Classification des principales méthodes d'analyse des risques combinant la sécurité et la sûreté

Tamara Oueidat, Jean-Marie Flaus, François Massé

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

Classification des principales méthodes d'analyse des risques combinant la sécurité et la sûreté

Classification of principles risk analysis approaches combining security and safety

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

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

François Massé
Direction des Risques Accidentels
INERIS
Paris, France
francois.masse@ineris.fr

***Résumé*—Les systèmes industriels utilisent des technologies issues de l'informatique et sont de plus en plus vulnérables à des cyberattaques pouvant affecter l'environnement et les humains. L'article présente et classifie des méthodes intégrant l'analyse des risques de sûreté et de sécurité de ces systèmes.**

***Abstract*—Industrial systems use Information Technology (IT)-based technologies and are increasingly vulnerable to cyberattacks that can have human or environmental consequences. The article presents and classifies methods that integrate safety and security in risk analysis of these systems.**

Mots clés—Sûreté, Cyber sécurité, Événement indésirable, Analyse des risques

I. INTRODUCTION

Les exploitants des installations classées, de l'industrie chimique par exemple, doivent maîtriser les risques que leurs installations font peser sur les personnes et l'environnement. Ces risques sont identifiés par les risques liés à la sûreté dans la suite de cet article. Leurs causes aléatoires et accidentelles sont généralement couvertes par des méthodes d'analyse. La protection contre les actes malveillants pouvant avoir des conséquences graves pour l'installation ou son environnement, c'est la sécurité. Des événements de sécurité peuvent avoir des conséquences pour la sûreté. Pour les actes malveillants visant les systèmes informatiques, les termes « cyberattaque » et « cyber sécurité » seront utilisés.

Les systèmes industriels intègrent de plus en plus de technologies numériques et communicantes dans les systèmes de contrôle automatisés comme par exemple l'utilisation des objets connectés (Industrial Internet of Things IIoT), la convergence technologique et l'interconnexion entre Information Technology IT et Operational Technology OT, ou la connexion à l'internet et à distance des systèmes de contrôle et de gestion [1]. Malgré les avantages de cette numérisation, elle rend les infrastructures vulnérables à des cyberattaques et augmente la surface de ces attaques et pouvant affecter la sûreté du système. Par conséquent, la cyber sécurité est devenue un sujet critique dans les systèmes de contrôle industriels (ICS), tels que ceux des industries de production d'énergie ou des industries chimiques [2]. Les industries à risque se concentrent sur le sujet de sûreté sans nécessairement prendre en considération qu'une cyberattaque peut affecter la sûreté du système. Récemment, plusieurs incidents de sécurité, affectant les installations industrielles, ont été observés tels que NotPeya ou TRITON [3]. Les industries doivent se sensibiliser aux risques liés à la cyber sécurité.

Il y a un fort d'intérêt aux développements de méthodes d'analyse des risques combinant la sécurité et la sûreté. Elles doivent être adaptées aux technologies, aux domaines d'application et aux types de risques considérés. Un grand nombre de méthodes ont été proposées, la plupart de ces méthodes évaluent séparément les risques liés à la sécurité et à la sûreté [4], malgré les interdépendances et les conséquences communes. Des exemples d'approches d'analyse des risques pour la sûreté sont les méthodes FMEA [5], APR [1], Nœud Papillon [6] ou HAZOP [7], les trois dernières méthodes sont utilisées en particulier dans le contexte réglementaire français et pour la sécurité sont les arbres d'attaques [8], EBIOS [1] ou CORAS [9]. En revanche, dans le contexte réglementaire français, aucune méthode spécifique ne s'impose pour l'analyse des événements de sécurité ayant des conséquences de sûreté. Récemment, plusieurs méthodes d'analyse des risques intégrant la sécurité et la sûreté ont été proposées dans le but d'avoir une analyse complète des risques. Dans cet article, la deuxième section présente des travaux sur ce sujet, suivie d'une revue de certaines méthodes d'analyse des risques et leur application sur un cas de test dans la troisième section. La quatrième section présente une classification multicritère de ces méthodes analysées. La dernière section présente une conclusion et une synthèse de cette étude.

II. TRAVAUX RELATIFS

De nombreux travaux de recherche portent sur des revues des méthodes d'analyse des risques combinant la sécurité et la sûreté. Lisova et al. [10] ont présenté l'analyse de certaines méthodes afin de les mieux comprendre et de

présenter le type d'intégration qu'elles utilisent. Chaque méthode a été classifiée en se basant sur sa relation avec l'industrie, son domaine d'application et si les traitements de la sûreté et la sécurité sont en parallèle ou non. Chockalingam et al. [11] ont présenté une revue des méthodes d'analyse des risques intégrant la sécurité et la sûreté, leur analyse a été basée sur les critères suivants : la citation dans la littérature scientifique, les étapes impliquées du processus d'analyse des risques, les domaines d'application et la méthode d'intégration. Cherdantseva et al. [12] ont présenté une revue des méthodes d'analyse des risques liés à la cyber sécurité pour les systèmes SCADA, ils ont comparé les méthodes en se basant sur les critères suivants : le nombre de citations, le niveau de détail, la méthode basée sur une formule ou dirigée par un modèle, l'utilisation d'une analyse quantitative ou qualitative, les sources de données pour le calcul des probabilités, le but et le domaine d'application. Kriaa et al. [13] ont décrit plusieurs méthodes génériques considérant la sûreté et la sécurité au niveau détaillé dans l'évaluation des risques et ont présenté certaines méthodes dirigées par des modèles fondés sur la représentation des aspects fonctionnels ou non fonctionnels du système. Ils ont classifié les méthodes analysées en se basant sur les critères suivants : la méthode intégrée ou unifiée, l'application d'une analyse qualitative ou quantitative et les phases couvertes du cycle de vie du système. Toutes ces publications présentent en conclusion une synthèse des résultats.

Dans notre travail, nous présentons un panorama plus large d'autres méthodes d'analyse des risques mixtes, puis les appliquons sur un cas de test (système de production de bière) et les classifions en se basant sur les critères et les caractéristiques regroupés des revues, en ajoutant si l'analyse est simple ou détaillée. Nos résultats seront basés sur l'application de l'étude de cas. Dans la section suivante, l'étude de cas et les méthodes d'analyse des risques sont présentées.

