Un nouveau modèle pour générer les scénarios des attaques dans un système industriel pour une analyse des risques

Tamara Oueidat, Jean-Marie Flaus, François Masse

Institut pour la Maîtrise des Risques
Sûreté de Fonctionnement - Management - Cindyniques

Un nouveau modèle pour générer les scénarios des attaques dans un système industriel pour une analyse des risques

A new model to generate the attack scenarios in an industrial system for a risk analysis

OUEIDAT Tamara
Université Grenoble Alpes – Laboratoire G-SCOP
Grenoble, France
tamara.oueidat@grenoble-inp.fr

FLAUS Jean-Marie
Université Grenoble Alpes – Laboratoire G-SCOP
Grenoble, France
jean-marie.flaus@grenoble-inp.fr

MASSE François
INERIS – Direction des risques accidentels
Paris, France
francois.masse@ineris.fr

Résumé — La révolution des systèmes industriels et l'introduction des nouvelles technologies dans leurs systèmes de contrôle rendent les infrastructures vulnérables à des cyber attaques pouvant affecter la sûreté et le fonctionnement du système avec les situations accidentelles. L'analyse de ces attaques est devenue un sujet critique pendant l'analyse des risques, et il y avait un fort intérêt à développer des méthodes d'analyse des risques qui combinent la sûreté et la cyber sécurité dans la même analyse. Dans ce but, cet article représente une nouvelle méthode d'analyse des risques, permettant de générer les possibles scénarios des attaques qui peuvent survenir sur un système industriel systématiquement dans des nouveaux méta-modèles, et de les générer automatiquement en utilisant un code informatique dans le but de simplifier le processus de l'analyse des risques surtout pour les non experts dans le domaine de la cyber sécurité.

Mots-clefs — Cyber sécurité, Scénarios des attaques, Analyse des risques, Sûreté.

Abstract— The revolution of industrial systems and the integration of connected systems and digital technologies into their control systems make them vulnerable to new cybersecurity threats that affect the safety of the system with the hazardous situations. Analyzing these new threats becomes a crucial matter during risk analysis, and there is a strong interest in developing risk analysis approaches that combine safety and cybersecurity in the same analysis. For this purpose, this article represents a new risk analysis approach, which aims to generate and present the possible attack scenarios that can occur on an industrial system systematically in new meta-models, and to generate these scenarios automatically using a computerized code in order to simplify the risk analysis process especially for the no expert in the cybersecurity field.

Keywords — Cybersecurity, Attack scenarios, Risk analysis, Safety.

I. INTRODUCTION

La sûreté et la cyber sécurité pour les systèmes industriels sont deux concepts différents qui font référence à différents types de risques. Les situations accidentelles et les modes de défaillance désignent les risques de sûreté, tandis que les actes malveillants et les attaques représentent les risques pour la cyber sécurité. Au niveau de l'analyse des risques, ces deux types de risques peuvent conduire à des événements physiques redoutés identiques, de sorte qu'ils peuvent avoir des similitudes et des interdépendances [1]. Les systèmes industriels critiques, tels que la production d'énergie, production chimique, etc., dans les dernières années, sont devenus plus vulnérables à des cyber attaques et sont exposés à des nouvelles menaces de cyber sécurité qui pourrait affecter la sûreté et le fonctionnement du système, suite à l'introduction des nouvelles technologies telles que la convergence entre les deux parties informatique (IT) et opérationnelle (OT), la connexion à l'internet et à distance de leurs systèmes de contrôle et de gestion [2]. Par conséquent, la cyber sécurité est devenue une question importante, et ses risques doivent être pris en compte dans le processus d'analyse des risques et conjointement avec les risques de sûreté.

