EBIOS pour les systèmes industriels

Jean-Marie Flaus, Jean Caire

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

EBIOS pour les systèmes industriels

EBIOS for Industrial Control Systems

CAIRE Jean
RATP
jean.caire@ratp.fr

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

Résumé — EBIOS est une méthode proposée oar l'ANSSI pour l'analyse de risque des systèmes informatiques et identifier les mesures de sécurité à mettre en œuvre. Les systèmes informatiques industriels présentent la spécificité d'être à même de pouvoir créer des dommages dans le monde physique en plus du monde numérique. Ce travail présente une instanciation de la méthode EBIOS pour cette classe de système. Il vise à proposer une approche générique permettant de construire des scénarios en s'appuyant sur des bases de connaissance qu'il est possible de raffiner progressivement. L'objectif est d'adopter un point de vue similaire à celui de la Sûreté de Fonctionnement pour une maîtrise rigoureuse des risques

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

Abstract— EBIOS is a method proposed by ANSSI for analyzing the risks of IT systems and identifying the security measures to be implemented. Industrial computer systems have the specificity of being able to create damage in the physical world in addition to the digital world. This work presents an instantiation of the EBIOS method for this class of system. It aims to propose a generic approach for building scenarios based on knowledge bases, which can be gradually refined. The objective is to adopt a point of view similar to that of the system safety for a rigorous control of the risks

Keywords — Cybersecurity, Risk analysis, Safety.

I. INTRODUCTION

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 les vulnérabilités potentielles 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, le standard NIST SP 800-82 ou les guides de l'ANSSI ([2], [3], [4]).

Dans toutes ces approches, une étape importante qui doit être réalisée au début du processus, puis de façon périodique, est l'analyse de risque. Cette analyse qui est au cœur du processus de maîtrise des risques (Fig. 4) est d'une importance capitale ; cependant le choix de la méthode est généralement laissé à l'appréciation de l'analyste.

EBIOS Risk Manager (EBIOS RM) est la méthode d'appréciation et de traitement des risques numériques publiée par l'Agence nationale de la sécurité et des systèmes d'information (ANSSI) avec le soutien du Club EBIOS. Elle propose une boite à outils adaptable, dont l'utilisation varie selon l'objectif du projet, et est compatible avec les référentiels normatifs en vigueur en matière de gestion des risques comme en matière de sécurité du numérique. Toutefois elle a d'abord été conçue pour les systèmes IT.

L'objectif de ce travail est donc de proposer une adaptation de la méthode EBIOS pour les systèmes industriels.

II. CONTEXTE

A. La méthode EBIOS

La méthode EBIOS Risk manager se compose de 5 ateliers :

- L'atelier 1 a pour but de définir le cadre de l'étude, ses périmètres métier et technique, les événements redoutés associés et le socle de sécurité. Cet atelier est un prérequis à la réalisation d'une appréciation des risques.
- L'atelier 2 a pour objectif d'identifier les sources de risque (SR) et leurs objectifs visés (OV), en lien avec le contexte particulier de l'étude. Il vise à répondre à la question suivante : qui ou quoi pourrait porter atteinte aux missions et aux valeurs métier identifiées dans l'atelier 1, et dans quel but ?
- L'objectif de l'atelier 3 est, d'abord, de disposer d'une vision claire de l'écosystème, afin d'en identifier les parties prenantes les plus vulnérables, ensuite, de bâtir des scénarios de haut niveau, appelés scénarios stratégiques. Ces derniers sont autant de chemins d'attaque depuis l'écosystème que pourrait exploiter une source de risque pour atteindre son objectif.
- L'atelier 4 permet alors de construire des scénarios opérationnels. Ils schématisent les modes opératoires que pourraient mettre en œuvre les sources de risque pour réaliser les scénarios stratégiques.

- Le but l'atelier 5 est d'effectuer une synthèse des scénarios de risque retenus et de définir une stratégie de traitement du risque. Cette stratégie aboutit à la définition de mesures de sécurité, recensées dans un plan d'amélioration continue de la sécurité (PACS).

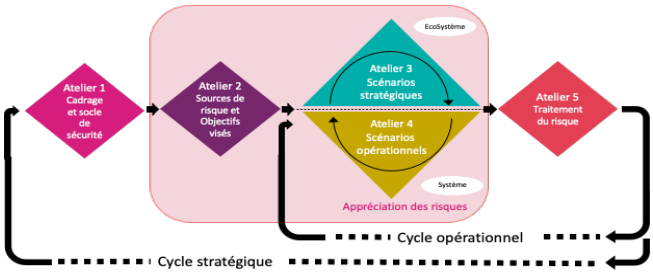

Fig. 1 Ateliers de la méthode EBIOS

B. Spécificités des systèmes industriels

Les systèmes de contrôle industriels (ICS) sont des systèmes informatiques particuliers. Leur objectif est de piloter un système physique qui permet de produire des biens ou des services (Fig. 2). Le système physique piloté par un système informatique est souvent appelé système cyber-physique.