III. METHODES D'ANALYSE DES RISQUES INTEGREES

Premièrement, nous allons décrire l'étude de cas présentant un site industriel pour la production de la bière artisanale. Les systèmes de fermentation et de stérilisation interagissent entre eux pour produire de la bière, dans des meilleures conditions d'hygiène optimales. Les vannes, les capteurs et les actionneurs de ces systèmes sont contrôlés par un automate PLC et supervisés par un système SCADA, qui possède un accès à distance. Un site e-commerce pour les achats en ligne est implémenté sur un serveur web connecté à l'internet. Fig. 1 représente le schéma de ce système. Dans la phase de fermentation, les ingrédients interagissent entre eux dans le fermenteur pour produire la bière. Le capteur S1 est utilisé pour mesurer le niveau de l'eau dans le fermenteur et envoie les données collectées au PLC, qui compare la quantité d'eau nécessaire pour cuire la bière avec les données collectées et envoie un signal de contrôle à la vanne V1 pour faire passer la quantité d'eau nécessaire. La phase de stérilisation consiste à nettoyer le fermenteur avec une certaine pression, le capteur S2 est utilisé dans le fermenteur pour mesurer s'il est vide ou non. S'il est vide, la vanne V2 reçoit un signal de contrôle du PLC pour injecter la vapeur dans le fermenteur, jusqu'à atteindre une pression spécifique. S'il n'est pas vide, la vanne V3 reçoit un signal de contrôle pour le vider.

Différents événements indésirables peuvent avoir un impact critique sur le système : Dans le cas d'augmentation de la pression dans le fermenteur, si V2 n'agit pas correctement, un éclatement du fermenteur peut se produire ; Altération des données (configuration), provoquant un mauvais fonctionnement des vannes et des capteurs ; Indisponibilité du site e-commerce, provoquant une perte de crédibilité et des pertes financières.

La sûreté et la sécurité peuvent être intégrées : une cyberattaque peut impacter le serveur SCADA et affecter l'intégrité des données échangées avec le PLC, menant à un mal fonctionnement du système de stérilisation en fonction de la pression et causant un incendie. En revanche, il est également possible d'identifier des conflits entre les mesures de sûreté et de sécurité, par exemple [14], une porte avec des accès limités au processus de production : pour des raisons de sécurité, la porte doit être fermée pour prévenir les accès non autorisés et pour des raisons de sûreté elle doit être ouverte pour intervenir en cas d'un incendie.

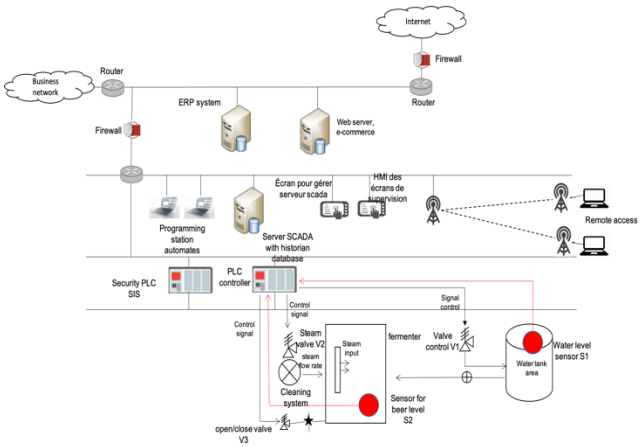

Fig. 1. Le système de production de bière

Dans la suite, les méthodes d'analyse des risques de sûreté et de sécurité sont présentées, dans le but d'expliquer leurs processus pour définir et analyser les risques, puis elles sont illustrées en les appliquant sur le système de production de bière pour les classifier et les comparer.

Les méthodes d'analyse des risques à présenter ont été choisies parmi les plus récentes et les plus représentatives des trois grandes catégories : Extension des méthodes d'analyse tabulaire classiques, Extension des méthodes décrivant les scénarios de dangers et d'attaques sous forme de chaines d'événements, Extension de la méthode STPA.

A. *Extension des méthodes d'analyse classiques*

Cette catégorie de méthodes se base sur des méthodes d'analyse des risques de sûreté classiques, en ajoutant l'aspect de sécurité comme une cause menant à des situations de danger. Les méthodes classiques les plus utilisées sont du type APR (Analyse Préliminaire des Risques), AMDEC (Analyse des Modes de Défaillance, leurs Effets et Criticité), et HAZOP (HAZard and OPerability analysis). Les méthodes d'analyse des risques combinant la sûreté et la sécurité appartenant à cette catégorie sont les suivantes :

1) Security Guidewords Method

La méthode SGM [15] est une extension de la méthode HAZOP, à laquelle sont intégrées pour chaque mot-clé les menaces de sécurité. SGM permet une identification

structurée des objectifs de protection, qui peuvent être utilisés dans l'analyse de la sécurité. Les situations de menaces et de dangers sont classifiées en utilisant les paramètres de l'ISO 26262 pour l'analyse des dangers.

Les étapes de SGM sont les suivantes : **1**. Définir les entités, les flux de données entre les entités et les besoins de sûreté ; **2**. Définir un ensemble des mots-clés de défaut (fault-type) en basant sur la méthode HAZOP, comme présenté dans la TABLE I. ; **3**. Créer une liste des situations opérationnelles en se basant sur des analyses historiques ; **4**. Identifier les situations de danger pour chaque défaut (TABLE I.) ; **5**. Instancier des mots-clés de sécurité et identifier les objectifs de protection, en présentant les menaces de sécurité pour chaque défaut, comme présenté dans la TABLE II. ; **6**. Identifier la sévérité S, l'exposition E et la contrôlabilité C pour chaque situation de danger identifiée en conformité par ISO 26262 ; **7**. Classifier les menaces en utilisant la sévérité des situations de danger en relation, en se basant sur le défaut sélectionné ; **8**. Définir les besoins de sécurité et de sûreté en se basant sur les objectifs de protection.

Pour l'application sur le système de production de bière, le système de stérilisation est analysé, avec deux exigences de sécurité principales (B). Les TABLE I. et TABLE II. présentent les situations de danger avec les relations avec les menaces.

- B1- le fermenteur sera nettoyé sauf s'il est vide.
- B2- la vanne de vapeur devra être fermée quand la pression atteint un taux spécifique.