Cette combinaison des risques liés à la sûreté et à la cyber sécurité n'a pas été prise en considération et sont traités séparément dans la plupart des méthodes d'analyse des risques proposées au fil du temps. Des exemples de méthodes qui traitent des risques pour la sûreté sont les méthodes AMDEC [3], HAZOP [4], APR [5], ou nœud papillon [6]. Autres exemples pour les méthodes qui traitent des risques de cyber sécurité sont les méthodes EBIOS [2], CORAS [7], ou arbres d'attaque [8]. Récemment, l'importance de combiner les risques de sûreté et cyber sécurité en un seul processus d'analyse des risques a été reconnue, et de nombreuses méthodes d'analyse des risques ont été proposées et élaborées pour combiner la sûreté et la cyber sécurité. Dans la deuxième section des travaux relatifs, plusieurs méthodes développées sont répertoriées et catégorisées. Chacune de ces méthodes a ses avantages et il vaut mieux l'appliquer, mais cela peut aussi

avoir des limitations dans la modélisation de l'architecture physique et informatique du système industriel à analyser, ou au niveau de l'identification des scénarios d'attaques, ou au niveau de l'évaluation des risques combinés (vraisemblance et sévérité). L'objectif de cet article est d'introduire une nouvelle méthode d'analyse des risques combinant la sûreté et la cyber sécurité, offrant une nouvelle façon d'identifier les scénarios d'attaques, et générer automatiquement ceux qui existent dans un cas de test lorsque la méthode proposée est utilisée, puis les intégrer avec les risques de sûreté dans le même nœud papillon. La troisième section de cet article décrit le concept global de la méthode proposée, ainsi que les étapes de l'identification des scénarios d'attaques et leur génération automatique. La dernière section résume et conclut l'article avec des futurs travaux.

II. Travaux relatifs

Puisque l'importance de combiner la sûreté et la cyber sécurité a augmenté dans l'analyse des risques pour les systèmes industriels critiques, une transformation a été observée dans la proposition de méthodes d'analyse des risques avec des processus dans lesquels les concepts de la sûreté et la cyber sécurité sont considérés conjointement. Il y a plusieurs méthodes développées dont les processus permettent une extension des méthodes classiques d'analyse des risques de sûreté pour ajouter les risques de cyber sécurité, telles que FMVEA (adaptation AMDEC) [9], Cyber HAZOP [4], SECFT (adaptation CFT) [10], ou elles permettent une extension des méthodes d'analyse des risques de cyber sécurité afin d'ajouter l'aspect sûreté, telles que l'extension de la méthode TVRA [11]. D'autres méthodes développées sont sur le point de combiner les méthodes actuelles d'analyse des risques de sûreté et de cyber sécurité, telles que SAHARA [12], ATBT [13]. D'autres méthodes ont été développées à partir de zéro pour combiner les risques de sûreté et de cyber sécurité dans la même analyse, telles que S-cube [14], CHASSIS [15]. D'autres méthodes d'analyse des risques ont été développées et basées sur le processus de la méthode STPA, qui traite les accidents et les pertes comme un problème de contrôle, ainsi, un accident peut se produire en cas de défaillance d'un comportement de contrôle, et non pas comme une conséquence d'une défaillance [16]. Voici des exemples de cette catégorie de méthodes sont STPA-SafeSec [17], combinaisons de STPA avec STRIDE [18], et STPA-Sec avec FMVEA [19].

Chaque méthode d'analyse des risques développée présente ses avantages et elle est utile de l'appliquer, malgré l'existence de quelques limitations, soit dans la modélisation de l'architecture physique et informatique du système industriel qui représente une étape importante avant de commencer l'analyse, soit la manière de définir les scénarios d'attaques de façon non systématique et détaillée, soit le degré de détail et de complexité de l'application de la méthode d'analyse des risques. Dans notre travail, nous proposons une nouvelle méthode d'analyse des risques tenant compte des liens entre la sûreté et la cyber sécurité durant le processus d'analyse des risques, avec les principaux objectifs de couvrir les limitations des méthodes existantes et de faire les étapes pour définir les scénarios d'attaques plus simple et plus facile à appliquer avec un degré suffisant de détail, et en tenant compte du niveau d'expertise des utilisateurs dans le domaine de la cyber sécurité. La section suivante illustre notre méthode d'analyse des risques proposée avec la contribution de la génération automatique des scénarios d'attaques.

