Une approche systémique pour l'analyse de cybersécurité des systèmes industriels

Jean-Marie Flaus, John Georgakis

Une approche systémique pour l'analyse de cybersécurité des systèmes industriels

A systemic approach for cybersecurity analysis of industrial control systems

Jean-Marie Flaus, John Georgakis

Univ. Grenoble Alpes, CNRS, G-SCOP,
F-38000 Grenoble, France
jean-marie.flaus@univ-grenoble-alpes.fr

Résumé

L'objectif de cette communication est de décrire une méthode d'analyse systémique pour réaliser l'analyse des risques de cybersécurité des installations composées d'éléments informatiques et de système de commande de systèmes industriels. Nous rappelons d'abord le principe des approches systémiques de risque, précisons le contexte puis détaillons la méthode proposée. Elle s'appuie sur une décomposition en systèmes en interaction. Pour chaque système un modèle des risques est réalisé à partir d'une base de connaissance. Les scénarios sont obtenus par composition. Cette approche est illustrée sur un exemple d'installation. Nous terminons en proposant des pistes d'amélioration.

Summary

The purpose of this paper is to describe a systemic analysis method for performing cybersecurity risk analysis of installations composed of computer components and industrial system control systems. We first recall the principle of systemic approaches to risk, specify the context and then detail the proposed method. It is based on a decomposition into interacting systems. For each system a risk model is produced from a knowledge base. The scenarios are obtained by composition. This approach is illustrated on an example installation.
We finish by suggesting ways to improve the proposed approach.

1. Objectifs

La cybersécurité des installations industrielles est un sujet préoccupant de nos jours. De récentes attaques (WannaCry, 2017) ou d'autres un peu plus anciennes comme Stuxnet (2010) ont montré la vulnérabilité potentielle de ce type de systèmes. Un certain nombre de démarches pour maîtriser ce risque ont été proposées par les principaux guides et normes, notamment la norme IEC 62443 ou le guide de l'ANSSI [13][14].
Dans toutes ces démarches, une étape importante qui doit être réalisée au début du processus, puis de façon périodique, est l'analyse de risque. Le choix de la méthode est laissé libre. Cette analyse de risque est au cœur du processus de management des risques (figure 4) et est d'une importance capitale.
Une des principales difficultés de la mise en œuvre de l'analyse de risques est d'être à la fois systématique et exhaustive tout en gardant la capacité d'imaginer des situations imprévues et de conserver une vue de synthèse des risques. Un compromis doit être fait en fonction du contexte et des objectifs. C'est la raison pour laquelle de nombreuses méthodes ont été proposées. Pour l'analyse des risques des systèmes physiques, il existe des méthodes très structurées et détaillées comme l'AMDEC [6], d'autres un peu moins détaillées comme l'APR [6], d'autres sont basées sur une démarche de brainstorming comme la méthode WHAT-IF ou au contraire à base de CHECKLIST pour être très systématique, et enfin certaines s'appuient sur une démarche systémique comme la méthode MADS-MOSAR [26] pour favoriser une vue globale. Cette approche peut être vue comme une version simplifiée des approches de type MBSE (Model Based Safety Analysis) [29] qui sont de plus en plus utilisées aujourd'hui pour les systèmes complexes.
Dans le domaine de l'analyse des risques des systèmes d'information, il existe là aussi de nombreuses méthodes, certaines étant des adaptations des méthodes classiques comme l'AMDEC logiciel [23], d'autres étant des méthodes dédiées comme la méthode EBIOS, OCTAVE ou CORAS [15].

Pour analyser les risques des systèmes de contrôle industriels, composé d'un système d'information en relation avec un système physique, les approches proposées sont, soit des méthodes d'analyse de risque provenant du monde de la sécurité informatique adaptées aux systèmes physiques, notamment pour les impacts possibles, soit des méthodes classiques pour lesquelles on ajoute certains aléas générés par le système informatique. Certaines méthodes sont même modifiées pour conduire à une méthode hybride comme la méthode Cyber-PHA [9,8] ou le cyber-bowtie [7].
Dans ce contexte, il nous a paru intéressant de réfléchir au développement d'une approche d'analyse systémique des risques pour les systèmes cyber physiques en nous inspirant des approches développées pour les systèmes physiques. Cet article présente la méthode élaborée et discute de son intérêt et de ses limites.
Le plan est le suivant : la première partie expose les différents aspects du contexte et décrit les principes de l'approche systémique pour l'analyse des risques ainsi que la problématique de la cyber sécurité des systèmes industriels.
La seconde partie décrit la méthode proposée ainsi qu'une première ontologie utilisée pour réaliser l'analyse. La troisième partie présente un cas d'étude et l'application de la méthode. L'article se termine par une discussion sur l'intérêt de l'approche et les développements qui pourraient être envisagés.

2. Contexte

2.1 Approche systémique pour l'analyse des risques des systèmes physiques

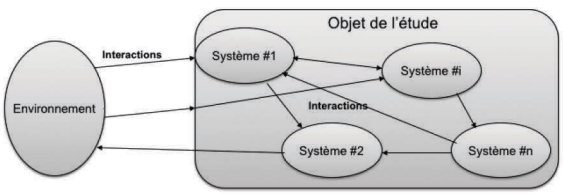

Figure 1 : Décomposition en systèmes

La systémique a été développée par J.P..Lemoigne pour l'analyse des systèmes complexes [25]. Cette approche a été utilisée pour l'analyse des risques dans la méthode MOSAR (Méthode organisée et Systémique d'Analyse des Risques) proposée par P. Périlhon [26]. Cette approche a été formalisée [19]. L'idée de base de cette méthode consiste à décomposer le système à analyser en sous-systèmes (figure 1). Chaque système est analysé d'un point de vue entrée sortie à l'aide d'une checklist des flux de danger possibles, ceux-ci étant définis comme des interactions non souhaitées conduisant à des états dommageables. On obtient alors un modèle appelé modèle de danger du système qui recense ce à quoi il est vulnérable et ce qu'il peut générer comme flux de danger (figure 2)

La combinaison de ces flux permet ensuite de construire les scénarios de danger, et de préconiser la mise en place de barrières.