Le schéma général de fonctionnement de ce type de système est présenté sur la figure 2. L'objectif de la maîtrise des risques pour ces systèmes est de garantir qu'aucun événement redouté (ER) ne pourra porter atteinte à l'intégrité ou à la disponibilité de l'ensemble. Les ER peuvent, d'une part, avoir une origine informatique, physique ou mixte, et, d'autre part, entraîner des conséquences sur la partie informatique, la partie physique ou les deux.

La Sûreté de Fonctionnement (SdF), définie comme la maîtrise des défaillances ([19]), vise alors à réduire à un niveau acceptable les risques liés à la partie physique, dont les causes peuvent être techniques comme humaines, en garantissant la disponibilité du système physique et en évitant les dommages physiques.
Bien souvent, les moyens utilisés pour garantir la SdF sont basés sur une technologie électronique et informatique.

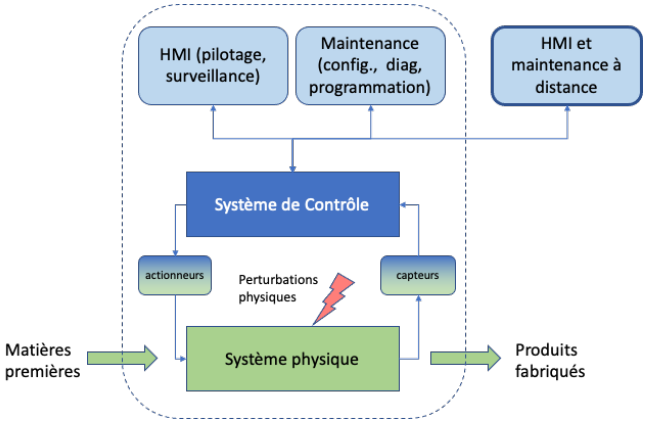

Fig. 2 Principales fonctions d'un ICS

Les différents éléments d'un ICS sont souvent représentés selon une certaine structure appelée architecture CIM (Fig. 3). Celle-ci est subdivisée en 5 niveaux en partant du système physique.

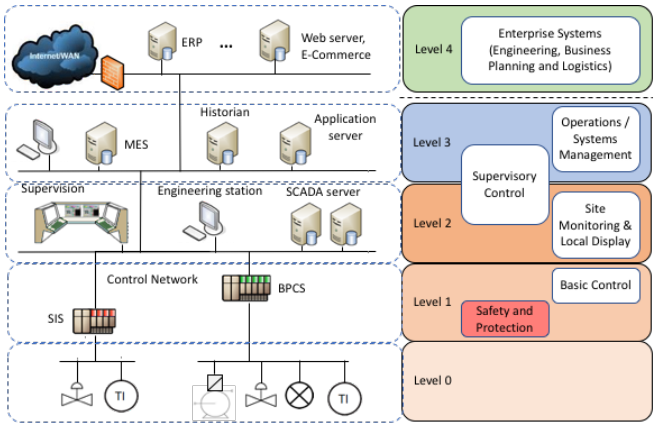

Fig. 3 Architecture CIM

Le niveau 0 est composé des capteurs et actionneurs, le niveau 1 contient les éléments de pilotage réactifs (PLC) plus les équipements de sécurité (SIS), les niveaux 2 et 3 assurent, eux, les fonctions de supervision et l'interface homme-machine.

Idéalement, la connexion à l'informatique IT se fait par le dernier niveau mais ce n'est pas toujours le cas en pratique. En outre, des architectures plus ouvertes, avec une partie des fonctionnalités distribuées dans le *Cloud* et des connexions à différents niveaux se rencontrent de plus en plus (Fig. 4).

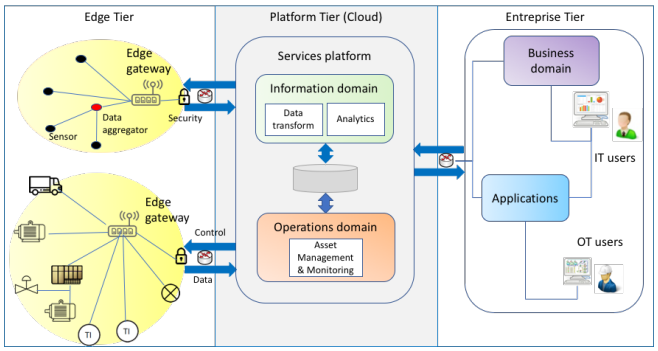

Fig. 4 Architecture Cloud

III. METHODOLOGIE

La combinaison de la complexité des systèmes, la diversité et le nombre de leurs interactions avec l'environnement ainsi que l'importance des enjeux font de la Cybersécurité des systèmes industriels un problème réellement difficile.

Pour le résoudre, il est nécessaire d'adopter une approche systémique qui concilie une vision holistique des situations – où l'ensemble des entités en jeu et de leurs interactions successives sont prises en compte – avec des exigences d'assurance clairement spécifiées.

Il faut donc :

- développer un modèle global qui intègre toutes les variables du problème dans une même représentation en assurant leur parfaite cohérence ;

- disposer de règles de raffinement permettant d'introduire progressivement le détail de la modélisation afin de conduire des raisonnements rigoureux et maîtrisés.