Pour des besoins de sécurité, le PLC doit être protégé des accès non autorisés, pour diminuer l'exposition aux attaques modifiant les données échangées entre le PLC et la vanne.

TABLE I. MOTS CLES AVEC LES SITUATIONS DE DANGER

Défaut ID	Défaut
1	No fermeture
2	Plus de pression

ID	Danger	S	E	C	ASIL ISO 26262
1	Augmentation de pression	S3	E2	C3	C
2	Pas du système stérilisation	S0	E3	C2	B

TABLE II. RELATIONS ENTRE LES MENACES DE SECURITE ET LES DEFAUTS

Menace ID	Défaut ID	Type de l'attaque	Signal ou fonction	Composant ou sous-système	Point d'accès	Classification
1	1	Déclenchement	Fermeture de vanne	Système de stérilisation	PLC	C
2	1	Modification	Fermeture de vanne	Système de stérilisation	Station de programmation	C

2) Security-Aware Hazard and Risk Analysis

La méthode SAHARA [16] est une combinaison des méthodes HARA (basée sur les méthodes APR et AMDEC) et STRIDE [17]. L'ajout de l'analyse de sécurité par STRIDE améliore l'exhaustivité de l'analyse de HARA, en intégrant des facteurs des menaces de sécurité d'une manière plus structurée.

Les étapes de la méthode sont les suivantes : **1**. Identifier les événements de danger potentiel en utilisant HARA, les classifier en se basant sur Automotive Safety Intergrity Levels ASIL et déterminer leurs gravités, leurs probabilités d'exposition et leurs contrôlabilités, avec la proposition de quelques exigences de sûreté ; **2**. Identifier les menaces de sécurité en utilisant STRIDE, les quantifier en se basant sur les ressources demandées, les connaissances demandées et la criticité des menaces, pour obtenir le niveau de sécurité SecL ; **3**. Considérer les menaces de sécurité avec des criticités supérieures à deux (>2) comme des événements en relation avec la sûreté, et les ajouter dans l'analyse des risques de sûreté. Les TABLE III. et TABLE IV. présentent respectivement les scénarios de dangers et d'attaques pour l'application du système de production de bière. Nous observons que seule la première menace de sécurité est en relation avec la sûreté et doit être ajoutée à l'analyse de sûreté. Les échelles utilisées sont définies dans [16].

TABLE III. SCENARIOS DE DANGERS

Scénarios de dangers	Gravité	Probabilité	Contrôlabilité
Échec du PLC, envoie des fausses instructions à la vanne, causant une augmentation de pression	2	3	2
Échec de la vanne de vapeur, ne travaille pas correctement, causant une augmentation de pression	2	2	2
Panne électrique, causant un incendie affectant les êtres humains, le système	3	1	3

TABLE IV. SCENARIOS DE MENACES

Scénarios de menaces	Ressource	Connaissance	Criticité
Buffer Overflow, résultant du langage de programmation pour développer les automates	1	1	3
Denial of Service, puisque le système est accessible d'une grande taille	0	2	2
Emails infectés par un virus, sans une surveillance	0	0	2

3) Failure Mode, Vulnerabilities and Effect Analysis

La méthode FMVEA [18] est basée sur la méthode FMEA (en français AMDEC) en incluant les aspects de sécurité en intégrant les vulnérabilités (V) comme des sources de causes des scénarios d'attaques menant à des situations de dangers.

Les étapes d'une FMVEA sont les suivantes : **1**. Identifier les fonctionnalités du système, avec ses composants et préciser ceux qui doivent être analysés et protégés ; **2**. Identifier les modes d'échecs et les menaces pour les composants sélectionnés ; **3**. Identifier les effets des menaces et des échecs ; **4**. Déterminer les gravités des effets finaux, par l'aide des experts et en utilisant des échelles spécifiques ; **5**. Identifier les causes et les vulnérabilités ; **6**.

Déterminer les probabilités des événements de sûreté et des menaces de sécurité qui sont la somme des propriétés des menaces et du système. La propriété des menaces est la somme des ressources de la motivation d'un potentiel agent et de ses capacités pour exploiter une vulnérabilité. Tandis que la propriété du système est la somme du niveau d'accessibilité, de la facilité de connecter à un système, de la singularité des composants et de l'architecture du système. Toutes les valeurs sont définies à partir des échelles listées dans [5] ; **7**. Estimer le niveau du risque en multipliant les probabilités des attaques/des échecs avec leurs niveaux de gravité. Fig. 2 présente quelques scénarios d'échecs et d'attaques pour l'application de FMVEA sur le système de production de bière.

Elément	Menace / mode d' échec	Effet direct	Effet sur système	Cause / vulnérabilité	Gravité	Propriété de menaces	Propriété du système	Probabilité	Evaluation du risque
Communication entre le PLC et la vanne de vapeur	Des fausses données transférées du PLC	La vanne ne fonctionne pas correctement	Augmentation de pression dans le fermenteur	Erreur dans la configuration du PLC Attaquer change dans le code de l' automate exploitant le mode d' accès à distant toujours actif sur la station de programmation	2 3	2 + 2 = 4	2 + 3 = 5	1 9	2 27
Serveur Web	Modification des données et configuration sur le serveur Web	Modification dans les achats en ligne	Perte de crédibilité et notoriété	Erreur de configuration sur le serveur Accès non autorisé sur le serveur Web en craquant les mots de passe, exploitant l' utilisation des mots de passe génériques	1 2	1 + 2 = 3	2 + 3 = 5	2 8	2 16

Fig. 2. Scénarios des échecs et des attaques pour l'application de FMVEA

4) Six-Step Model

La méthode SSM [19] est une approche fonctionnelle. Elle commence par présenter les liens entre les fonctions et les objectifs du système. SSM présente clairement les impacts et les effets d'une dimension d'un système sur toutes les autres dimensions. Les six dimensions de ce modèle sont les fonctions d'un système, ses structures, les scénarios de dangers, les mesures de sûreté, les scénarios d'attaques et les mesures de sécurité. Par exemple, les impacts d'un scénario d'attaque sur un scénario de danger et sur une mesure de sûreté seront analysés. La démarche de SSM est intéressante, mais dans le cas de grandes industries avec beaucoup de scénarios, la modélisation avec SSM sera compliquée.