III. La methode d'analyse des risques proposee

Dans cette section, la méthode d'analyse des risques proposée est présentée afin de générer les scénarios d'attaques et les intégrer avec les risques de sûreté, de plus, cela simplifie les étapes du processus d'analyse des risques. Voici les principales étapes de notre méthode proposée :

- La modélisation de l'architecture de l'installation industrielle.
- La proposition d'un guide, une liste pour la recherche et la définition des vulnérabilités possibles.
- La proposition des nouveaux méta-modèles pour identifier les scénarios des attaques possibles.
- La génération automatique des scénarios des attaques.
- La combinaison des attaques générées avec les risques de sûreté dans le même méta-modèle.

Dans cet article, nous nous concentrons sur les étapes d'identification des scénarios d'attaques dans des méta-modèles, et de la génération automatique de ces scénarios pour un cas de test. Pour réaliser ces étapes, certaines données de l'installation industrielle doivent être recueillies, comme les composants de l'architecture du système, avec leurs attributs, tels que l'accès physique, la connexion à l'internet, les médias amovibles, la réception des emails, et les logiciels. Ces attributs peuvent révéler des vulnérabilités importantes sur le système industriel, et ils sont collectés à partir de l'inventaire et la cartographie du système industriel à analyser. Une autre donnée importante est une liste de vulnérabilités qui est identifiée à partir d'une check-list et d'un guide représentant les vulnérabilités génériques que l'on peut trouver sur les systèmes industriels. Les données de vulnérabilités sont collectées à partir des politiques organisationnelles et des barrières de sécurité qui sont en place et appliquées sur un système industriel. Par exemple, s'il n'existe pas une politique bien définie sur les accès physiques aux locaux, alors une vulnérabilité existe et peut-être exploiter dans le but d'exécuter un acte malveillant. Les données collectées aident à la création de simulations qui sont utilisées pour identifier automatiquement les scénarios d'attaques potentiels. Dans la section suivante, le principe de la méthode d'analyse des risques proposée est présenté. Ensuite, la façon d'identifier les scénarios d'attaques dans des méta-modèles, ainsi que la façon de les générer automatiquement sont expliquées.

A. Principe de la méthode proposée

La méthode d'analyse des risques s'appuie sur une base de connaissance, qui contient les données nécessaires à la génération des scénarios d'attaques, telles que, la liste définie des vulnérabilités, ainsi que les scénarios d'attaques génériques qui sont générés après dans la section suivante dans des méta-modèles. Les données génériques et les méta-modèles de la base de connaissance, ainsi que l'architecture du système (composants et attributs), fournissent des entrées pour la génération automatique de scénarios d'attaques, et ces

scénarios sont considérés comme les résultats du traitement automatique dans la méthode proposée.

Fig. 1 décrit le principe de la méthode d'analyse de risques proposée. Le traitement d'un algorithme à l'aide de données produites à partir des méta-modèles de scénarios d'attaques et d'autres entrées entraine la génération automatique de scénarios d'attaques existants dans un cas de test. Par conséquent, la contribution ici est de générer automatiquement des scénarios d'attaques et d'identifier les données nécessaires pour la base de connaissance. La section suivante explique comment déterminer les différents scénarios d'attaques qui peuvent exister sur un système industriel est abordée, ainsi que la génération automatique de scénarios.

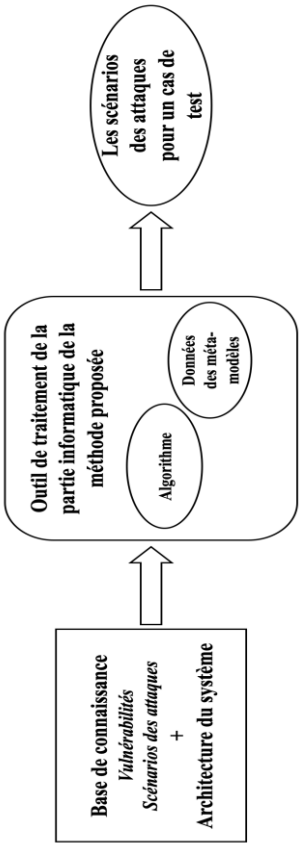

Fig. 1. Principe de la méthode proposée

B. Idnetification des scénarios d'attaques dans des méta-modèles

Pour exécuter une attaque, l'attaquant doit franchir une ou plusieurs étapes pour atteindre son but. Le point de départ pour une attaque est la surface d'attaques qui existe sur le composant ou sur n'importe quel niveau du système industriel. En fonction des attributs des composants, cinq surfaces d'attaques sont établies et peuvent être des sources de vulnérabilités conduisant à l'exécution d'attaques.