En particulier, l'Attaquant, ses caractéristiques propres et ses relations avec le Système cible ou l'Environnement, ainsi que ses activités doivent être représentés dans ce modèle intégral.

Cette démarche est simplement une évolution et une adaptation de l'approche classique définie dans des standards comme l'IEC 61508, où la SdF est fondée sur un cycle de vie spécifique qui permet d'appréhender progressivement et méthodiquement les situations dangereuses.

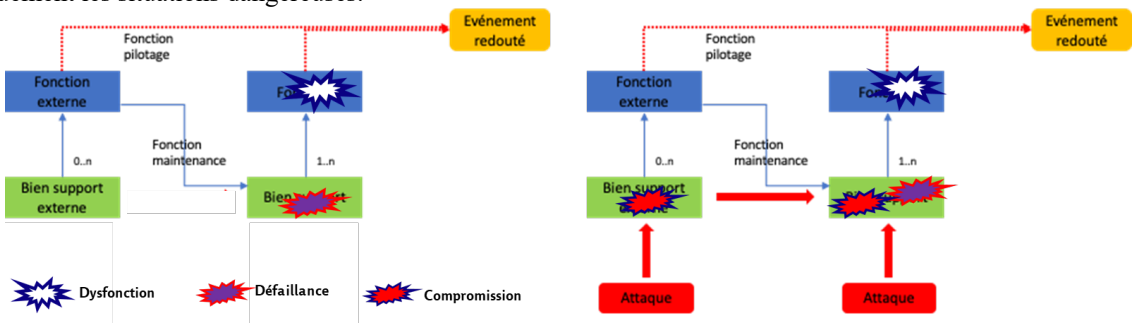

Fig. 5 Sûreté de Fonctionnement et cyberattaques

Ce raisonnement permet de développer des scénarios d'attaque et de les insérer dans les modèles de la SdF comme les arbres de défaillance.

Si la Cybersécurité, tout comme la SdF, repose sur le paradigme de la Maîtrise du risque, en revanche l'appréciation des risques en Cybersécurité est très différente : le déclenchement d'une attaque résulte de la décision d'une intelligence hostile qui repose, en toute rationalité, sur un calcul de type Gain/Coût. La stratégie de défense doit donc chercher modifier ces paramètres en la défaveur de l'attaquant.

Dans ce cadre, les modèles du système étudié développés pour la SdF ont un double intérêt pour la Cybersécurité : d'abord ils fournissent un ensemble de représentations du système pleinement applicables (si l'on sait comment y projeter les séquences d'événements constituant les scénarios), ensuite ils déterminent le niveau de détail des modèles complémentaires qu'il faudra développer et intégrer pour mener à bien l'étude de Cybersécurité.

S'agissant de systèmes critiques, il est indispensable de construire puis d'analyser les scénarios d'attaque avec un très haut niveau de détail et de rigueur. Pour ce faire, nous avons fait le choix d'utiliser la base ATT@CK-ICS du MITRE, qui est incontestablement la plus complète publiée à ce jour.

Cependant, sa mise en œuvre pose deux difficultés particulières :

- la base ATT@CK est très riche mais elle ne fournit pas de règles explicites pour composer ses éléments (les stéréotypes d'attaque) afin de construire les scénarios ;

- la pluralité des stéréotypes d'attaque et, par suite, la diversité des options possibles pour un événement donné peuvent entraîner l'explosion du nombre de scénarios au delà de ce qui est gérable.

Un point fondamental concerne l'impact potentiel des cyberattaques sur la SdF : il s'agit précisément de déterminer les conditions dans lesquelles une cyberattaque peut provoquer un ER malgré le déploiement de mesures de SdF.

En SdF, les ER sont les conséquences des dysfonctions des fonctions essentielles causées par les défaillances de leurs composants critiques. De fait, une cyberattaque qui parvient à corrompre ou paralyser un composant critique, provoquant ainsi sa défaillance, peut conduire à un ER (Fig. 5).

Pour répondre à ces deux points, nous proposons une démarche fondée sur l'élaboration progressive d'un système de défense complet en raffinant pas à pas les modes d'attaque, depuis les ER jusqu'aux scénarios détaillés, et en intégrant à chaque phase des mesures de défense qui réduisent graduellement la liberté d'action de l'attaquant.

La mise en œuvre s'appuie sur un ensemble cohérent de bases de connaissance et de règles préalablement développées dans [11].

Il faut noter que nous excluons de cette communication les attaques visant spécifiquement la chaîne logistique qui appellent une étude tout à fait particulière.

IV. ADAPTATION DE LA METHODE

A. Généralités

Pour illustrer notre propos, nous considérerons un système de contrôle industriel générique que nous allons compléter et détailler au fur et à mesure de l'analyse EBIOS.
Notre contribution se situe à chaque étape de la méthode EBIOS, en proposant des solutions génériques pour instancier la méthode EBIOS sur les systèmes industriels.

