threat modeling-uncover security design flaws using the stride approach. *MSDN Magazine-Louisville*, pages 68–75. 136

Hoffman, F. O. and Hammonds, J. S. (1994). Propagation of uncertainty in risk assessments : the need to distinguish between uncertainty due to lack of knowledge and uncertainty due to variability. *Risk analysis*, 14(5) :707–712. 102

Hollot, C. V., Misra, V., Towsley, D., and Gong, W. (2002). Analysis and design of controllers for aqm routers supporting tcp flows. *IEEE Transactions on automatic control*, 47(6) :945–959. 16, 143

Howard, G., Butler, M., Colley, J., and Sassone, V. (2017). Formal analysis of safety and security requirements of critical systems supported by an extended stpa methodology. In *2017 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, pages 174–180. IEEE. 57, 63

Huang, K., Zhou, C., Tian, Y.-C., Tu, W., and Peng, Y. (2017). Application of bayesian network to data-driven cyber-security risk assessment in scada networks. In *2017 27th International Telecommunication Networks and Applications Conference (ITNAC)*, pages 1–6. IEEE. 58

Huang, K., Zhou, C., Tian, Y.-C., Yang, S., and Qin, Y. (2018). Assessing the physical impact of cyberattacks on industrial cyber-physical systems. *IEEE Transactions on Industrial Electronics*, 65(10) :8153–8162. 59

Initiative, J. T. F. T. et al. (2014). Guide for applying the risk management framework to federal information systems : A security life cycle approach. Technical report, National Institute of Standards and Technology. 122

ISA (2016a). Isa-62443 : Security for industrial automation and control systems. *Standard, International Society of Automaton*. 122

ISA (2016b). Security for industrial automation and control systems. standard, international society of automaton (isa). *Standard*. 122

Islam, M. M., Lautenbach, A., Sandberg, C., and Olovsson, T. (2016). A risk assessment framework for automotive embedded systems. In *Proceedings of the 2nd ACM International Workshop on Cyber-Physical System Security*, pages 3–14. 54, 64

ISO. (2009). *International Standard : Risk Management : Principles and Guidelines. ISO 31000. Principes Et Lignes Directrices*. ISO. 51

ISO, E. (2009). Iso/iec 15408-1 :2009 preview information technology – security techniques – evaluation criteria for it security – part 1. *Standard,*. 122

ISO, E. (2010). Iec 61508-1 :2010 : Functional safety of electrical/electronic/programmable electronic safety-related systems - part 1 : general requirements. *Standard*. 120

ISO, I. (2011). 26262 : Road vehicles-functional safety. *International Standard ISO/FDIS*, 26262. 53, 54

ISO, I. (2012). Iec 62645 - draft - draft document - nuclear power plants - instrumentation and control systems - requirements for security programmes for computer-based systems (iec 45a/890/cdv :2012. *Standard*. 127

ISO, I. (2013). Iso/iec 27001 :2013, information technology — security techniques — information security management systems — requirements. *Standard*. 127

ISO, I. (2016). Iso/iec 27000 : Prévisualiser technologies de l'information – techniques de sécurité – systèmes de gestion de sécurité de l'information – vue d'ensemble et vocabulaire. *Standard*. 122

Ito, M. (2014). Finding threats with hazards in the concept phase of product development. In *European Conference on Software Process Improvement*, pages 277–284. Springer. 60, 64

Johnson, P., Gorton, D., Lagerström, R., and Ekstedt, M. (2016). Time between vulnerability disclosures : A measure of software product vulnerability. *Computers & Security*, 62 :278–295. 65

Kennedy, R. and Kirwan, B. (1998). Development of a hazard and operability-based method for identifying safety management vulnerabilities in high risk systems. *Safety Science*, 30(3) :249–274. 48

Keramati, M. (2016). New vulnerability scoring system for dynamic security evaluation. In *2016 8th International Symposium on Telecommunications (IST)*, pages 746–751. IEEE. 70

Knowles, W., Prince, D., Hutchison, D., Disso, J. F. P., and Jones, K. (2015). A survey of cyber security management in industrial control systems. *International journal of critical infrastructure protection*, 9 :52–80. 122

Ko, J., Lim, H., Lee, S., and Shon, T. (2014). Avqs : attack route-based vulnerability quantification scheme for smart grid. *The Scientific World Journal*, 2014. 70