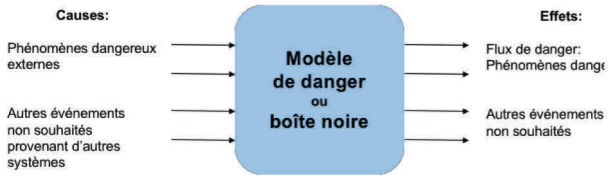

Figure 2 : Modèle de danger

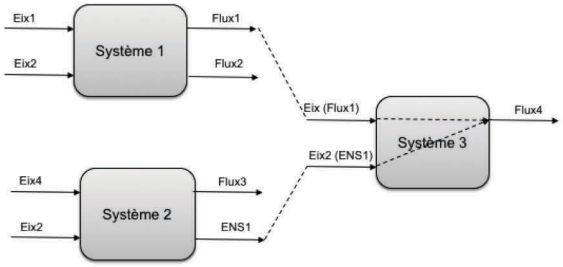

Figure 3 : Construction des scénarios

Le principal intérêt de cette approche, que les contraintes d'espace nous empêchent de présenter plus en détail ici, est de permettre une analyse avec une vue globale du système, ce qui n'est pas le cas des méthodes comme l'HAZOP ou l'AMDEC. Par ailleurs, l'utilisation d'une checklist des flux permet une certaine homogénéité de l'analyse. Ce type d'approche a été utilisé dans un certain nombre de domaines et a fourni des résultats satisfaisants [20][27]. Elle a jusqu'ici été appliquée pour l'analyse des risques des systèmes physiques pour lesquels on considère deux types d'impacts : les dommages physiques et les pertes de service.

Dans le cas de la sécurité des systèmes d'information, l'analyse de risques est abordée en général en caractérisant trois critères de base : la disponibilité, l'intégrité et la confidentialité (DIC) :
- la disponibilité correspond à la propriété d'assurer le service pour un équipement ou à être accessible pour une donnée au moment utile,
- l'intégrité est la caractéristique d'une information de n'être modifiée que par des personnes autorisées et selon un procédé défini
- et la confidentialité comme le fait de s'assurer que l'information n'est accessible qu'à ceux dont l'accès est autorisé.

Le risque est défini comme étant l'éventualité qu'une attaque ne génère des dommages sur un bien en portant atteinte à la disponibilité, l'intégrité ou à la confidentialité de l'information. Le recherche des menaces et des sources de menace, est couplée la recherche des vulnérabilités pour établir la vraisemblance de la menace. Les dommages sont immatériels puisqu'ils concernent l'information. La norme 27005 défini un cadre pour mettre en œuvre la démarche, appelé processus de gestion des risques (figure 4), qui est calquée sur le modèle général de la norme 31000.

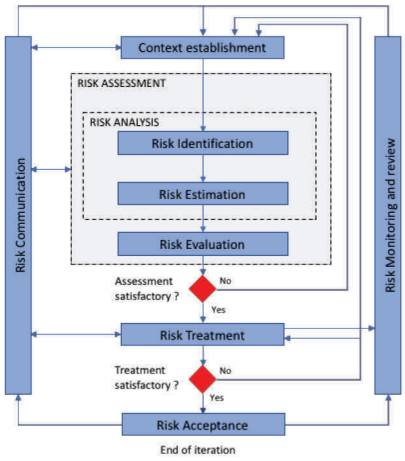

Figure 4 : Processus de gestion des risques

2.2 Cybersecurité des systèmes industriels

La cybersécurité des installations industrielles, des systèmes cyber-physiques et plus généralement des systèmes d'IIoT (Industrial IoT) est une problématique très actuelle. La cybercriminalité se développe de façon importante ces dernières années [4][3] : de nombreux systèmes informatiques de traitement de l'information (IT) font l'objet d'attaques qui peuvent se propager rapidement et avoir un impact important. L'évolution des installations industrielles (OT) pour lesquelles on assiste à une convergence technologique avec le monde de l'informatique classique et une interconnexion de plus en plus poussée entre les systèmes les rend de plus en plus vulnérable. Cette évolution se poursuit dans le cadre du développement et la mise en œuvre de l'internet des objets. Cette convergence apporte des avantages indéniables, mais fait émerger des risques nouveaux pour les processus physiques dont on peut perdre le contrôle à la suite d'une attaque sur le système informatique de pilotage.
Par rapport à la sécurité des systèmes d'information pour lesquels les dommages ont immatériels, une nouvelle catégorie de dommages doit être prise en compte : il s'agit des dommages créés par le système physique, ou d'une perte du service qu'il fournit, mais causés par un dysfonctionnement du système d'information. Ce peut être par exemple un accident de la circulation dû à un dysfonctionnement du système de pilotage pour une voiture, ou une explosion d'un processus de production dans le monde de la chimie.