B. Atelier 1 : cadrage et socle de (cyber)sécurité

Pour l'atelier 1, nous proposons à la fois un canevas pour modéliser l'installation en tenant compte de l'architecture des ICS et un cadre spécifique pour l'analyse des ER en intégrant la SdF.

1) Cadrage

Pour notre exemple, nous considérons qu'une étude de SdF a démarré et que les principales capacités opérationnelles du système ont été identifiées.
De plus, nous nous limiterons aux ER liés aux dommages aux biens et aux personnes, identifiés par les analyses préliminaires de SdF.

2) Système

La première étape de l'atelier 1 consiste à représenter le système dans son environnement (Fig. 6).

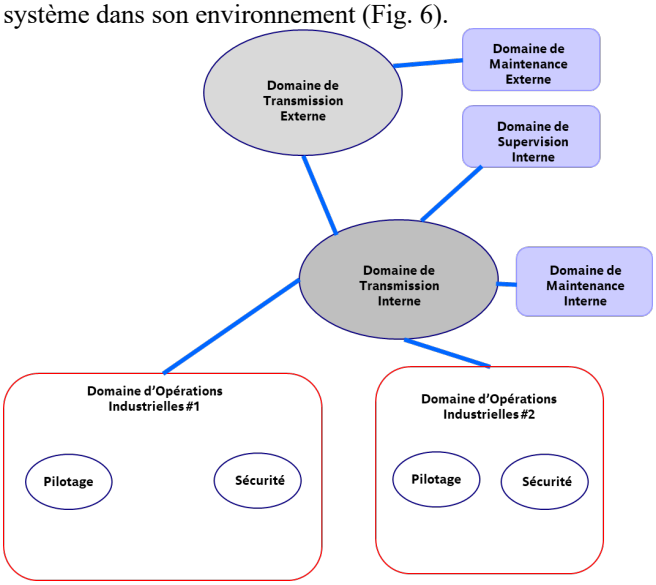

Fig. 6 Graphe des capacités opérationnelles de l'ICS

De façon générale, les missions d'un ICS participent de trois catégories [16] :

- Pilotage du système : ces fonctions gèrent le contrôle et la surveillance des processus. On peut distinguer des sous-fonctions :
  - Contrôle du processus dans des conditions de fonctionnement définies
  - Optimisation pour obtenir un produit de qualité
    - Surveillance du processus par l'opérateur
    - Journalisation des alarmes/événements et des historiques

- Sûreté : fonctions destinées à protéger le personnel, l'unité de production et l'environnement en amenant le processus à un état sûr.

- Maintenance et Ingénierie : fonctions de configuration, diagnostic et entretien des systèmes des Unités de production.

Dans notre exemple, on sépare les fonctions réalisées en interne de celles exécutées depuis l'extérieur par un tiers.

3) Evénement redoutés

La guide EBIOS-RM suggère d'identifier les ER en étudiant les atteintes aux attributs Disponibilité, Intégrité, Confidentialité sur les valeurs métier. Cette approche est inadaptée aux spécificités des systèmes industriels et nous choisissons plutôt d'exprimer les ER à partir de la base ATT@CK-ICS :

Impact	Description
Damage to Property	*To cause damage to infrastructure, equipment, and the surrounding environment when attacking ICS*
Denial of Control	*To prevent temporarily operators and engineers from interacting with process controls*
Denial of View	*To attempt to disrupt and prevent operator oversight on the status of an ICS environment*
Loss of Availability	*To attempt to disrupt essential components or systems to prevent owner and operator from delivering products or services*
Loss of Control	*To achieve a sustained loss of control or a runaway condition in which operators cannot issue any commands*
Loss of Productivity	*Loss of productivity and revenue through disruption and even damage to the availability and integrity of ICS operations, devices, and related processes*
Loss of Protection	*To compromise protective functions designed to prevent the effects of faults or abnormal conditions.*
Loss of Safety	*To compromise safety system functions designed to maintain safe operation of a process when unacceptable or dangerous conditions occur.*
Loss of View	*To cause a sustained or permanent loss of view where the ICS equipment will require local, hands-on operator intervention*
Manipulation of Control	*To manipulate physical process control within the industrial environment*
Manipulation of View	*To attempt to manipulate the information reported back to operators or controllers.*
Theft of Operational Information	*To steal operational information on a production environment as a direct mission outcome for personal gain or to inform future operations.*

Tab. 1 ATT@CK-ICS : Tactique Impact

4) Socle de sécurité

A ce stade, le socle n'existe pas à proprement parler mais on applique un ensemble coordonné de **Principes Directeurs** (cf. [12,13]) :

Principes	Description
Partition	Le système est subdivisé en domaines de sécurité selon la criticité des fonctions
Réduction	Les interfaces constituant la surface d'attaque sont énumérées et minimisées
Compacité	Les interfaces sont contrôlées par des Moniteurs de référence, les vulnérabilités des composants sont éliminées ou couvertes
Modularité	Les services et les composants sont remplaçables
Vigilance	L'état du système, tout particulièrement celui des domaines critiques, est surveillé en permanence
Défense en Profondeur	La compromission des domaines moins robustes est anticipée, la défense s'adapte tout en ralentissant la progression de l'attaque

Tab. 2 Exemples de Principes stratégiques de Sécurité

C. Atelier 2 : Sources de risque

Au niveau de l'atelier 2, nous intégrons les Sources de risque dans le modèle précédent.