Kornecki, A. J., Subramanian, N., and Zalewski, J. (2013). 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*, pages 1393–1399. IEEE. 58, 63

Kriaa, S. (2016). *Joint safety and security modeling for risk assessment in cyber physical systems*. PhD thesis. 24, 26, 36, 51

Kriaa, S., Bouissou, M., Colin, F., Halgand, Y., and Pietre-Cambacedes, L. (2014). Safety and security interactions modeling using the bdmp formalism : case study of a pipeline. In *International Conference on Computer Safety, Reliability, and Security*, pages 326–341. Springer. 60, 64

Kriaa, S., Laarouchi, Y., and Bouissou, M. (2015). A model based approach for SCADA safety and security joint modelling : S-cube. Institution of Engineering and Technology. 49, 60, 64

Kumar, P., Bensekrane, I., Riad, C., Conrard, B., Toguyeni, A., and Merzouki, R. (2019). Functionability analysis of redundant systems having multiple configurations. In *2019 4th Conference on Control and Fault Tolerant Systems (SysTol)*, pages 282–287. IEEE. 154

Laprie, J.-C. (1985). Dependable computing and fault-tolerance. *Digest of Papers FTCS-15*, pages 2–11. 132

Lee, D., Lee, J., Cheon, S., and Yoo, J. (2013). Application of system-theoretic process analysis to engineered safety features-component control system. In *Proc. of the 37th Enlarged Halden Programme Group (EHPG) meeting*. 49

Li, X., Zhou, C., Tian, Y.-C., Xiong, N., and Qin, Y. (2017). Asset-based dynamic impact assessment of cyberattacks for risk analysis in industrial control systems. *IEEE Transactions on Industrial Informatics*, 14(2) :608–618. 59

Lundteigen, M. A. (2009). Safety instrumented systems in the oil and gas industry : Concepts and methods for safety and reliability assessments in design and operation. 16, 121

Macher, G., Armengaud, E., Brenner, E., and Kreiner, C. (2016). Threat and risk assessment methodologies in the automotive domain. *Procedia computer science*, 83 :1288–1294. 53

Macher, G., Höller, A., Sporer, H., Armengaud, E., and Kreiner, C. (2014). A combined safety-hazards and security-threat analysis method for automotive systems. In *International Conference on Computer Safety, Reliability, and Security*, pages 237–250. Springer. 53, 64

Macher, G., Sporer, H., Berlach, R., Armengaud, E., and Kreiner, C. (2015). Sahara : a security-aware hazard and risk analysis method. In *2015 Design, Automation and Test in Europe Conference Exhibition (DATE)*, pages 621–624. IEEE. 53

Mamdani, E. H. (1977). Application of fuzzy logic to approximate reasoning using linguistic synthesis. *IEEE transactions on computers*, (12) :1182–1191. 107

Manurung, D. T. (2020). Designing of user authentication based on multi-factor authentication on wireless networks. *Jour of Adv Research in Dynamical & Control Systems*, 12(1). 149

McQueen, M., Boyer, W., Flynn, M., and Beitel, G. (2006). Quantitative cyber risk reduction estimation methodology for a small SCADA control system. In *Proceedings of the 39th Annual Hawaii International Conference on System Sciences (HICSS'06)*, pages 226–226. IEEE. 66

Mell, P. and Scarfone, K. (2007). Improving the common vulnerability scoring system. 1(3) :119–127. 66

Mell, P., Scarfone, K., and Romanosky, S. (2007). A complete guide to the common vulnerability scoring system version 2.0. In *Published by FIRST-forum of incident response and security teams*, volume 1, page 23. 15, 71, 72

Modarres, M. and Cheon, S. W. (1999). Function-centered modeling of engineering systems using the goal tree–success tree technique and functional primitives. *Reliability Engineering & System Safety*, 64(2) :181–200. 48

Morris, T. H., Thornton, Z., and Turnipseed, I. (2015). Industrial control system simulation and data logging for intrusion detection system research. page 6. 35, 91

Nakashima, E. and Warrick, J. (2012). Stuxnet was work of us and israeli experts, officials say. *Washington Post*, 2 :13. 29