Une norme importante dans ce contexte est la norme IEC 62443 qui a été élaborée par l'ISA [13]. Les travaux ont commencé en 2002 et les premiers standards ont été publiés sous le nom ISA99. A l'heure actuelle, même si certaines parties ne sont pas encore finalisées, un nombre important de documents a été publié et cette norme fait référence. La démarche de maîtrise des risques s'appuie sur une analyse des risques. Aucune méthode n'est proposée par la norme, mais le document 62443-3-2, intitulé Security Risk assessment and System Design, préconise une approche à deux niveaux : une première analyse est menée de façon globale, étape dans laquelle on décompose l'installation en zones et conduits, puis en fonction des résultats obtenus, une analyse plus détaillée de chaque zone est menée. Les autres guides, comme par exemple celui de l'ANSSI ou celui du NIST préconisent aussi de réaliser une analyse des risques mais laissent le choix en termes de méthode.

3 Méthode proposée

3.1 Idée générale

La méthode proposée s'articule autour des étapes suivantes :
Etape 1 : décomposer l'installation et de son environnement en systèmes pouvant combiner plusieurs types d'actifs
Etape 2 : analyser chaque système en utilisant une base de modèles génériques (BMG) représentée avec un formalisme simple de type sur action/état, ceci pour obtenir le modèle de risque du système. La BMG a vocation à s'enrichir au fur et à mesure des analyses.
Etape 3 : composer les modèles de risque de chaque système, de façon à représenter les scénarios d'attaque comme une succession d'étapes faisant apparaître la source, la cible et les "enablers" (les relais d'attaque).
Etape 4 : évaluer les différents scénarios en termes de vraisemblance et gravité
Etape 5 : Mise en place des mesures en utilisant les modèles de risque de chaque système en examinant les liens entrées/état et état/sorties.

Cette démarche d'analyse s'inscrit dans le processus proposé par la norme ISO 27005.
Le principal intérêt potentiel de l'approche est l'aide à la construction des scénarios qui est facilitée et rendue plus systématique par la décomposition et la BMG par rapport aux méthodes laissant l'analyste élaborer le scénario librement.

3.2 Modélisation du système

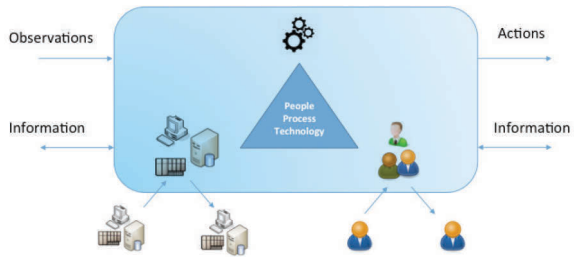

Figure 5 : Modèle d'un système

La première étape consiste à décomposer l'installation analysée et son environnement en systèmes. Chaque système regroupe des composants techniques, composé du matériel et de l'information, des personnes et des processus. Le matériel et l'information sont regroupés dans la même catégorie car l'information est stockée par un dispositif technique. L'ensemble de ces éléments permet d'assurer le bon fonctionnement du système. Cependant des échanges avec l'extérieur existent. Ces échanges, représentés sur la figure 5, sont classés de la façon suivante :

- échange de données via les réseaux d'information (filaire, wifi, faible débit …)
- échange de données entre la partie informatique et la partie physique sous forme d'observations et d'actions
- échange de données sur des mémoires amovibles
- échange de machines ou de composants (remplacements d'éléments, flux de poste portables ..)
- échange de personnes

Les flux physiques (énergie, chaleur, …) pourraient aussi être ajoutés à cette description, mais ils n'ont pas été pris en compte dans un premier temps pour éviter de rendre l'approche trop complexe.
Cette décomposition et l'analyse des liens permet de construire un modèle systémique de l'installation. Le fonctionnement interne du système n'est pas détaillé, mais les différents types d'éléments sont listés. Chaque élément appartient à une catégorie et possède un type générique. Par exemple, un ordinateur de bureau est de type "poste de travail" dans la catégorie ressource matérielle. La liste des éléments génériques proposée est la suivante :

- Matériel : serveur web, poste de travail, équipement réseaux: point d'accès sans fil ou filaire .., équipement OT : automate, unité terminale distante, …
- Logiciels : système d'exploitation, drivers, firmware, application
- Information : information de configuration d'un système, topologie du réseau, inventaire du matériel, logiciel de l'infrastructure et de la configuration, identifiants, bases de données, fichiers de travail …
- Support de l'infrastructure : câbles et connecteurs, bâtiment, alimentation électrique, système de refroidissement, éléments de sécurisation physique
- Ressources humaines : opérateur, administrateur, support, développeur, manager, utilisateur final, stagiaire, auditeur
- Processus : production, maintenance, surveillance et mesure, …

Cette liste peut être complétée si besoin.

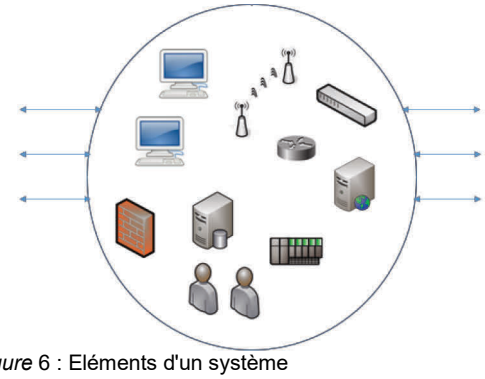

Figure 6 : Eléments d'un système

La décomposition d'une installation en systèmes est relativement classique : l'approche est assez proche de la notion de zone proposée par la norme 62443. L'inventaire des interactions est un peu plus complet, puisqu'il est limité à l'échange d'information dans la norme. L'idée de faire l'inventaire des composants provient de l'approche EBIOS, qui ne structure pas explicitement en systèmes mais le fait de façon indirecte via la notion de bien essentiel. Par rapport à EBIOS, l'approche proposée ici prend aussi en compte les ressources humaines et organisationnelles. Notre objectif est de faire apparaître les aspects importants d'un système en vue de l'analyse des risques