1) Identifier les Sources de risque et leurs Objectifs

Le guide EBIOS-RM fournit des caractères de description clairs mais il ne propose pas de méthode pour modéliser ces Sources de Menace avec le niveau de détail requis.

De manière plus générale, cette question est délicate car :
- l'analyse de la Menace ressortit d'abord aux Services de l'Etat comme le rappelle le Code de la Défense ;

- pour être pleinement opérante, cette analyse doit être contextualisée dans le cadre particulier du système étudié en s'appuyant sur l'opérateur du système.

Nous proposons ici de décrire les Sources de risque par leur signature (***Intention***, ***Capacités***, ***Opportunités***) où l'Intention est une constante qui exprime le projet spécifique de l'Attaquant, tandis que les Capacités et Opportunités sont des variables représentant respectivement la combinaison des ***Connaissances*** & ***Aptitudes*** de l'Attaquant et les ***Accès*** qu'il peut exploiter pour engager la cible et manœuvrer en son sein.

Nous retenons pour la suite, une Source de risque étatique dont l'Intention est de provoquer un accident industriel.

Pour représenter les Capacités, on applique la structure définie dans [14]. Il faut souligner qu'il s'agit des capacités effectives (i.e. celles que l'Attaquant est prêt à mobiliser pour cette opération particulière) et non ses capacités totales qui sont plus étendues (Fig.7).

Les Opportunités se déduisent naturellement de la structure du graphe des capacités opérationnelles, c'est pour cela qu'il est fondamental de ne pas se contenter d'un simple inventaire des ressources du système mais identifier aussi leurs dépendances.

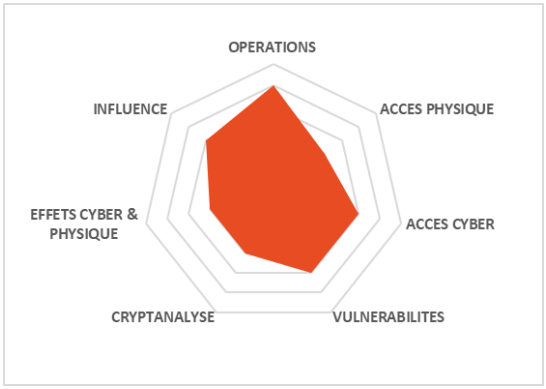

Fig. 7 Profil capacitaire de la Source de Menace

2) Evaluer les couples Sources / Objectif

Pour notre étude, L'Objectif stratégique est réexprimé sous la forme d'ER qui vont entraîner l'accident industriel.

De plus, on exploite la description précédente du système ciblé afin de décliner les objectifs sous la forme d'options stratégiques qui seront affinées durant l'atelier 3.
On applique alors la Grammaire d'Attaque Stratégique ([11]), cf. Fig. 8.

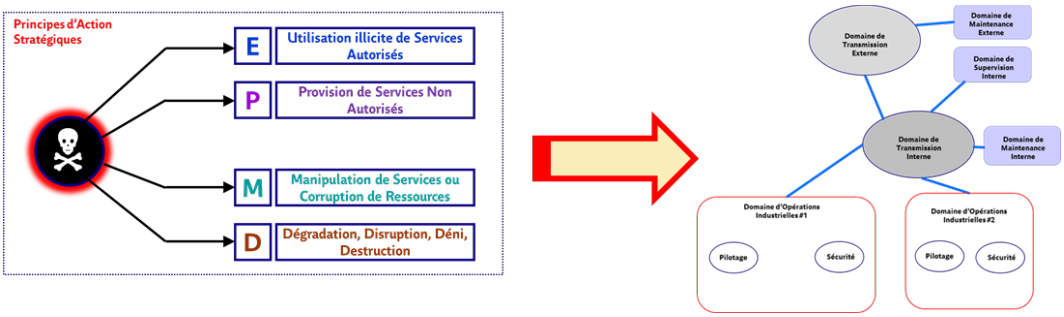

Fig. 8 Détermination des Options de l'Attaquant

L'exemple ci-dessous (Fig. 9) présente trois macro-scénarios d'attaque (sachant qu'il en existe beaucoup plus).