Naraine, R., Protalinski, E., and Danchev, D. (2010). Stuxnet attackers used 4 windows zero-day exploits. *ZDnet Blog*. 29

Nicklas, J.-P., Mamrot, M., Winzer, P., Lichte, D., Marchlewitz, S., and Wolf, K.-D. (2016). Use case based approach for an integrated consideration of safety and security aspects for smart home applications. In *2016 11th System of Systems Engineering Conference (SoSE)*, pages 1–6. IEEE. 61

Niemann, K.-H. (2017). It security in production facilities an introduction for small and medium-sized enterprises. Technical report. 16, 124

NIST (2012). Nist sp 800–30 revision 1, guide for conducting risk assessments. 14(2) :608–618. 53

Nourian, A. and Madnick, S. (2015). A systems theoretic approach to the security threats in cyber physical systems applied to stuxnet. *IEEE Transactions on Dependable and Secure Computing*, 15(1) :2–13. 48

Olovsson, T. (2018). Healing vulnerabilities to enhance software security and safety (heavens). 2015. *URL : https ://research. chalmers. se/en/project/5809 (besucht am 20*, pages 33–89. 55

Oracle (2020). docs.oracle.com. 150

Orojloo, H. and Azgomi, M. A. (2017a). A game-theoretic approach to model and quantify the security of cyber-physical systems. *Computers in Industry*, 88 :44–57. 20

Orojloo, H. and Azgomi, M. A. (2017b). A method for evaluating the consequence propagation of security attacks in cyber–physical systems. 67 :57–71. 59

Pereira, D., Hirata, C., Pagliares, R., and Nadjm-Tehrani, S. (2017). Towards combined safety and security constraints analysis. In *International Conference on Computer Safety, Reliability, and Security*, pages 70–80. Springer. 57, 63

Pietre-Cambacedes, L., Quinn, E. L., and Hardin, L. (2013). Cyber security of nuclear instrumentation & control systems : overview of the iec standardization activities. *IFAC Proceedings Volumes*, 46(9) :2156–2160. 127, 129

Pièrre-Cambacèdès, L. (2010). Des relations entre sûreté et sécurité. 20

Plósz, S., Schmittner, C., and Varga, P. (2017). Combining safety and security analysis for industrial collaborative automation systems. In *International Conference on Computer Safety, Reliability, and Security*, pages 187–198. Springer. 53, 64

Ponsard, C., Dallons, G., and Massonet, P. (2016). Goal-oriented co-engineering of security and safety requirements in cyber-physical systems. In *International Conference on Computer Safety, Reliability, and Security*, pages 334–345. Springer. 61, 64

Popov, P. T. (2014). Stochastic modeling of safety and security of the e-motor, an asil-d device. In *International Conference on Computer Safety, Reliability, and Security*, pages 385–399. Springer. 60, 64

Powell, D. and Stroud, R. (2003). Conceptual model and architecture for maftia. *School of Computing Science Technical Report Series*. 136

Procter, S., Vasserman, E. Y., and Hatcliff, J. (2017). Safe and secure : Deeply integrating security in a new hazard analysis. In *Proceedings of the 12th International Conference on Availability, Reliability and Security*, pages 1–10. 61, 64

Pub, F. (2004). Standards for security categorization of federal information and information systems. *NIST FIPS–199*. 122

PUB, F. (2006). Minimum security requirements for federal information and information systems. 122

Qu, Y. and Chan, P. (2016). Assessing vulnerabilities in bluetooth low energy (BLE) wireless network based IoT systems. In *2016 IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS)*, pages 42–48. IEEE. 67

Raspotnig, C., Karpati, P., and Katta, V. (2012). A combined process for elicitation and analysis of safety and security requirements. In *Enterprise, business-process and information systems modeling*, pages 347–361. Springer. 16, 61, 63, 128, 129

Rausand, M. (2013). *Risk assessment : theory, methods, and applications*, volume 115. John Wiley & Sons. 48

Reichenbach, F., Endresen, J., Chowdhury, M. M., and Rossebø, J. (2012). A pragmatic approach on combined safety and security risk analysis. In *2012 IEEE 23rd International Symposium on Software Reliability Engineering Workshops*, pages 239–244. IEEE. 56, 63