Modèle d'un système	
Structure	
ID de l'entité	
Nom de l'entité	
Éléments :	
Nom	*Type générique*
Interactions avec les autres systèmes	
Flux de données via réseaux	
Flux de données via mémoire amovible	
Flux de données entre cyber et physique	
Flux de composants et machines	
Flux de personnes	
Fonctions du système	
Principales fonctions	
Liens fonctionnels	
Systèmes contribuant à la fonction	

Figure 7 : Description tabulaire d'un système

Catégorie	Elément générique
Eléments Matériels	Poste, serveur web, réseau, point d'accès sans fil, point d'accès filaire, automates (PLC)
Ressource humaine	Opérateur

Figure 8 : Extrait de la typologie des éléments

3.3 Élaboration des modèles de risques

Dans l'approche proposée, un système est vu comme soumis à des attaques qui sont définies comme étant les entrées du modèle de risque. Ces actions ont pour objectif d'amener le système dans un état donné. Par exemple, une attaque peut être d'utiliser une vulnérabilité d'un logiciel serveur, l'objectif étant un accès illégal aux données du serveur. Cette possibilité d'accès illégal est défini comme un état. Si le serveur est correctement mis à jour, la vulnérabilité ne pourra pas être exploitée et donc l'état visé ne sera pas atteint. Si par contre l'état est atteint, d'autres actions peuvent être envisagées. Dans notre exemple, un accès illégal aux données peut permettre de voler celles-ci ou de des modifier. Le modèle de risque d'un système est donc composé des entrées, les actions reçues, d'un état interne de niveau de "corruption" que les actions visent à atteindre des actions générées en sortie (figure 9). Les actions de sortie peuvent aussi s'appliquer au système lui-même. Le modèle proposé est analogue au modèle de danger des méthodes systémiques classiques.

De façon formelle, un modèle de risque est défini par :

- les entrées du système, notées *sin_i* : ce sont les actions auxquelles le système est potentiellement vulnérable, cette liste étant déterminée en fonction des types d'éléments présents dans le système,
- les états internes, appelé *état de corruption*, notés *cm_i* , qui peuvent être atteints ou non atteints, cette transition étant possible ou non en fonction des vulnérabilités effectives et des mesures de sécurité,
- les sorties du système, notées *sout_i* : ce sont les actions du système qui s'appliquent au système lui-même et aux autres systèmes et qui peuvent se classer en actions créant directement des dommages ou actions visant à faire passer un système dans un état de corruption. Les relations logiques décrivant le lien entre les entrées et les états, et les relations logiques entre les états et les sorties, sont notées de la façon suivante :

Entree : sin_q → cm_i, cm_j
Sortie : cm_i & cm_j, cm_k → so_p

Un même état peut être obtenu par plusieurs entrées, une même entrée peut amener à plusieurs états. L'opérateur logique "et", noté & est possible.

- les vulnérabilités et les mesures de contrôle associées aux différentes entrées sorties du système notées de la façon suivante:

vul(se_j →cm_i)= {v1, …vn}|v'1,…v'm…}
ctrl(se_j →cm_i)= {c1, …cn}|c'1,…c'm…}

ce qui signifie que sur les chemins entre se et cm, séparés par le symbole |, il existe v1..vn vulnérabilités qu'il faut franchir successivement.

Pour réaliser une analyse synthétique, l'état de corruption du système est caractérisé de façon globale. On pourra donc identifier un certain de causes ou de vulnérabilités sur les éléments d'un système, mais on les considérera de façon globale.

On note la un des intérêts de l'approche systémique : les caractéristiques sont dues à un élément du système mais caractérise globalement l'état du système. Il est donc plus facile de caractériser des états dus à plusieurs éléments considérés ensemble.

La recherche des flux d'entrée (entrées du modèle de risque) et l'analyse des mesures existantes (verrou ou non vers le mode de corruption) permet d'obtenir la surface d'attaque du système (figure 11). Un état interne est équivalent à un état de type relais (enabler) défini dans le modèle d'attaque proposé par [21][22].

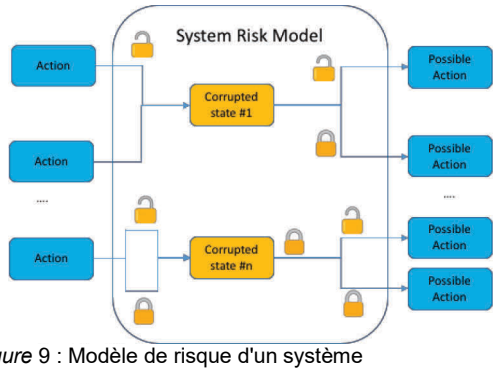

Figure 9 : Modèle de risque d'un système

Input model si PLC présent dans le système	
Input	*Corruption mode*
Recherche des identifiants par essai erreur ou force brute	Accès illégal PLC
Test identifiants usine	Accès illégal PLC
Utilisation vulnérabilité	Accès illégal PLC
Corruption trafic réseau	(Réception) Programme corrompu depuis station ingénierie
Corruption trafic réseau	(Réception) Données corrompues depuis station ingénierie
Corruption trafic réseau	(Réception) Données corrompues depuis SCADA
Réception volume important requête	Surcharge unité centrale

Output model si PLC présent dans le système	
Corruption Mode	*Output*
Accès illégal PLC	Corruption programme automate
	Corruption données automate
Données corrompues	Actions incorrectes (dysfonctionnement)
	Actions incorrectes (dommages)
	Désactivation fonction sécurité
	Perte contrôle procédé
Programme corrompu	actions incorrectes (dysfonctionnement)
	actions incorrectes (dommages)
	Désactivation fonction sécurité
	Perte contrôle procédé
Surcharge unité centrale	Perte contrôle procédé