- Accès physique : L'attaquant peut utiliser un accès physique incontrôlé sur le système industriel pour obtenir un accès non autorisé et exécuter l'attaque.

- Réception des emails : Un composant du système industriel qui reçoit des emails de l'extérieur de l'industrie peut être utilisé pour exécuter des attaques par les emails phishing.

- Accès à distance : Si un composant peut être accédé par un poste connecté à distance sur le réseau du système industriel, il devient une cible pour les attaques, et surtout si l'accès est non protégé et non réglementé.

- Connexion à l'internet : Si un composant est connecté à l'internet, il peut devenir la cible pour les attaques si la connexion est mal ou non sécurisée.

- Un logiciel implémenté non sécurisé sur un composant peut être utilisé pour exécuter des attaques.

Les scénarios d'attaques sont générés dans des méta-modèles, un méta-modèle représente la séquence d'événements débutant avec la surface d'attaque arrivant à l'objectif de l'attaquant sous forme graphique. Chaque méta-modèle contient les surfaces d'attaques existantes sur les différentes zones d'un système industriel, et aussi les différentes étapes pour conduire une attaque à partir de chaque surface d'attaque. Le travail est concentré sur les trois niveaux de l'ICS avec les zones suivantes : Niveau physique (zone des équipements physiques), niveau de contrôle (deux zones : zone des PLC et zone des stations de programmation et de configuration), et niveau de supervision (zone du système SCADA et zone des stations des postes). Les niveaux de l'ICS dans le travail sont décomposés par des zones puisque sur le même niveau, chaque zone peut avoir différentes surfaces d'attaques avec différents niveaux de vulnérabilités. Les sorties de cette partie seront un catalogue de scénarios d'attaques qui peuvent être rencontrés sur un site industriel. L'objectif est de rechercher autant de scénarios génériques que possible afin de les associer à des risques de sûreté. Dans le domaine de la cyber sécurité, il est également impossible de couvrir toutes les attaques, puisque les sources des attaques ne sont pas bien connues par l'analyseur [1], il existe également la vulnérabilité 0-day, qui est une source inconnue d'attaques, sauf que l'attaquant en est conscient [20] et que les attaquants ont des profils et motivations différents [21]. Le méta-modèle dans lequel les scénarios d'attaques sont générés est représenté dans Fig. 2.

- Une attaque peut être interrompue par un ou plusieurs événements de sécurité. Un événement de sécurité peut avoir lieu comme un résultat de l'occurrence d'un ou plusieurs sous-événements de sécurité connectés par ET/OU, ou un événement de sécurité peut avoir lieu comme un événement initiateur du scénario d'attaque ou un événement complémentaire.