Rekik, M., Gransart, C., and Berbineau, M. (2018). Cyber-physical security risk assessment for train control and monitoring systems. In *2018 IEEE Conference on Communications and Network Security (CNS)*, pages 1–9. IEEE. 16, 121, 126, 138, 139

Roy, A., Kim, D. S., and Trivedi, K. S. (2012). Scalable optimal countermeasure selection using implicit enumeration on attack countermeasure trees. In *IEEE/IFIP International Conference on Dependable Systems and Networks (DSN 2012)*, pages 1–12. IEEE. 49

Ruijters, E., Schivo, S., Stoelinga, M., and Rensink, A. (2017). Uniform analysis of fault trees through model transformations. In *2017 Annual Reliability and Maintainability Symposium (RAMS)*, pages 1–7. IEEE. 62, 65

Sabaliauskaite, G. and Mathur, A. P. (2015). Aligning cyber-physical system safety and security. In *Complex Systems Design & Management Asia*, pages 41–53. Springer. 47

Sae, S. (2016). j3061, cybersecurity guidebook for cyber-physical vehicle systems. *Nr*, 1 :52. 54, 65

Sallhammar, K., Helvik, B. E., and Knapskog, S. J. (2006). On stochastic modeling for integrated security and dependability evaluation. 1(5) :31–42. 58

Sauter, T. (2007). The continuing evolution of integration in manufacturing automation. *IEEE Industrial Electronics Magazine*, 1(1) :10–19. 106

Scarfone, K. and Mell, P. (2009). An analysis of CVSS version 2 vulnerability scoring. In *2009 3rd International Symposium on Empirical Software Engineering and Measurement*, pages 516–525. IEEE. 66

Schmittner, C., Gruber, T., Puschner, P., and Schoitsch, E. (2014a). Security application of failure mode and effect analysis (fmea). In *International Conference on Computer Safety, Reliability, and Security*, pages 310–325. Springer. 16, 53, 63, 131, 132

Schmittner, C., Ma, Z., and Puschner, P. (2016). Limitation and improvement of stpa-sec for safety and security co-analysis. In *International Conference on Computer Safety, Reliability, and Security*, pages 195–209. Springer. 57, 63

Schmittner, C., Ma, Z., Schoitsch, E., and Gruber, T. (2015). 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*, pages 69–80. 49, 53

Schmittner, C., Ma, Z., and Smith, P. (2014b). Fmvea for safety and security analysis of intelligent and cooperative vehicles. In *International Conference on Computer Safety, Reliability, and Security*, pages 282–288. Springer. 57

Schwab, W. and Poujol, M. (2018). The state of industrial cybersecurity 2018. *Trend Study Kaspersky Reports*, page 33. 24

Shafer, G. (1976). *A Mathematical Theory of Evidence*. Princeton University Press. 102

Shapiro, S. S. (2016). Privacy risk analysis based on system control structures : Adapting system-theoretic process analysis for privacy engineering. In *2016 IEEE Security and Privacy Workshops (SPW)*, pages 17–24. IEEE. 57, 63

Silva, N. and Lopes, R. (2013). Practical experiences with real-world systems : Security in the world of reliable and safe systems. In *2013 43rd Annual IEEE/IFIP Conference on Dependable Systems and Networks Workshop (DSN-W)*, pages 1–5. IEEE. 62, 63

SIT, F. (2008). E-safety vehicle intrusion protected applications. 62, 65

Soerby, K. (2003). Relationship between security and safety in a security-safety critical system : Safety consequences of security threats. *NTNU, Trondheim, Norway, MSc thesis*. 120

Spanos, G., Sioziou, A., and Angelis, L. (2013a). Wivss : a new methodology for scoring information systems vulnerabilities. In *Proceedings of the 17th Panhellenic Conference on Informatics - PCI '13*, page 83. ACM Press. 66, 70

Spanos, G., Sioziou, A., and Angelis, L. (2013b). Wivss : a new methodology for scoring information systems vulnerabilities. In *Proceedings of the 17th panhellenic conference on informatics*, pages 83–90. 70

Steiner, M. and Liggesmeyer, P. (2013). Combination of safety and security analysis-finding security problems that threaten the safety of a system. 154

Steiner, M. and Liggesmeyer, P. (2014). Qualitative and quantitative analysis of cfts taking security causes into account. In *International Conference on Computer Safety, Reliability, and Security*, pages 109–120. Springer. 62, 64