Input model si Utilisateur présent dans le système	
Input	*Corruption mode*
Hameçonnage	Identifiants volés
	(Corrompu par) Malware

Figure 10 : Extrait de la BMG (base des modèles générisques)

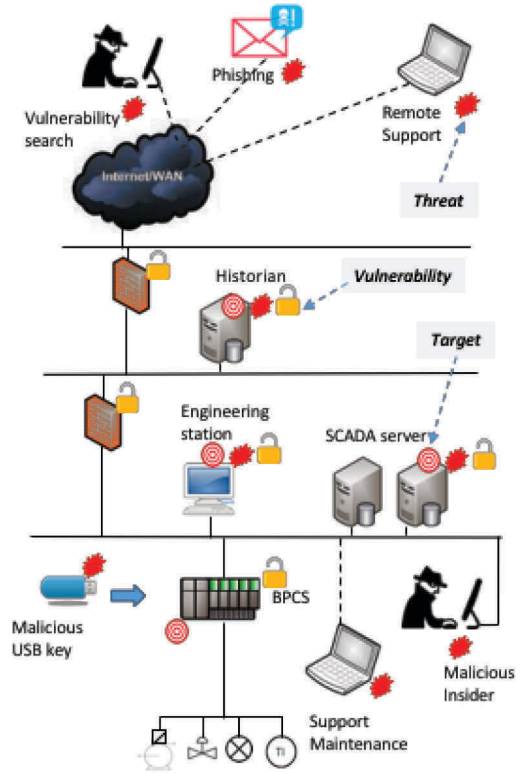

Figure 11 : Exemple de surface d'attaque

3.4 Construction des scénarios

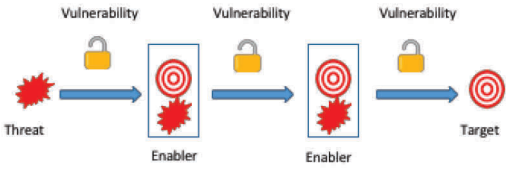

Figure 12 : Scénario composé différentes étapes

Après avoir analysé chaque système, la construction de scénarios d'attaque est obtenue combinant les sorties d'un système et les entrées d'un autre. Pour ce faire, deux informations sont combinées :
1. La sortie et l'entrée des modèles de risque
2. Les types de liens identifiés lors de la construction du modèle systémique

Pour décrire les scénarios, la notation est la suivante :
- un état de corruption du système Si est noté @cm:Si
- une action de Si vers Sj est notée action:Si-Sj. Si les systèmes source ou cible Si ou Sj sont quelconques, on le note avec ?
- une succession action-état ou état-action est notée action:Si-Sj→@cm:Sj → action:Sj-Sk
- les connecteurs logiques apparaissant dans les liens entrées-mode et mode-sortie sont repris si besoin : @mode_n:Si&@mode_m:Si → action:Si-?.

Si par exemple un système Sa possède comme sortie une action de type "@Malware:Sa → Corruption trafic:Sa-?", qu'un autre système B a comme entrée-état "Corruption trafic:?:Sb → @Données reçues corrompues:Sb" et que les deux systèmes possèdent un lien de réseau d'information, alors un scénario @Malware sur A:Sa → Corruption trafic:Sa-Sb → @Données corrompues:Sb.

Il est possible de générer des arbres d'attaques à partir des scénarios complets. Compte tenu de la combinatoire, la génération explicite de tous les arbres est à éviter. Il est préférable de travailler directement sur modèle des interactions entre systèmes pour mettre en place les mesures de sécurité.

On notera que l'approche de composition de dysfonctionnement, qui reprend l'idée proposée par MOSAR a été aussi utilisée dans d'autres approches comme celles des modèles de propagation de pannes d'ALTARICA [30].

3.5 Mise en place des mesures

Chaque système possède des états de corruption. Les mesures à mettre en place doivent empêcher ou limiter l'activation de ces modes. Comme présenté sur la figure 9, les vulnérabilités et mesures de contrôle associées ont pour objectif de modifier la relation cause-effet entre une entrée et un état ou entre un état et une sortie. Sur une relation, plusieurs vulnérabilités peuvent exister, de façon conjonctive ou disjonctive. Les mesures de contrôles sont globales au niveau du système, et doivent être déclinées en pratique sur chaque élément concerné. Par exemple, si un état correspond à plusieurs éléments (par ex 10 postes), le état corrompu par malware concerne chaque poste.

Une mesure peut être technique, humaine ou organisationnelle. Sur un chemin, chaque mesure fait baisser la possibilité de la relation cause-effet. Par exemple, une mesure peut être la mise en place d'un pare feu et cette mesure sera renforcée par une mesure organisationnelle, comme mettre en place un processus périodique de gestion des règles.

La cotation des mesures se fait en évaluant le niveau de maîtrise du lien cause-effet. L'idée est de définir un niveau d'efficacité technique et un niveau organisationnel. Pour des raisons d'espace, cet aspect n'est pas développé plus enn détail dans le cadre de cette communication.