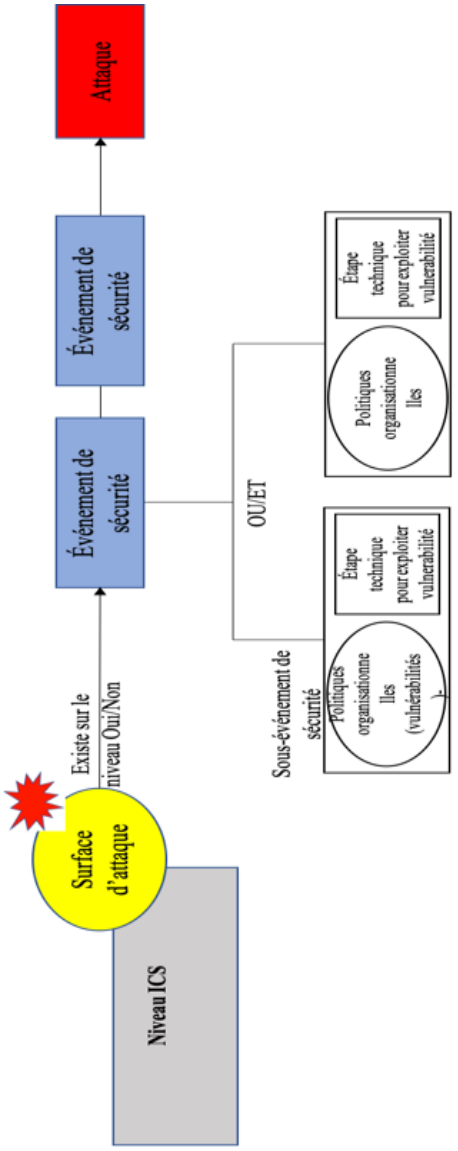

Fig. 2. Méta-moèle représentant la séquence d'un scénarios d'attaque

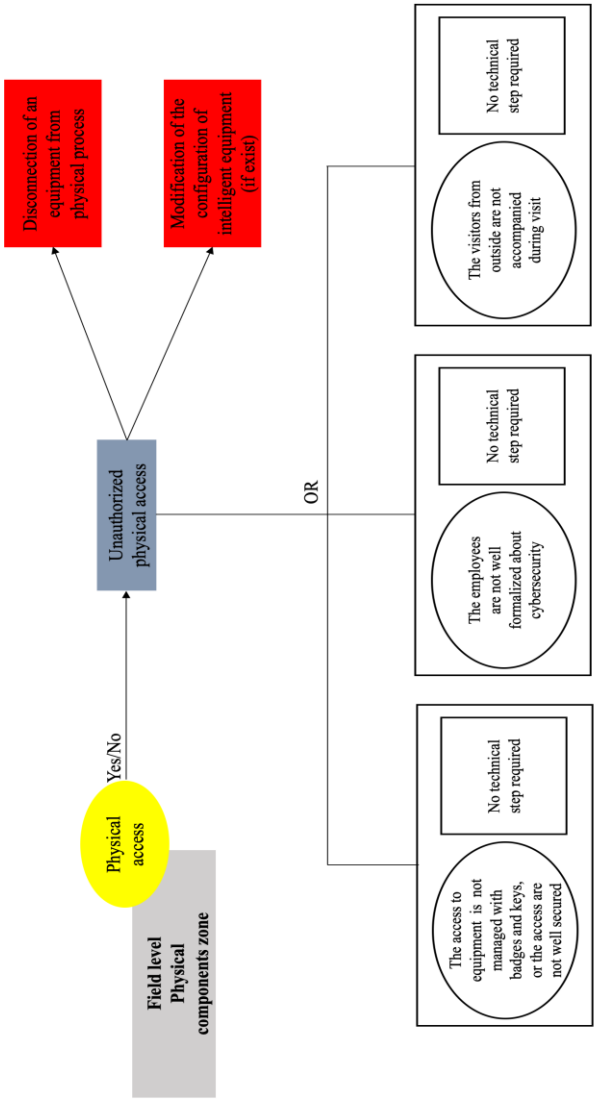

Fig. 3. Les scénarios d'attaques sur le niveau ohysique via l'accès physique

- Le sous-événement de sécurité dans le méta-modèle est une combinaison de la vulnérabilité et l'étape technique spécifique requise pour exploiter la vulnérabilité.

Les scénarios d'attaques possibles de chaque surface d'attaque et pour chaque zone des niveaux ICS sont générés à l'aide du méta-modèle expliquant ci-dessus. Dans le but de définir le plus nombre possible des scénarios d'attaques, la recherche était basée sur le cadre MITRE ATTACK [22]. Les scénarios d'attaques peuvent être modifiés selon l'application sur un cas de test (ajout des scénarios, des événements et des sous-événements de sécurité). Fig. 3 illustre un exemple de scénario d'attaque sur la zone de composants physiques du niveau physique à partir de la surface d'attaque d'accès physique. Fig. 4 représenta un autre scénario d'attaque via la surface de la réception des emails sur zone des stations au niveau de contrôle.