Le modèle SSM présente l'analyse des risques en se basant sur les six dimensions hiérarchiques présentées avant. Les étapes du modèle SSM sont les suivantes : **1**. Décrire les fonctions du système en utilisant le Goal Tree et identifier les relations entre eux ; **2**. Définir la structure du système en utilisant le Success Tree et identifier les relations entre eux et avec les fonctions ; **3**. Identifier les échecs du système (B), avec leurs relations d'impacts sur les fonctions et la structure ; **4**. Identifier les mesures de sûreté (X), avec leurs relations d'impacts sur les autres dimensions identifiées ; **5**. Identifier les attaques (A), avec leurs relations d'impacts sur les autres dimensions identifiées ; **6**. Identifier les mesures de sécurité (Z), avec leurs relations d'impacts sur les dimensions identifiées. Ces étapes sont présentées dans la fig.3. Toutes ces relations sont présentées sous forme des matrices. Pour l'application de production de bière, le sous-système est le processus de stérilisation (P1), avec support les sous-systèmes de contrôle et de réseau. La structure de P1 est présentée comme celle dans Fig.1. À noter que Fig. 3 représente le schéma général de SSM. Les six dimensions sont identifiées et modélisées avec SSM :

- B1 : une erreur de configuration dans le PLC, peut fortement affecter sur le fonctionnement de la vanne de vapeur, du capteur, du PLC et de P1.
- B2 : une défaillance de la vanne de vapeur, peut avoir un effet moyen sur son fonctionnement et sur P1.
- X1 : une redondance du PLC et de la vanne de vapeur, peut fortement diminuer l'effet de B1 et B2.
- A1 : Un malware sur la station de programmation des PLC, affecte la communication entre PLC et la vanne de vapeur et affecte fortement X1, B1 et P1.
- A2 : L'attaque Stuxnet [3] sur le système SCADA, peut affecter très faiblement sur X1 et B2, et fortement sur B1.
- Z1 : Désactivation du mode d'accès à distance, quand il n'est pas utilisé, peut diminuer l'effet de A1, il n'a aucun effet sur les échecs et les mesures de sûreté et protège le processus de stérilisation.

Les relations d'impacts dans l'exemple sont représentées par des losanges comme dans Fig. 3.

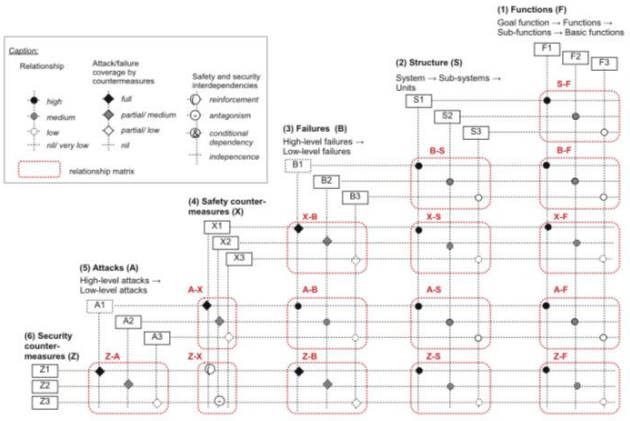

Fig. 3. Représentation générale de SSM

B. Extension des méthodes décrivant les scénarios sous forme de chaines d'événements

Cette catégorie de méthodes permet de présenter les scénarios de dangers et d'attaques sous forme de chaines d'événements, pour définir les scénarios d'occurrence mixtes menant à des événements redoutés physiques.

1) Attack Tree Bow Tie

La méthode ATBT [4] permet de représenter dans un même modèle graphique les événements liés aux défaillances et aux attaques et de proposer une double cotation pour l'évaluation des probabilités des classes d'évènements. L'intérêt de cette méthode est d'avoir une vue d'ensemble des scénarios mixtes et d'évaluer un niveau de sûreté quel que soit le niveau de sécurité.

La méthode ATBT combine les nœuds-papillon (Bow Tie – BT) et les arbres d'attaques (Attack Tree – AT) pour identifier les causes liées à la sécurité pour les scénarios décrits dans les analyses de risques de sûreté. Les étapes de réalisation sont les suivantes : **1**. Construire le nœud-

papillon (BT) [6], relatif à l'analyse des risques pour la sûreté, pour les événements redoutés physiques, identifiés par APR [1], le BT représente les causes et les conséquences des événements redoutés analysés ; **2**. Construire l'arbre d'attaques (AT), relatif à l'analyse des risques de sécurité : pour chaque événement élémentaire du nœud-papillon – qui peut être une défaillance d'un élément du système de contrôle industriel (dérive de capteur, fermeture de vanne…) – identification s'il existe des incidents de sécurité pouvant provoquer le même événement et description des étapes et des vulnérabilités exploitées par l'attaquant. Les événements sont reliés par des portes logiques AND/OR ; **3**. Évaluation des différents scénarios, selon un vecteur à deux dimensions ($\overline{L_s, L_f}$), représentant respectivement la probabilité des événements de sécurité et la probabilité des événements de sûreté, cette phase se fait en trois étapes : **3.1**. Déterminer les Coupes Minimales (MCs) d'un modèle ATBT : elles sont les plus petites combinaisons d'événements de sûreté et de sécurité causant l'occurrence de l'événement redouté, c'est-à-dire les scénarios menant à cet événement. Les coupes minimales peuvent être composées uniquement d'événements de sûreté, uniquement d'événements de sécurité ou d'une combinaison des deux ; **3.2**. Pour chaque coupe minimale, caractériser la probabilité ou la vraisemblance de chaque événement élémentaire. Des échelles spécifiques sont utilisées pour évaluer la probabilité et la vraisemblance ; **3.3**. Déterminer les probabilités des couples vecteurs de chaque MC en résolvant sauf les événements reliés par AND et en prenant la valeur minimale de probabilité des événements formant le couple. Les couples sont classifiés en se basant sur une échelle définie.

L'utilisation de la notion des MCs avec un couple de probabilité/vraisemblance est expliquée par la différence de nature entre événements de sûreté et de sécurité et permet d'évaluer un niveau de sûreté quel que soit le niveau de sécurité. Fig. 4 et Fig. 5 présentent la combinaison d'AT et BT pour le système de production de bière, et dans la TABLE V. , les vecteurs sont évalués et permettent de choisir un niveau de sûreté pour un niveau de cyber sécurité.