Stouffer, K., Falco, J., and Scarfone, K. (2011). Guide to industrial control systems (ics) security. *NIST special publication*, 800(82) :16–16. 32

Subramanian, N. and Zalewski, J. (2014). Quantitative assessment of safety and security of system architectures for cyberphysical systems using the nfr approach. *IEEE Systems Journal*, 10(2) :397–409. 58

Takagi, T. and Sugeno, M. (1985). Fuzzy identification of systems and its applications to modeling and control. *IEEE transactions on systems, man, and cybernetics*, (1) :116–132. 107, 108

Tan, W., Marquez, H. J., Chen, T., and Liu, J. (2005). Analysis and control of a nonlinear boiler-turbine unit. *Journal of process control*, 15(8) :883–891. 111

Technica, A. (2012). Confirmed : Us and israel created stuxnet, lost control of it. *Wayback archive : http ://web. archive. org/web/20190424092854/https ://arstechnica. com/tech-policy/2012/06/confirmed-us-israel-created-stuxnet-lostcontrol-of-it*. 29

Temple, W. G., Wu, Y., Chen, B., and Kalbarczyk, Z. (2017). Systems-theoretic likelihood and severity analysis for safety and security co-engineering. In *International Conference on Reliability, Safety and Security of Railway Systems*, pages 51–67. Springer. 57, 65

Tran, T. D., Thiriet, J.-M., Marchand, N., El Mrabti, A., and Luculli, G. (2019). Methodology for risk management related to cyber-security of unmanned aircraft systems. In *2019 24th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*, pages 695–702. IEEE. 49

Troubitsyna, E. (2016). An integrated approach to deriving safety and security requirements from safety cases. In *2016 IEEE 40th Annual Computer Software and Applications Conference (COMPSAC)*, volume 2, pages 614–615. IEEE. 57, 64

Vilches, V. M., Gil-Uriarte, E., Ugarte, I. Z., Mendia, G. O., Pisón, R. I., Kirschgens, L. A., Calvo, A. B., Cordero, A. H., Apa, L., and Cerrudo, C. (2018). Towards an open standard for assessing the severity of robot security vulnerabilities, the robot vulnerability scoring system (RVSS). 67

Wei, J., Matsubara, Y., and Takada, H. (2015). Hazop-based security analysis for embedded systems : Case study of open. In *2015 7th International Conference on Electronics, Computers and Artificial Intelligence (ECAI)*, pages SSS–1. IEEE. 60, 64

Williams, T. J. (1989). A reference model for computer integrated manufacturing (cim). *International Purdue Works*. 25

Wolf, M. and Scheibel, M. (2012). A systematic approach to a qualified security risk analysis for vehicular it systems. *Automotive-Safety & Security 2012*. 45, 139

Wollschlaeger, M., Sauter, T., and Jasperneite, J. (2017). The future of industrial communication : Automation networks in the era of the internet of things and industry 4.0. *IEEE industrial electronics magazine*, 11(1) :17–27. 15, 104, 105

Xiang, Y., Wang, L., and Zhang, Y. (2014). Power system adequacy assessment with probabilistic cyber attacks against breakers. pages 1–5. IEEE. 59

Young, W. and Leveson, N. (2013). Systems thinking for safety and security. In *Proceedings of the 29th Annual Computer Security Applications Conference*, pages 1–8. 56, 57

Zadeh, L. (1999). Fuzzy sets as a basis for theory of possibility. *Fuzzy Sets and Systems*, 1 :9–34. 102, 104

Zadeh, L. A. (1965a). Fuzzy sets. 8(3) :338–353. 21

Zadeh, L. A. (1965b). Fuzzy sets. *Information and control*, 8(3) :338–353. 106

Zadeh, L. A. (1973). Outline of a new approach to the analysis of complex systems and decision processes. *IEEE Transactions on systems, Man, and Cybernetics*, (1) :28–44. 106

Zhang, H., Lou, F., Fu, Y., and Tian, Z. (2017a). A conditional probability computation method for vulnerability exploitation based on cvss. In *2017 IEEE Second International Conference on Data Science in Cyberspace (DSC)*, pages 238–241. IEEE. 70