Pour effectuer une attaque par déconnexion d'un composant physique via un accès physique, l'attaquant doit d'abord obtenir un accès physique non autorisé à partir de l'un des sous-événements de sécurité suivants :

- L'attaquant peut exploiter une vulnérabilité existante sur l'accès physique aux locaux des composants, l'accès peut être sans badges ou clés sans aucune étape technique nécessaire pour exploiter la vulnérabilité.

- L'attaquant peut exploiter la vulnérabilité lors d'une visite non supervisée par un visiteur externe dans les locaux, et ainsi obtenir un accès non autorisé sans qu'aucune étape technique ne soit requise.

- Les employés qui sont mal formalisés à la cyber sécurité et les risques résultants peuvent être une source importante de vulnérabilité afin d'obtenir un accès non autorisé sans qu'aucune étape technique ne soit requise.

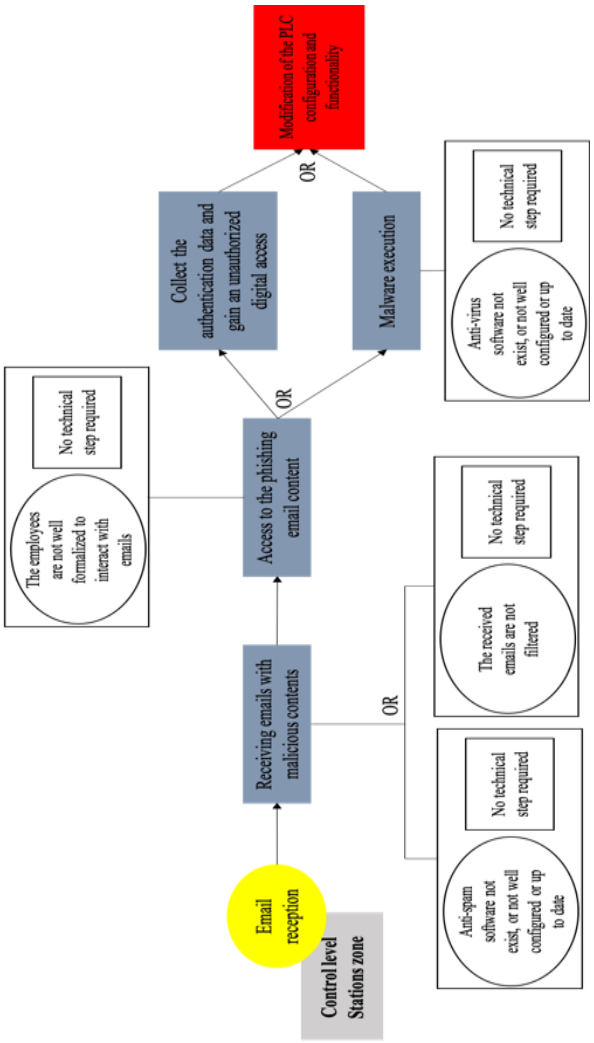

Fig. 4. Les scénarios d'attaques sur le niveau de contrôle via la réception des emails

Fig. 4 présente comment un attaquant peut modifier la configuration ou la fonctionnalité du PLC en envoyant un email à la station appropriée. L'attaquant envoie un email avec un contenu malveillant sans aucune étape technique comme une première étape, en exploitant l'une des deux vulnérabilités suivantes :

- Aucun logiciel anti spam installé sur la station ne peut empêcher ces types d'emails d'être reçu.
- Les emails reçus sur la station de configuration ne sont pas filtrés.

Une fois la station reçoit un email avec un contenu malveillant, un employé qui n'est pas formé à la cyber sécurité peut le voir et potentiellement être affecté par celui-ci en accédant au contenu de l'email (virus, malveillants sites web, etc.). Après avoir accédé à ce contenu, l'attaquant peut voler les données d'authentification et les utiliser pour obtenir un accès logique non autorisé à la station, ou l'attaquant peut installer un logiciel malveillant sur la station en exploitant une vulnérabilité qui peut être présente dans le logiciel antivirus implémenté sur la station (pas d'antivirus, ou il n'est pas à jour) pour empêcher le logiciel malveillant d'être exécuté. Dans la partie suivante, l'algorithme de la génération automatique des scénarios d'attaques sera fourni.