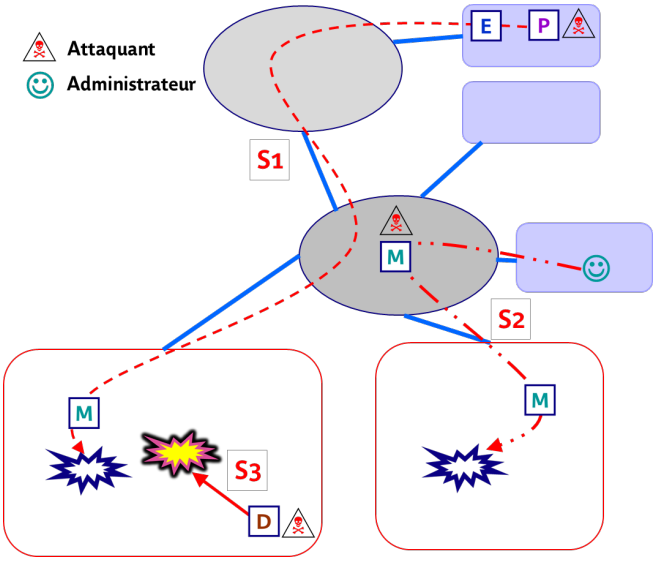

Fig. 9 Options stratégiques de l'Attaquant

S1 : l'Attaquant **usurpe** le domaine d'administration externe, puis **exploite** les fonctions d'administration pour **modifier** le processus industriel afin de provoquer un accident.

S2 : l'Attaquant, qui **contrôle** le domaine de transmission, **modifie** l'exécution d'une fonction pour **corrompre** le processus industriel afin de provoquer un accident

S3 : l'Attaquant, qui est **entré** physiquement dans l'Unité de Production 1, **sabote** une fonction de sécurité afin de provoquer un accident.

3) Identification des Options de Défense

De la même façon que précédemment, on peut alors exploiter les modèles obtenus pour identifier des Options Stratégiques de Défense et les allouer dans le système.

On applique alors la Grammaire de Défense Stratégique ([11]) (Fig.10).

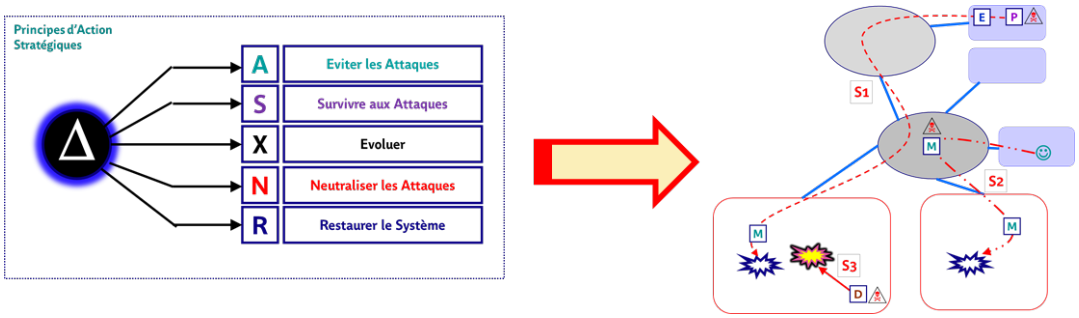

Fig 10. Détermination des Options du Défenseur

Cette méthode permet de chercher de manière systématique les options possibles du Défenseur. L'idée n'est pas de superposer toutes les mesures de Défense mais de sélectionner les combinaisons les plus pertinentes.

Le raisonnement est similaire à celui mis en œuvre pour identifier les Options stratégiques de l'Attaquant (Fig. 11).

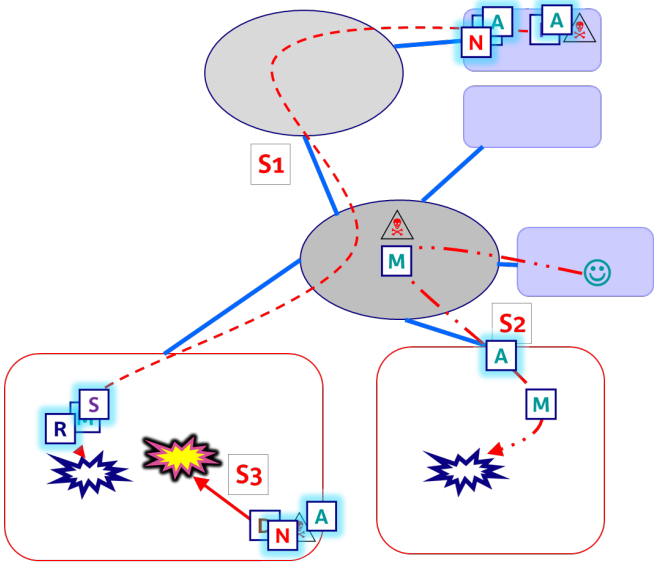

Fig. 11 Options stratégiques du Défenseur

D1 : **Empêcher** la prise de contrôle du domaine d'administration externe, **Dissuader** ou **Evincer** un Administrateur compromis, **Limiter** les possibilités d'action distante contre le processus industriel.

D2 : **Immuniser** la transmission entre le domaine de maintenance interne et l'unité de production 2 contre les modifications d'informations en transit.

D3 : **Empêcher** l'Attaquant de pénétrer dans l'Unité de Production 1 ; **Neutraliser** le plus rapidement tout intrus.

Il faut noter que **D2** se réduit à une fonction unique parce qu'elle fournit une Assurance très forte compte tenu du seuil des capacités de cryptanalyse de l'Attaquant retenu.