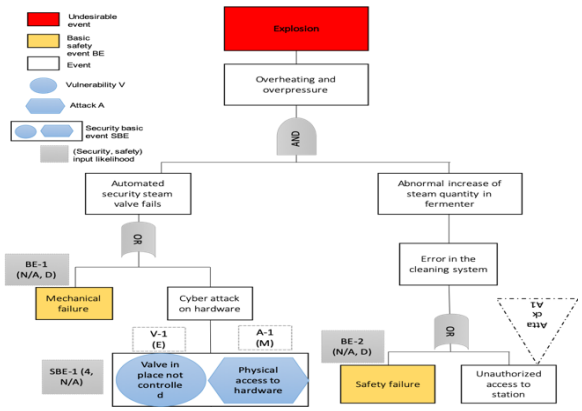

Fig. 4. Combinaison AT et BT

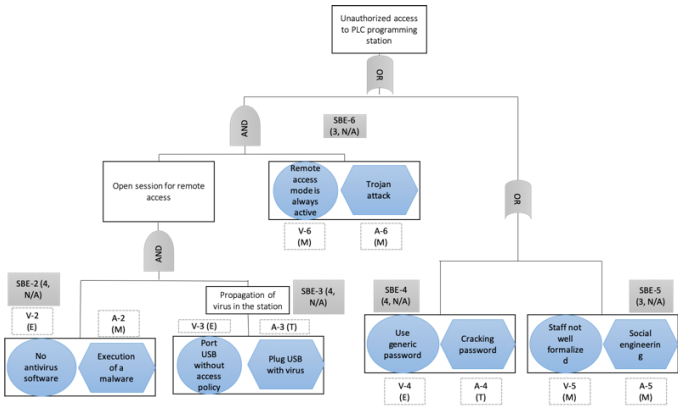

Fig. 5. Attaque A1

TABLE V. MINIMAL CUT SET ET VECTEURS AVEC LEURS PROBABILITES

MCs	Vecteurs	Niveau
SBE-2, SBE-3, SBE-6, SBE-1	(4, N/A)	Very High
SBE-4, SBE-1	(4, N/A)	Very High
SBE-5, SBE-1	(3, N/A)	High
BE-1, BE-2	(N/A, D)	Low
SBE2, SBE-3, SBE-6, BE-1	(4, D)	Low
SBE-4, BE-1	(4, D)	Low
SBE-5, BE-1	(3, D)	Low
SBE1, BE-2	(4, D)	Low

2) S-cube

La méthode S-cube [20] permet une modélisation détaillée du système de contrôle-commande et une génération automatique des scénarios de dangers et d'attaques. S-cube est une méthode intéressante, mais très détaillée ce qui la rend difficile pour la mettre en œuvre.

S-cube permet une modélisation de l'architecture du système, associant les aspects de sécurité et de sûreté et générant automatiquement les scénarios des risques possibles menant à des événements indésirables identifiés auparavant au moyen d'une HAZOP [7]. Les phases de la méthode S-cube sont les suivantes : **1**. Modéliser et décrire le système, les données d'entrée, telles que ses architectures fonctionnelles et logiques, les différentes zones, les machines connectées, les logiciels et les flux de données entre les composants, en se basant sur une base de connaissance S-cube KB comme un Domain Specific Language. Après, des experts définissent les aspects de sûreté et de sécurité et les échelles ; **2**. L'architecture du système est traitée avec S-cube KB pour générer des résultats, tels que les scénarios d'attaques et de dangers, avec une évaluation des probabilités et les mesures proposées pour améliorer la sûreté et la sécurité du système et minimiser la probabilité d'occurrence ; **3**. Définir une nouvelle analyse quantitative ou qualitative, puisque l'architecture principale du système est modifiée et des nouvelles données sont produites. Les phases de S-cube sont présentées dans Fig. 6. L'exemple du système de production de bière est présenté ci-dessous :

- Phase 1 : Étape (1, i) : L'architecture fonctionnelle du système est modélisée, telle que les équipements physiques et l'architecture logique représentée par

les flux de données entre les équipements. Étape (1, ii) : les aspects de sécurité et de sûreté, tels que, des privilèges d'accès au serveur SCADA, des mises à jour mensuelles des logiciels et les vulnérabilités, telles que l'accès sans privilèges à la station de programmation, le mode d'accès à distance est toujours actif sont renseignés.

- Phase 2 : Étape (2, i) : Les événements menant à l'événement indésirable « Augmentation anormale de la pression dans le fermenteur » sont définis, on peut considérer par exemple que la vanne de vapeur n'est pas maintenue depuis un an, ou que d'autres facteurs peuvent mener à l'échec de cette vanne et qu'elle ne répond pas aux commandes du PLC. En se basant sur les étapes d'attaques et les modes d'échec définis, les scénarios d'attaques et de danger sont générés et présentés dans les TABLE VI. et TABLE VII. Étapes (2, ii) et (2, iii) : Des mesures de sûreté et de sécurité sont proposées, telles qu'une maintenance mensuelle des équipements, des mises à jour mensuelles des logiciels, des authentifications d'accès aux équipements.

TABLE VI. SCENARIOS D'ATTAQUES

Attaque 1	Accès physique sur la station de programmation
	Exploiter la vulnérabilité sur cette station, sans privilèges d'accès
	Envoyer des instructions erronées à la vanne de vapeur
Attaque 2	Exploiter la vulnérabilité sur la station de programmation dans le langage utilisé
	Attaque Buffer overflow

TABLE VII. SCENARIOS DE DANGERS

Accident 1	Échec accidentel de la vanne de vapeur
Accident 2	Échec accidentel du PLC
Accident 3	Échec accidentel sur le réseau des instruments (la connexion entre la vanne de vapeur et le PLC)

S-cube contient une phase importante consistant à modéliser le système industriel et générer les scénarios d'attaques et de dangers automatiquement. Elle a des limites, l'analyse du risque en se basant seulement sur les probabilités d'occurrence et pas sur les impacts des scénarios.