C. Algorithme pour la génération automatique des scénarios des atatques

L'objectif principal de la génération automatique de scénarios d'attaques à l'aide de la méthode proposée est de faciliter les étapes de la recherche de scénarios d'attaques possibles, surtout pour les utilisateurs qui non experts dans le domaine de la cyber sécurité. Cette génération permet une application simple du processus d'analyse avec un niveau suffisant de détail pour les scénarios d'attaques en limitant la complexité et le coût en temps de l'analyse des risques. Afin de réaliser cette étape, les données du KB de la partie A sont nécessaires dans le but d'exécuter un algorithme et obtenir les scénarios d'attaques potentiels comme des données de sortie. Deux catégories des données d'entrée sont à considérer :

- Les données des méta-modèles des scénarios d'attaques générés à l'étape précédente, qui sont des données fixes et identiques dans tous les cas d'études de l'analyse des risques des systèmes industriels. Ces données comprennent les différentes zones des niveaux de l'ICS, la liste générée des vulnérabilités, les différentes surfaces d'attaques, toutes les séquences et les schémas des évènements et sous-événements de sécurité, et toutes les relations entre eux afin de réaliser une attaque.

- Le deuxième type de données est celui qui doit être complété par l'utilisateur en utilisant la méthode d'analyse des risques. L'utilisateur doit compléter les niveaux d'applicabilité des politiques organisationnelles appliquées sur les différentes zones des niveaux ICS, ainsi que les surfaces d'attaques existantes sur chaque zone en fonction de l'étude de cas.

Les deux types de données d'entrée pour l'algorithme sont convertis en fichiers dans un format d'échange de données, qui seront utilisés dans un code développé pour générer automatiquement les scénarios d'attaques existants comme données de sortie dans le même format de données d'entrée.

En arrivant à cette étape de la méthode, les événements redoutés qui peuvent avoir lieur sur un site industriel sont répertoriés avec leurs situations accidentelles représentant des risques de sûreté à partir d'une méthode d'analyse conventionnelle, et la liste des attaques possibles qui peuvent avoir lieu est établie représentant des risques de cyber

sécurité. Dans le reste de l'approche, ces deux types de risques qui peuvent conduire à la survenue du même événement redouté sont combinés dans le même nœud papillon, appelé dans notre approche Cyber Bow-Tie. La vraisemblance d'occurrence des risques combinés est évaluée, et finalement, les risques combinés inacceptables sont pris en compte en proposant des mesures de sûreté et de sécurité dans le but de minimiser les criticités de ces risques.

D. Exemple et résultats

Cette partie comprend un exemple pour démontrer les étapes de la méthode d'analyse des risques proposée. L'exemple présente un cas d'étude d'un système de polymérisation. Le niveau physique de ce système est composé de différents capteurs, vannes, pompes pour réaliser une réaction chimique, et ils sont accessibles physiquement. Ces composants physiques sont contrôlés par un PLC au niveau de contrôle, et ce PLC peut être accédé à distance de l'extérieur du système industriel, et il est configuré sur une station de configuration au niveau de contrôle. Cette station est accessible physiquement, a également un accès à distance de l'extérieur, et elle est implémentée par des logiciels tels que le système d'exploitation et l'anti-virus. Les niveaux physique et de contrôle sont supervisés par un système SCADA contenant un serveur doté d'une base de données, et une station de supervision. Ces composants sont accessibles physiquement. De plus, au niveau de supervision, plusieurs postes existent et sont connectés à l'internet, possèdent des accès à distance, ils reçoivent des emails de l'extérieur de l'industrie et ils sont implémentés par une variété de logiciels.