D. Atelier 3 : scénarios stratégiques

Dans cet atelier nous produisons une nouvelle suite de modèles en raffinant les précédents de manière cohérente.

1) Construire la cartographie de l'écosystème

En fait, nous disposons déjà d'une carte de haut niveau avec le graphe des capacités opérationnelles, identifiant les parties prenantes pour des services OT externes (e.g. supervision).

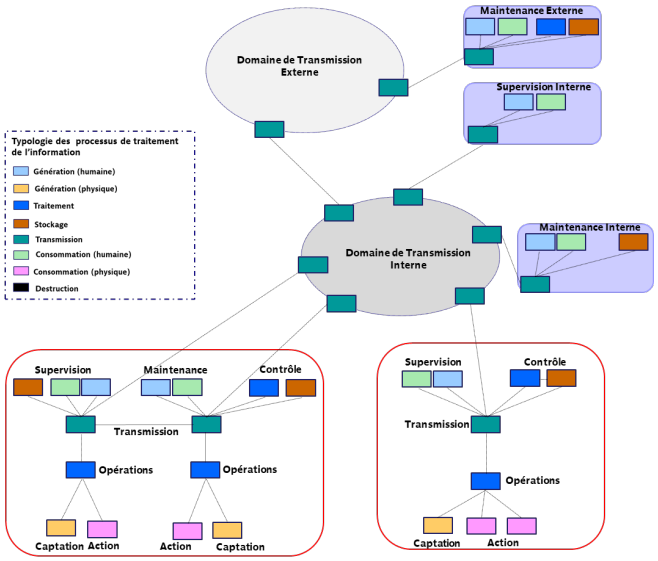

Fig. 12 Architecture informationnelle du Système

Cette représentation décompose le graphe des capacités opérationnelles en une combinaison de processus canoniques qui spécifient le cycle de vie des informations ([17], [18].

Les principales caractéristiques de ce modèle sont :

- **Réticulation** : les processus de traitement des données numériques sont les nœuds d'un graphe fonctionnel.
- **Structure hologrammatique** ([20]) : on peut décomposer un processus en un graphe de sous-processus, ce qui permet de choisir le niveau de détail des analyses.
- **Stratification** : les processus se répartissent dans les trois strates du cyberespace, ce qui permet de visualiser immédiatement l'hypersurface d'attaque.
  On fait apparaître en particulier les interfaces avec, d'une part, les individus et, d'autre part, les machines par les processus de génération et de consommation d'information.

2) Elaborer les scénarios stratégiques

Les scénarios stratégiques au sens d'EBIOS-RM sont en fait les Lignes d'Opération de l'Attaquant au sens de [15].

Pour les obtenir, nous raffinons les macro-scénarios en utilisant une nouvelle grammaire ([11]).

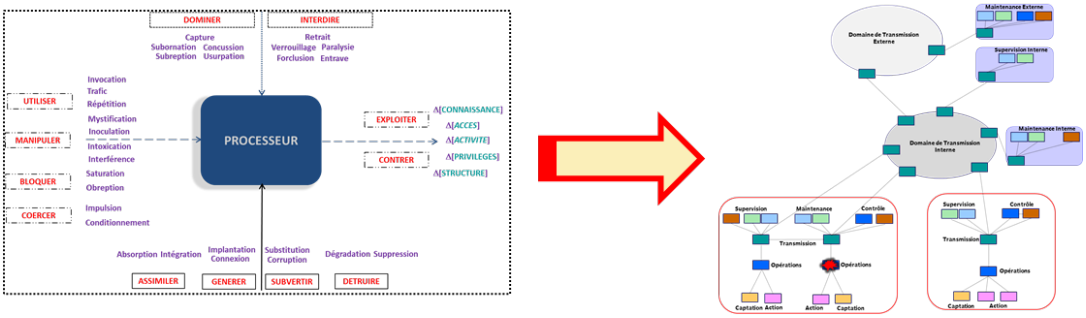

Fig 13. Lignes d'Opération de l'Attaquant

Seul le macro-scénario **S1** est analysé (cf. plus haut), il se subdivise en plusieurs Lignes d'Opération (Fig. 14).

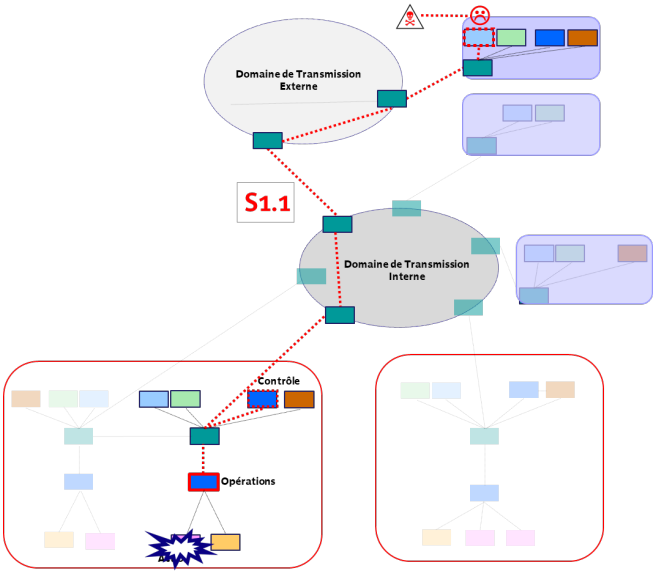

Fig 14. Ligne d'Opération S1.1

- **S1.1** : l'Attaquant **recrute** un administrateur externe qui **envoie des commandes illicites** au serveur SCADA afin de faire **exécuter** par le PLC des actions non autorisées dans le contexte.