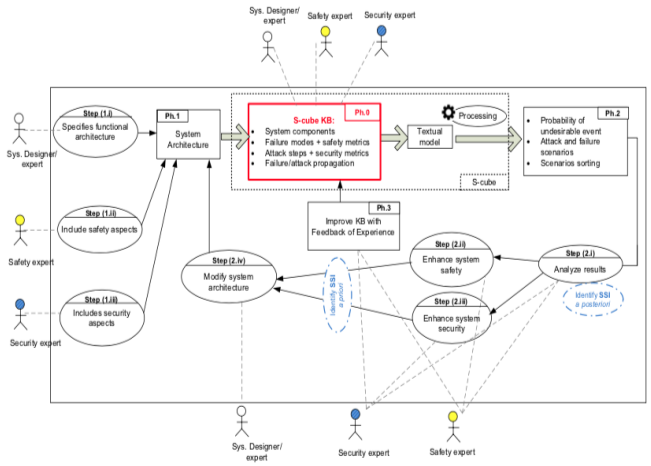

Fig. 6. L'approche S-cube

C. *Extension de System-Theorectic Process Analysis*

De nombreux développements actuels se fondent sur la méthode STPA [21]. Sa démarche et son processus sont différents de ceux d'autres méthodes. Plusieurs auteurs ont proposé des extensions de STPA, ou se sont basés sur STPA pour intégrer la sécurité ([22], [23], [24], et d'autres). Cet article présente l'extension STPA-Safesec est présentée.

1) System-Theoretic Process Analysis-SafeSec

La méthode STPA-SafeSec [25] est une intégration de la méthode STPA pour l'analyse des événements dangereux et l'évaluation de la sûreté et d'une extension STPA-Sec [26][27] pour l'analyse des risques de sécurité. Dans STPA, la sûreté du système est vue comme un problème du contrôle qui doit réagir adéquatement, l'accident intervient en cas de défaut de comportement de ce contrôle et non comme la conséquence d'une défaillance (qui peut être supposée toujours possible). Dans STPA-Sec, l'impact de la sécurité informatique sur la boucle de contrôle est analysé. STPA-SafeSec permet de guider en profondeur l'analyse de la sécurité sur les composants critiques et d'intégrer les résultats avec l'analyse de sûreté. Cette méthode est intéressante, mais reste complexe à l'appliquer en coûteuse en temps dans le cas de grandes industries.

Les situations de dangers et d'attaques sont présentées comme des problèmes de contrôle et pour chacune, il existe un ensemble des conditions et mots-clés pour identifier les scénarios de perte. STPA-SafeSec contient deux boucles (Fig. 7) : la boucle représentant le système appliqué de manière itérative pour gérer les modifications et les stratégies de mitigation et la boucle de contrôle pour gérer la complexité du système. Les étapes de STPA-SafeSec sont les suivantes : **1**. Identifier les accidents et les pertes du système dont leurs niveaux sont élevés et les dangers du système ; **2**. Identifier les contraintes de sûreté et de sécurité ; **3**. Construire la couche de contrôle, qui est une représentation graphique de la boucle de contrôle et des interactions entre les contrôleurs ; **4**. Définir les actions de contrôle et les dangers pour chaque boucle (dangereux et non sécurisé) ; **5**. Relier la couche de contrôle et la couche des composants, pour identifier les algorithmes, les réseaux et les logiciels de chaque composant physique ; **6**. Affiner et relier les contraintes de sûreté et de sécurité vers la couche des composants et ajouter des contraintes spécifiques si elles existent ; **7**. Identifier les scénarios de dangers et d'attaques ; **8**. Guider une analyse de sécurité détaillée pour les composants qui devront être analysés en priorité ; **9**. Identifier et appliquer des stratégies de mitigation effectives sur le système.

Les étapes pour l'application sur le système de production de bière sont les suivantes :

- Les pertes du système : P-1 : éclatement, P-2 : blessures des personnes, P-3 : indisponibilité du système de production.
- Les dangers : D-1 : une augmentation anormale de la pression dans le fermenteur, D-2 : une panne d'électricité.
- Les contraintes de sûreté : CTR-S-1 : un arrêt du flux de vapeur dans le fermenteur, quand le taux spécifique sera atteint, CTR-S-2 : le fermenteur sera

nettoyé sauf s'il est vide, CTR-S-3 : une source d'électricité continue.

- Pas de contraintes de sécurité.

Le diagramme de la boucle de contrôle est présenté dans Fig. 8. Deux boucles : le contrôleur de production avec les systèmes de stérilisation et de fermentation. Le système de stérilisation est analysé, avec les nœuds (N-X), les interactions et les connexions (C-X), les relations entre les nœuds sont présentées dans l'explication de l'étude de cas.

Deux actions de contrôle dangereuses pour cette boucle : AC-1 : la vanne n'arrête pas le flux de vapeur après que la pression est atteinte, AC-2 : la vanne injecte la vapeur dans le fermenteur même s'il n'est pas vide. Après le mappage vers la couche des composants, N-1 contient le PLC, les composants de N2 sont les mêmes présentés dans l'étude de cas.

La TABLE VIII. présente les contraintes de sûreté et de sécurité qui peuvent être enfreintes sur chaque nœud et connexion au niveau du contrôle. Pour N-2, un mauvais fonctionnement peut causer une augmentation anormale de pression dans le fermenteur, une attaque sur N-2 peut causer l'indisponibilité de la communication avec N-1. Ces contraintes sont reliées et affinées avec la couche des composants et les causes et les scénarios sont définis pour chaque danger.

Scénario 1 : la vanne de vapeur reçoit un signal de contrôle incorrect du PLC, ce scénario est composé de D-1, AC-1, N-1, N-2, PLC, vanne de vapeur, fermenteur, CTR-S-1, et les contraintes de sécurité « Command Injection » et « Command Delay ».

TABLE VIII. NŒUDS ET CONNEXIONS AVEC LES CONTRAINTES VIOLEES

	Command injection	**Command delay**	**Communication drop**	**D1**	**D2**
N-1	X	X	X		
N-2		X	X	X	X
C1	X	X	X		X
C2		X	X		X

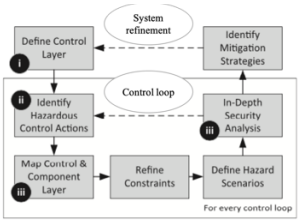

Fig. 7. Les étapes de STPA-SafeSec

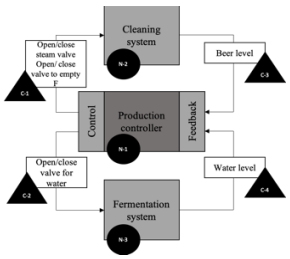

Fig. 8. Le diagramme de la couche de contrôle

Il existe d'autres méthodes d'analyse des risques intégrant la sécurité et la sûreté, telles que la combinaison de STRIDE et FMEA [28] (différente de FMVEA), Unified Security and Safety Risk Assessment [29], AFT [30], FACT [31], CHASSIS [18], KAOS-SE [32], etc. La section suivante présente l'évaluation et la comparaison des méthodes d'analyse détaillées ci-dessus.