Dans cette étude de cas, un nœud papillon est utilisé pour présenter et analyser les différents scénarios de risque de sûreté résultant à l'occurrence d'un événement redouté critique, tel qu'un rejet toxique dans l'atmosphère. En plus des risques liés à la sûreté, les problèmes et les questions de cyber sécurité devraient être abordés pour ce cas de test. Les composants sont modélisés correctement avec leurs attributs dans des tableaux, et la liste générée des vulnérabilités est validée pour ceux qui existent pour ce cas de test. Pour l'étape de la recherche de scénarios d'attaques possibles, pour chaque zone du niveau ICS, les surfaces d'attaques existantes sont définies ci-dessous avant de lancer la génération automatique.

- La zone des composants physiques (niveau physique) : accès physique.
- La zone du PLC (niveau de contrôle) : accès physique, accès à distance, software.
- La zone des stations (niveau de contrôle) : accès physique, accès à distance, software.
- La zone de supervision (niveau de supervision) : accès physique.
- La zone des postes (niveau de supervision) : accès physique, accès à distance, connexion à l'internet, réception des emails, software.

L'algorithme développé utilise les données de surfaces d'attaques définies, ainsi que les données de méta-modèles de scénarios d'attaques, pour définir ceux qui existent dans chaque zone pour ce cas de test. La station de configuration, par exemple, n'est pas connectée à l'internet, il n'y a donc pas dans cette zone de possibilité d'attaques via la connexion à l'internet. Les données de sortie de cet algorithme sont toutes les séquences d'événements de sécurité pour chaque zone et chaque surface d'attaque pour ce cas de test, ainsi que toutes les attaques qui peuvent intervenir comme un résultat de ces séquences d'événements de sécurité, en plus, toutes les combinaisons de vulnérabilités et d'étapes techniques représentant les sous-événements de sécurité pour chaque événement de sécurité. La dernière partie présente une conclusion de cet article avec des futurs travaux.

IV. CONCLUSION ET FUTUR TRAVAIL

Le besoin d'intégrer la sûreté et la cyber sécurité dans l'analyse des risques pour les systèmes industriels critiques est de plus en plus grand. Ces industries ont fait l'objet à des nouvelles menaces de cyber sécurité en raison de l'intégration de nouvelles technologies dans leurs systèmes de contrôle, ces menaces peuvent avoir des répercussions sur la sûreté et le fonctionnement du système industriel. Donc, en plus des problèmes de sûreté, les industries doivent être sensibilisées aux risques associés à la cyber sécurité. Plusieurs auteurs ont suggéré et développé des méthodes visant à inclure la sûreté et la cyber sécurité dans l'analyse des risques. Toutefois, pour identifier et analyser les scénarios d'attaques critiques du point de vue de la sûreté et la sécurité des êtres humains et de l'environnement, une stratégie d'analyse des risques basée sur les meilleures caractéristiques et les processus d'analyse choisis des méthodes existantes [23] est nécessaire.

Dans cet article, nous avons présenté notre méthode d'analyse des risques proposée. Elle met l'accent sur la fusion claire et directe de l'analyse des risques de sûreté et de cyber sécurité, avec le plus nombre possible des scénarios d'attaques. Son processus dans la recherche et la génération de la liste des vulnérabilités et des scénarios d'attaques se diffère des autres méthodes existantes. Les scénarios d'attaques sont générés automatiquement en se basant sur une base de connaissance KB comme des données d'entrée, contenant les méta-modèles de scénarios d'attaques avec les données collectées de l'installation industrielle. Dans cet article, le processus de la génération des attaques a été discuté, ainsi que la façon de les générer automatiquement. Les étapes restantes de la méthode proposée représentent l'intégration des risques de cyber sécurité avec les risques de sûreté dans un même nœud papillon, ainsi que l'évaluation de la vraisemblance des risques combinés et leur traitement pour minimiser leurs criticités. L'objective d'introduire une nouvelle méthode d'analyse des risques est de simplifier les étapes du processus de l'analyse des risques surtout pour les utilisateurs non experts dans le domaine de la cyber sécurité. Pour des futurs travaux, la méthode proposée sera illustrée sur un cas de test réel d'un système de polymérisation chimique. En plus, nous allons améliorer les futures recherches pour l'intégration de l'évaluation de la vraisemblance de chaque scénario d'attaque dans le même algorithme de la génération des scénarios d'attaques.

REFERENCES

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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