4. Mise en oeuvre

4.1 Exemple d'application

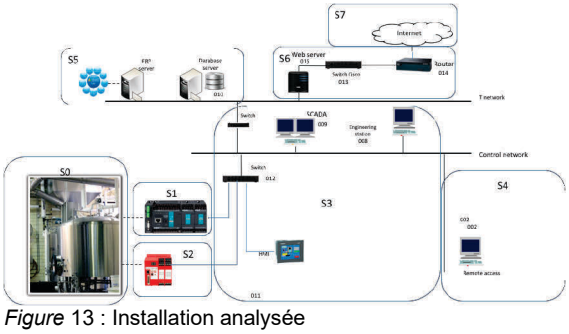

Figure 13 : Installation analysée

L'approche proposée a été évaluée sur un exemple d'installation de production de bière artisanale présenté sur la figure 13. Elle est composée d'un fermenteur piloté par un automate. Le système est relié au réseau d'entreprise.

4.2 Décomposition en système

Dans le cadre de cet exemple illustratif, le découpage réalisé est assez fin. Les systèmes identifiés sont les suivants :
S0 : Procédé de fabrication, le procédé physique,
S1 : PLC, composé de l'automate et du câblage,
S2 : SIS, composé de l'automate de sécurité,
S3: Scada, composé d'un switch, de câbles réseau, d'une HMI dédiée, de postes SCADA, d'un poste ingénieur et d'opérateurs
S4 : Remote support, composé d'un poste informatique, et d'un opérateur
S5 : Corporate network, le réseau informatique composé de postes, d'équipement réseau et des opérateurs
S6 : Webserver, composé de serveur web et routeur
S7 : Internet

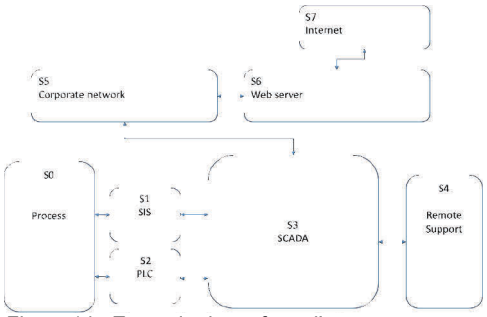

Figure 14 : Exemple de surface d'attaque

Les liens de données correspondant à des échanges de données par réseau d'information sont représentés sur la figure 14.

4.3 Analyse de risque

Un modèle de risque a été réalisé en utilisant la BMG dont un extrait est donné sur la figure 10. Seul le modèle E/S du système S3 est présenté pour des raisons de place.

Entrée	Mode de corruption
Accès illégal privilégié	(Corrompu par) Malware
Accès illégal user & Utilisation vulnérabilité OS	Elévation privilège (utilisateur à privilégié)
Connaissance Machine & Recherche vulnérabilité	Vulnérabilité découverte
Corruption trafic réseau	(Réception) Données corrompues depuis SCADA
Corruption trafic réseau	(Réception) Données corrompues depuis station ingénierie
Corruption trafic réseau	(Réception) Programme corrompu depuis station ingénierie
Hameçonnage	(Corrompu par) Malware
Hameçonnage	Identifiants volés
Propagation Malware & Utilisation vulnérabilité OS	(Corrompu par) Malware
Réception volume important requête	Surcharge unité centrale
Recherche identifiants par essai erreur ou force brute	Accès illégal PLC
Recherche identifiants par essai erreur ou force brute	Accès illégal utilsateur OU Accès illégal privilégié
Recherche prise RJ45 accessible	Accès illégal réseau
Scan réseau	Connaissance des machines réseau
Sur sollicitation E/S réseau	Surcharge unité centrale
Test identifiants par défaut	Accès illégal PLC
Test identifiants par défaut	Accès illégal utilisateur OU Accès illégal privilégié
Utilisation clé contaminée	(Corrompu par) Malware
Utilisation identifiants volés	Accès illégal utilisateur OU Accès illégal privilégié
Utilisation site web malveillant	(Corrompu par) Malware
Utilisation site web malveillant	Accès illégal utilisateur OU Accès illégal privilégié
Utilisation vulnérabilité	Accès illégal PLC
Utilisation vulnérabilité	Accès illégal utilisateur OU Accès illégal privilégié

Etat	Sortie
Identifiants volés	Accès illégal utilisateur OU Accès illégal privilégié
Données corrompues	Actions incorrectes (dommages)
Programme corrompu	actions incorrectes (dommages)
Données corrompues	Actions incorrectes (dysfonctionnement)
Programme corrompu	actions incorrectes (dysfonctionnement)
Accès illégal privilégié OU	Ajout script malveillant à site
Malware	web
Accès illégal PLC	Corruption données automate
Accès illégal PLC	Corruption pgm automate
Accès illégal privilégié OU Malware	Corruption trafic réseau
Données corrompues	Désactivation fonction sécurité
Programme corrompu	Désactivation fonction sécurité
Accès illégal utilisateur OU Accès illégal privilégié OU Malware	Destruction données
Accès illégal privilégié OU Malware	Ecoute trafic
Accès illégal réseau	Ecoute trafic
Accès illégal réseau	Ecoute trafic
Accès illégal privilégié OU Malware	installation Malware
Accès illégal réseau	Interception trafic
Accès illégal réseau	Interception trafic
Trafic intercepté et modifié (MitM)	Modifcation données envoyé à automate
Accès illégal privilégié OU Malware	Modification apparence site web
Trafic intercepté et modifié (MitM)	Modification consigne de Scada à automate
Accès illégal utilisateur OU Accès illégal privilégié OU Malware	Modification données
Trafic intercepté et modifié (MitM)	Modification données pour HMI Scada
Trafic intercepté et modifié (MitM)	Modification pgm envoyé à automate
Surcharge unité centrale	Panne
Données corrompues	Perte contrôle procédé
Programme corrompu	Perte contrôle procédé
Surcharge unité centrale	Perte contrôle procédé
Surcharge unité centrale	Perte service
Malware	Propagation par mail
Malware	Propagation via réseau
Accès illégal privilégié OU Malware	Scan réseau
Accès illégal réseau	Scan réseau
Accès illégal réseau	Scan réseau
Accès illégal privilégié OU Malware	Sur sollicitation E/S réseau
Accès illégal réseau & Connaissance type machine	Utilisation vulnérabilité
Connaissance des machines réseau	Utilisation vulnérabilité
Malware & Connaissance type machine	Utilisation vulnérabilité
Accès illégal aux données serveur	Vol données
Accès illégal utilisateur OU Accès illégal privilégié OU Malware	Vol données
Trafic écouté	Vol données