IV. EVALUATION DES METHODES D'ANALYSE DES RISQUES

Dans cette partie, à partir de l'application sur le système de production de bière, les méthodes d'analyse des risques de sécurité et de sûreté sont évaluées et comparées en se basant sur les critères suivants :

- Méthode est générique ou dirigée par un modèle ;
- Phases du processus d'analyse des risques couvertes par la méthode ;
- Méthode d'analyse quantitative ou qualitative ;
- Niveau de détail de l'analyse ;
- Principes d'intégration des risques de sécurité et de sûreté ;
- Phases de cycle de vie sur lesquelles la méthode peut être appliquée ;
- Domaines d'application ;

Les méthodes d'analyse des risques intégrant la sécurité et la sûreté sont classifiées soit comme génériques soit dirigées par un modèle. Les méthodes génériques étudient la sécurité et la sûreté au niveau de chaque composant [11] dans la conception du système ou l'évaluation du risque. Tandis que, les méthodes dirigées par des modèles consistent à modéliser le système à analyser, en représentant ses aspects fonctionnels et non fonctionnels et à ajouter et d'exploiter des différentes informations dans l'analyse des risques. Les méthodes présentées dans cet article sont classifiées ci-dessous :

- Les méthodes génériques : SAHARA, FMVEA, ATBT.
- Les méthodes dirigées par des modèles : SGM, SSM, S-cube, STPA-SafeSec.

Le processus d'analyse des risques est composé de trois étapes principales définies dans la norme ISO 31000 [1] :

- L'identification des risques : les scénarios des risques sont modélisés dans cette étape, c'est-à-dire par exemple les événements indésirables qui peuvent nuire potentiellement aux personnes ou à l'environnement.
- L'analyse des risques : cette étape porte sur l'analyse des probabilités et des conséquences, représentant respectivement la probabilité de l'occurrence et la gravité des impacts des scénarios des risques identifiés.
- L'évaluation des risques : dans cette étape, la liste des scénarios des risques analysés est établie, chacun est évalué pour déterminer son niveau (acceptable ou non).

Une étape de traitement des risques peut être ajoutée. Elle consiste à proposer des mesures de sécurité et de sûreté pour maitriser les risques. La TABLE IX. identifie les phases couvertes par les différentes méthodes d'analyse des risques.

Le risque peut être évalué et priorisé en utilisant une analyse quantitative ou qualitative, cela dépend des données disponibles et du système analysé :

TABLE IX. PHASES D'ANALYSE DES RISQUES

Méthodes d'analyse	Identification du risque	Analyse du risque	Évaluation du risque	Traitement du risque
SGM	X	X (probabilité et impact)		X
SAHARA	X	X (impact)		
FMVEA	X	X (probabilité et impact)	X	
SSM	X			X
ATBT	X	X (probabilité)		
S-Cube	X	X (probabilité)		X
STPA-SafeSec	X			X

- Une analyse qualitative évalue et documente les risques subjectivement en utilisant des échelles d'évaluation prédéfinies et en utilisant les données et l'élicitation des experts. Elle considère tous les risques identifiés dans le processus d'analyse.
- Une analyse quantitative évalue les risques de manière quantifiée en utilisant des données de retour d'expérience ou de bases de données. Elle est généralement utilisée pour les risques qui ont des conséquences importantes.

La classification des méthodes est présentée dans la TABLE X. :

TABLE X. APPROCHES AVEC LES TYPES D'ANALYSE

Analyse qualitative	Analyse quantitative	Quantitative et qualitative
FMVEA, SSM, STPA-SafeSec	Aucune	SGM, SAHARA, ATBT, S-cube

La méthode d'analyse des risques peut être simple ou détaillée. La classification selon ce critère est présentée ci-dessous :

- Une méthode simple applique des procédures peu complexes et peu couteuses en temps. Elle peut par exemple contenir seulement l'analyse des événements indésirables critiques. Cette catégorie comprend les méthodes SGM, SAHARA et FMVEA.
- Une méthode détaillée vise l'identification de tous les scénarios et événements indésirables, avec beaucoup de relations entre les événements de sécurité et de sûreté. Le processus est appliqué en détail et peut-être chronophage surtout dans le cas des systèmes industriels critiques de grande taille. Cette catégorie comprend les méthodes SSM, ATBT, S-cube et STPA-SafeSec.

Le développement des méthodes d'analyse des risques intégrant la sécurité et la sûreté prend plusieurs formes :

- Évolution d'une méthode d'analyse des risques de sûreté pour ajouter l'analyse des risques de sécurité. Cette catégorie comprend la méthode FMVEA.
- Évolution d'une méthode d'analyse des risques de sécurité pour ajouter l'analyse des risques de sûreté. Aucune des méthodes présentées existe dans cette catégorie.
- Intégration d'une méthode analyse des risques de sûreté déjà existante avec une autre pour l'analyse des risques de sécurité déjà existante. Cette catégorie comprend les méthodes SAHARA, ATBT et STPA-SafeSec.
- Proposition de nouvelles approches, cette catégorie comprend les méthodes SGM, SSM et S-cube.

En se basant sur les formes d'intégration, il existe deux types de méthodes pour présenter les étapes impliquées, qui sont : l'intégration séquentielle des méthodes d'analyse de sécurité et de sûreté, dans lesquelles les risques de sécurité et de sûreté sont réalisés séquentiellement et l'intégration non-séquentielle des méthodes, dans lesquelles la sécurité et la sûreté sont réalisées simultanément. La TABLE XI. présente la classification selon ce critère :

TABLE XI. APPROCHES AVEC TYPES D'INTEGRATION

Intégration séquentielle	Intégration non-séquentielle
SGM, SAHARA, SSM, ATBT	FMVEA, S-cube, STPA-SafeSec

Pour avoir une analyse complète et continue des risques, le processus doit couvrir toutes les phases du cycle de vie d'un système (le développement, le déploiement et l'exploitation), et toutes les modifications d'un système doivent être prises en considération dans l'analyse des risques. Dans la TABLE XII. , les méthodes sont classifiées en se basant sur les phases du cycle de vie qu'elles couvrent.