Zhang, Q., Zhou, C., Tian, Y.-C., Xiong, N., Qin, Y., and Hu, B. (2017b). A fuzzy probability bayesian network approach for dynamic cybersecurity risk assessment in industrial control systems. *IEEE Transactions on Industrial Informatics*, 14(6) :2497–2506. 59

Zhang, Q., Zhou, C., Xiong, N., Qin, Y., Li, X., and Huang, S. (2015). Multimodel-based incident prediction and risk assessment in dynamic cybersecurity protection for industrial control systems. *IEEE Transactions on Systems, Man, and Cybernetics : Systems*, 46(10) :1429–1444. 59

Zhang, Y. (2015). Cybersecurity and reliability of electric power grids in an interdependent CyberPhysical environment. 87

Methodology oriented safety for the cybersecurity of industrial control systems

Abstract: The nowadays ICS (industrial Contrôle système) depends essentially on Operational Technologies (OTs) that have been acquired from a wide assortment of Information Technologies (ITs). In order to guarantee the ICSs requirement, several of ITs have adjusted or adapted. As a result, new issues appeared, in the design of this production systems, such as the integration of safety and security and risk of vulnerabilities. The greater part the ICSs vulnerabilities have generally not been considered in the design phase. However, this dependence on ITs makes ICS increasingly vulnerable to cyber-attacks and security threats, which affect their global performance. The focus of this thesis is to address the cyber security challenges faced by these systems. It adressed the features of the ICS threat environment and aligns safety and security risk analysis. After, a new vulnerability scoring system, called ICVSS (Industrial Control Vulnerability Scoring System) is introduced . This scoring system uses different approaches to score vulnerabilities of ICS, taking into account their characteristics. The ICVSS not only makes possible to assess the vulnerability or to ease the communication between the safety and security teams, but also it is a good alternative to replace the likelihood in order to be able to reuse safety methods to evaluate security risks. Moreover a new approach to co-analysis and co-assessment of safety and security is presented.
Keywords: Cybersecurity, Safety, Security, Risk assessment, Risk management, CVSS, ICS, ICVSS.

Méthodologie orientée sûreté de fonctionnement pour la cybersécurité des systèmes de contrôle-commande

Résumé : Aujourd'hui, les systèmes de contrôle industriels (ICS) dépendent essentiellement des technologies opérationnelles (OT) qui ont été acquises à partir d'une large panoplie de technologies de l'information (TI). Afin de garantir les exigences du ICS, plusieurs technologies de l'information ont été ajustées ou adaptées. En conséquence, de nouvelles problématiques sont apparues, dans la conception de ce système de production, tel que l'intégration de la sécurité-innocuité (Safety) et de la sécurité-immunité (Security) et le risque des vulnérabilités. La plupart des vulnérabilités dans ICS n'ont généralement pas été prises en compte dans la phase de conception. Cependant, cette dépendance vis-à-vis des systèmes informatiques classiques (ITs) rend les ICS de plus en plus vulnérables aux cyberattaques et aux menaces, ce qui affecte leurs performances globales. L'objectif de cette thèse est d'aborder les défis de la cybersécurité auxquels ces systèmes sont confrontés. Elle examine les caractéristiques de l'environnement de menace des ICS et aligne l'analyse des risques en matière de sécurité-innocuité et de sécurité-immunité. En fait, le premier problème de l'analyse des risques de sécurité est de déterminer la probabilité des cyberattaques sur une installation donnée. Ensuite, un nouveau système de notation des vulnérabilités, appelé ICVSS (Industrial Control Vulnerability Scoring System) est présenté . Ce système de notation utilise différentes approches pour noter les vulnérabilités des ICSs, en tenant compte de leurs caractéristiques. L'ICVSS permet non seulement d'évaluer la vulnérabilité ou de faciliter la communication entre les équipes de sécurité-innocuité et de sécurité-immunité, mais il constitue également une bonne alternative pour remplacer les probabilités afin de pouvoir utiliser les méthodes de sécurité-innocuité pour évaluer les risques de la sécurité-innocuité. De plus, une nouvelle approche de co-analyse et de co-évaluation de la sûreté et de la sécurité est présentée.
Mots clés :, Cybersécurité, Sécurité-innocuité, Sécurité-immunité, Gestion des risques, Évaluation des risques, CVSS, ICS, ICVSS.