Figure 15 : Exemple de modèle de risque

En combinant les différents modèles, on obtient les scenarios. Un exemple de scénario obtenu est le suivant :

Hameçonnage :S6-S3->@Identifiants volés:S3 → Accès illégal:S3-S3 → @malware:S3 → Interception réseau:S3-S3 → @flux réseau modifié:S3(modification trames PLC) → modification données sur PLC:S3-S2 → @données modifiées: S2 → actions dommageables:S2-S0

Il représente le déroulement d'une attaque avancée sur l'ICS.
La mise en place des mesures peut être réalisée directement sur modèle de risque. Par exemple, pour la ligne 7 du modèle d'entrée de S3 et la première ligne du modèle de risque de sortie S3, on a

Entrée	Contrôle	Etat de corruption
Hameçonnage	Formation utilisateur	Identifiants volés

Etat	Contrôle	Sortie
Identifiants volés	Double identification	Accès illégal utilisateur OU Accès illégal privilégié

Les mesures n'empêchent pas complétement le passage dans un mode corrompu mais le limite.
Ces deux lignes apparaissent dans le scénario cité en exemple, et donc en limitent la probabilité d'occurrence.
Nous ne détaillerons pas la procédure de quantification. Notons seulement que l'impact s'évalue avec l'élément final et que la vraisemblance en examinant toute la chaîne action-> mode de corruption et en prenant en compte les mesures.

Les résultats obtenus sont intéressants. Ils ont permis de valider la BMG et les vulnérabilités et sources de menaces associées. L'analyse obtenue est un bon compromis entre une analyse détaillée et une simple checklist de bonnes pratiques. Elle permet de bien cibler les problèmes à résoudre pour maîtriser les risques de l'installation.
L'approche se base sur une checklist (BMG), ce qui peut a priori apparaître comme une limite à l'exhaustivité. Cependant la possibilité d'enrichir cette base de connaissance permet de converger vers une approche améliorant la répétitivité et le caractère systématique de l'analyse.

5. Discussion

L'objectif de ce travail était d'étudier l'intérêt d'une approche systémique pour l'analyse des risques des systèmes de contrôle industriels liés à la cyber-sécurité.
De façon synthétique, les étapes de la méthode, qui suit la démarche ISO27005, sont les suivantes :
- décomposition en systèmes, la taille permettant de déterminer la finesse de l'analyse (finesse au sens localisation des risques et non exhaustivité)
- analyse de façon relativement systématique grâce à une base de modèles de risques générique
- composition des modèles de risque pour obtenir les scénarios
- mise en place des mesures sur le modèle de risque

Les aspects positifs de cette méthode sont :
- qu'elle permet une construction homogène et systématique construction des scénarios en utilisant la modélisation en systèmes et la base de risques,
- qu'elle fournit implicitement une liste de tous les chemins d'attaque,
- qu'elle est bien adaptée au point de vue de défense en profondeur, puisqu'un scénario permet de lister les systèmes à franchir,
- qu'elle permet de factoriser les scénarios, ce qui évite de les répéter pour toutes les conséquences possibles, problème qu'on peut rencontrer dans les analyses centrées sur l'événement redouté,
- qu'elle permet de mettre en place les mesures de sécurité sur les modèles de risque (il n'est pas nécessaire de générer tous les scénarios possibles s'ils ont un chemin commun),
- qu'elle suite la démarche de l'ISO27005 et utilise un découpage compatible avec la notion de zone de la 62443.

Cependant, un élément clé de l'approche est la BMG. En fonction de la pertinence de celle-ci, l'analyse sera plus ou moins précise. Elle est basée sur le type d'élément contenu dans le système et structurée comme un modèle action/état, et état/action. Cette BMG offre une structuration intéressante de la connaissance et pour mieux s'adapter aux différents cas rencontrés, il sera nécessaire de capitaliser la connaissance en enrichissant la BMG.
Par ailleurs, l'approche peut être fastidieuse et complexe à mettre en place. Il serait donc intéressant de l'outiller pour faciliter la construction des modèles et ajouter des fonctionnalités permettant d'explorer tous les scénarios et valider le fait que chacun d'eux est maîtrisé.
Un outil automatique pourrait aussi permettre le partage de base de connaissances.

6. Conclusion

Ce papier a présenté une approche systémique pour l'analyse des risques en cybersécurité. Ce type de démarche utilisée pour l'analyse des risques industriels n'avait pas encore été adapté pour la cybersécurité.
Une approche basée sur ce principe a donc été proposée. Elle suit des étapes assez classiques : décomposition en systèmes, analyse des risques de ces systèmes de façon globale s'appuyant sur une base de connaissance, composition de ces modèles, génération des scénarios et mise en place des mesures au niveau du système.
La plupart des attaques se déroulent en plusieurs phases, et en utilisant des relais. Utiliser une approche systémique permet de capturer ce mécanisme comme cette étude le montre. L'approche proposée présente donc un intérêt et offre une base qui se prête bien au développement d'un outillage logiciel.
Par ailleurs, l'analyse par scénarios permettent de quantifier le risque en examinant la vraisemblance de chaque chemin. Cet aspect sera développé dans de futures communications.