TABLE XII. APPROCHES AVEC LES PHASES DE CYCLE DE VIE COUVERTES

	Développement	Déploiement
SGM	X	X
SAHARA	X	X
FMVEA		X
SSM	X	X
ATBT	X	X
S-cube	X	X
STPA-SafeSec	X	X

Finalement, le critère du domaine permet de comprendre les types d'applications et les domaines d'application correspondants des méthodes d'analyse intégrant la sécurité et la sûreté [11]. Plusieurs approches sont proposées et utilisées utiliser dans des domaines industriels génériques. La TABLE XIII. présente les méthodes avec leurs domaines d'application.

Nous analysons que les méthodes présentées utilisent des approches d'analyse classiques connues, avec des intégrations et des évolutions, par exemple pour la sûreté Bow Tie, STPA, APR, FMEA, HAZOP et pour la sécurité Attack Tree, STPA-Sec, STRIDE, avec différentes formes d'intégration. Les événements redoutés physiques analysées dans les méthodes présentées sont les mêmes, cependant la

logique pour prendre en compte la cyber sécurité et évaluer la vraisemblance des attaques est différente.

TABLE XIII. APPROCHES AVEC LEURS DOMAINES D'APPLICATION

Méthodes d'analyse des risques	Domaines d'application
SGM	Domaine des transports
SAHARA	Domaine des transports
FMVEA	Domaine des transports
SSM	Peut être appliquée dans le domaine industriel. Etude de cas sur un système de traitement d'eau
ATBT	Peut être appliquée dans le domaine industriel. Étude de cas sur un réacteur chimique
S-cube	Peut être appliquée dans le domaine industriel
STPA-SafeSec	Peut être appliquée dans le domaine industriel. Etude de cas dans le domaine de l'électricité

Chaque méthode possède ses spécificités et ses limites, celles qui n'incluent pas la phase de modélisation d'un système ou qui sont basées seulement sur une analyse qualitative ou celles qui ne couvrent pas l'étape d'évaluation du risque. Certaines de ces méthodes ne sont pas appliquées dans la phase de développement d'un système et d'autres sont appliquées sur l'ensemble du cycle de vie. La plupart des méthodes d'analyse des risques aussi n'utilisent pas les vulnérabilités comme des entrées pour l'identification des scénarios d'attaques. Il apparait qu'une méthode intégrant les meilleures caractéristiques et mixant les meilleurs processus devrait être proposée et étudiée pour répondre aux besoins de maitrise des risques sur les installations industrielles.

V. CONCLUSION ET FUTUR TRAVAIL

L'intégration de la sécurité et la sûreté est devenue cruciale dans l'analyse des risques pour les systèmes industriels, qui sont fortement automatisés et numérisés. Ces infrastructures sont devenues plus vulnérables à des cyberattaques pouvant nuire la sûreté du système. La sécurité et la sûreté possèdent des problématiques différentes, mais possèdent aussi des similitudes, des interactions et des interdépendances. Pour ces raisons, plusieurs auteurs ont proposé et développé des approches intégrant la sécurité et la sûreté dans l'analyse des risques. Dans cet article, nous avons présenté en détail des méthodes récentes d'analyse des risques de sûreté et de sécurité et les avons appliqués sur un système de production de bière. Finalement, elles sont classifiées et comparées en se basant sur une liste des critères objectifs. Chaque méthode possède ses caractéristiques et ses limites, notre futur travail sera concentré sur la proposition d'une méthode d'analyse complète des risques et dirigée par un modèle et prendra en considération la relation entre la sécurité et la sûreté. Elle sera basée sur différentes caractéristiques et processus d'analyses triés des méthodes existantes.

REFERENCES

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

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

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

[4] 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.

[5] 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.

[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] C. A. Ericson and others, *Hazard analysis techniques for system safety*. John Wiley & Sons, 2015.

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

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

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

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

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

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

[15] J. Dürrwang, K. Beckers, and R. Kriesten, "A lightweight threat analysis approach intertwining safety and security for the automotive domain," in *International Conference on Computer Safety, Reliability, and Security*, 2017, pp. 305–319.

[16] 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.

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

[18] 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.

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

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

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

[22] 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.

[23] G. Howard, M. Butler, J. Colley, and V. Sassone, "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)*, 2017, pp. 174–180.

[24] C. Schmittner, Z. Ma, and P. Puschner, "Limitation and improvement of STPA-Sec for safety and security co-analysis," in *International*

Conference on Computer Safety, Reliability, and Security, 2016, pp. 195–209.
[25] 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.
[26] 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.
[27] W. Young, "System-Theoretic Process Analysis for Security (STPA-SEC): Cyber Security and STPA." STAMP Conference, 2017, [Online]. Available: https://psas.scripts.mit.edu/home/wp-content/uploads/2017/04/STAMP_2017_STPA_SEC_TUTORIAL_as-presented.pdf.
[28] S. Plósz, C. Schmittner, and P. Varga, "Combining safety and security analysis for industrial collaborative automation systems," in *International Conference on Computer Safety, Reliability, and Security*, 2017, pp. 187–198.
[29] Y.-R. Chen, S.-J. Chen, P.-A. Hsiung, and I.-H. Chou, "Unified security and safety risk assessment-a case study on nuclear power plant," in *2014 International Conference on Trustworthy Systems and Their Applications*, 2014, pp. 22–28.
[30] E. Ruijters, S. Schivo, M. Stoelinga, and A. Rensink, "Uniform analysis of fault trees through model transformations," in *2017 Annual Reliability and Maintainability Symposium (RAMS)*, 2017, pp. 1–7.
[31] G. Sabaliauskaite and A. P. Mathur, "Aligning cyber-physical system safety and security," in *Complex Systems Design & Management Asia*, Springer, 2015, pp. 41–53.
[32] M. F. H. ABULAMDDI, "A survey of techniques requirements for integrating safety and security engineering for cyber physical systems," *Internatinol Journal of Computer Science and Engineering Survey (IJCSES)*, Dec. 2016.