Références

[1] Williams, T.J.. (1990). A Reference Model for Computer Integrated Manufacturing from the Viewpoint of Industrial Automation. IFAC Proceedings Volumes. 23. 281-291. 10.1016/S1474-6670(17)51748-6.

[2] ISA-62443-1-1, Security for industrial automation and control systems Models and Concepts. Draft 6 Edit 2, 2016,

[3] The State of Industrial Cybersecurity 2017 - Kaspersky Lab, Global Report, Accessed March 2018. https://go.kaspersky.com/rs/802-IJN-240/images/ICS%20WHITE %20PAPER.pdf

[4] Fortinet Q4 2017 Threat Landscape Report, Threat Landscape Report Q2 2017'. Fortinet. Accessed March 2018. https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/threat-report-q4-2017.pdf

[5] WannaCry, https://ics-cert.us-cert.gov/sites/default/files/FactSheets/ICS-CERT_FactSheet_WannaCry_Ransomware _S508C.pdf

[6] Risk Analysis: Socio-technical and Industrial Systems, Jean-Marie Flaus, 2013, John Wiley & Sons.

[7] H Abdo, M Kaouk, JM Flaus, F Masse, A safety/security risk analysis approach of Industrial Control Systems: A cyber bowtie–combining new version of attack tree with bowtie analysis
Computers & Security 72, 175-195

[8] F. Massé, H. Abdo, J.M. Flaus, Vers une approche intégrant les exigences de cybersécurité à la maîtrise des risques d'accidents majeurs pour les ICPE, F. Massé, H. Abda, J.M. Flaus, Qualita, 2017

[9] J. Cusinamo, Safety requires cybersecurity, Control Enginnering, March 2017

[10] J.M. Flaus, Cybersécurité industrielle: SCADA et Internet des Objects Industriels, ISTE, collection Sciences, 2018.

[11] Negrichi, K., Di Mascolo, M., & Flaus, J.-M. (2017). A model based approach to assess the performance of production systems in degraded mode. *International Journal of Production Research*, *55*(8), 2288–2303.

[12] Secrétariat général de la défense nationale – Direction centrale de la sécurité des systèmes d'information, Leaflet on The EBIOS Method, Expression of Needs and Identification of Security Objectives, 2010

[13] ISO/IEC 27002:2013 - information technology – security techniques – code of practice for information security management. Technical report

[14] Cybersecurity for Industrial Control Systems, ANSSI, 2014

[15] Expression des Besoins et Identification des Objectifs de Sécurité, EBIOS, ANSSI, 2010

[16] Flaus, J.-M. Risk analysis, 2013, Wiley, ISBN: 9781848214927

[17] Ralston, P. a S., Graham, J. H., & Hieb, J. L. (2007). Cyber security risk assessment for SCADA and DCS networks. *ISA Transactions*, *46*(4), 583–594. http://doi.org/10.1016/j.isatra.2007.04.003

[18] Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H., & Stoddart, K. (2016). A review of cyber security risk assessment methods for SCADA systems. *Computers & Security*, *56*, 1–27.

[19] A model-based approach for systematic risk analysis, J-M Flaus, Safety and Reliability for Managing Risk ESREL'11, 2011, Troyes, France, France. 1 p., 2011

[20] C. Girard, P. David, E. Piatyszek, and J.-M. Flaus. Emergency Response Plan: Assessement Based on Model with Multi-State Degradation. *Safety Science*. Vol. 85 pp230-240.

[21] Manadhata, P. K., & Wing, J. M. (2010). An Attack Surface Metric. IEEE Transactions on Software Engineering

[22] Howard, M., Pincus, J., & Wing, J. (2002, February 11). Measuring Relative Attack Surfaces, from Carnegie Mellon School of Computer Science: http://www.cs.cmu.edu/ ~wing/publications/Howard-Wing03.pdf

[23] Gee-Yong Park, Dong Hoon Kim, Dong Young Lee, Software FMEA analysis for safety-related application software,Annals of Nuclear Energy, Volume 70, 2014, Pages 96-102,

[24] Dennis P. Nolan, Chapter 5 - Specialized Reviews—CHAZOP, EHAZOP, Bow-Tie Analysis, Layers of Protection Analysis, Safety Integrity Level, Fishbone Diagram, and Cyber Security Vulnerability Analysis, In Safety and Security Review for the Process Industries (Fourth Edition), Gulf Publishing Company, 2015, Pages 17-27, ISBN 9780323322959,

[25] La modélisation des systémes complexes, Jean-Louis Lemoigne, Dunod 1990

[26] Perihlon Pierre, MOSAR : Présentation de la méthode, Techniques de l'ingénieur, article se 4060,2003

[27] El Hajj, Carine, Méthodologie pour l'analyse et la prévention du risque d'accidents technologiques induits par l'inondation (Natech) d'un site industriel, thèse de doctorat, EMSE, 2013,

[28] ENISA, Threat Landscape and Good Practice, 2015, https://www.enisa.europa.eu/publications/iitl/at_download/fullReport, last accessed April 2018.

[29] A. Rauzy and C. Blériot-Fabre, "Model-Based Safety Assessment: Rational and trends," *2014 10th France-Japan/ 8th Europe-Asia Congress on Mecatronics (MECATRONICS2014- Tokyo)*, Tokyo, 2014, pp. 1-10.

[30] Shaojun Li, Xiaoxun Li,Study on Generation of Fault Trees from Altarica Models, Procedia Engineering, Volume 80, 2014, Pages 140-152.