- **S1.2** : l'Attaquant **pénètre physiquement** dans le domaine d'administration externe, puis **prend le contrôle** d'un poste d'administrateur et **envoie des commandes illicites** au serveur SCADA afin de faire **exécuter** par le PLC des actions non autorisées dans le contexte.

- **S1.3** : l'Attaquant **prend le contrôle,** par une cyberattaque depuis Internet, du serveur d'administration externe, puis le **subvertit** en insérant un malware ; le serveur **injecte** le malware dans le serveur SCADA ; le malware **envoie des commandes illicites** au serveur SCADA afin de faire **exécuter** des actions non autorisées dans le contexte par le PLC.

Les raisonnements menés à l'atelier 2 sur **S2** et **S3** peuvent être reconduits : il suffit de bien spécifier les options de Défense physique et cybernétique sur le Domaine de Maintenance externe en imposant par exemple que ce soit une *enclave protégée physiquement* par des moyens robustes pour bloquer les scénarios **S1.2** et **S1.3** pour l'Attaquant retenu.

Ces fonctions de sécurité physique devraient être implémentées dans l'atelier 5 dans le cadre du contrat qui lie l'Opérateur eux tiers chargés des services externes.

3) Définir les mesures de sécurité

L'élaboration des Lignes de Défense s'effectue en suivant le même schéma.

On applique alors la Grammaire de Défense Opérative [11].

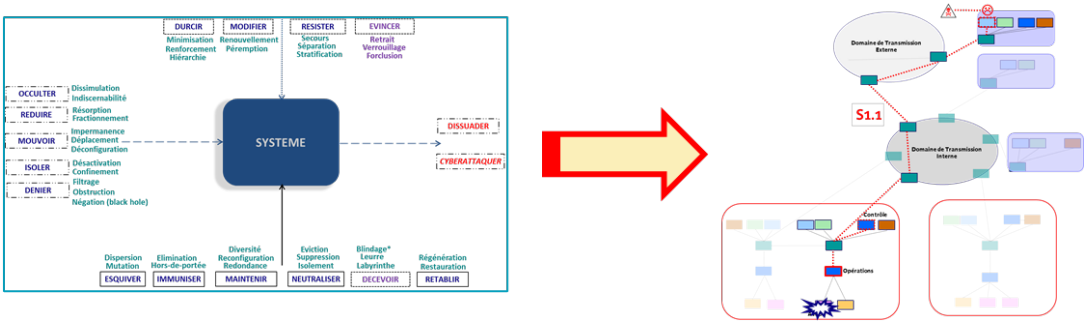

Fig. 15 Lignes d'Opération du Défenseur

De nouveau, la grammaire permet la recherche systématique de toutes les fonctions de défense (Fig. 16).

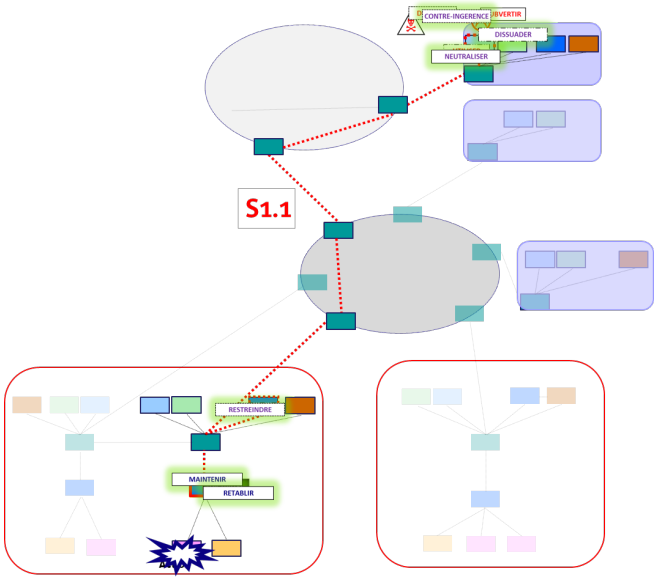

Fig. 16 Lignes de Défense contre S1.1

La comparaison des capacités élevées de l'Attaquant retenu en matière d'influence avec l'efficacité modérée des techniques de contre-ingérence montre qu'on ne peut pas limiter la défense au niveau du domaine de maintenance externe et qu'il faut poursuivre l'analyse du scénario **S1.1**.

De même, les deux fonctions de **D3** (cf. *C.3*) seront suffisantes si elles sont implémentées par des moyens de sécurité physique (e.g. contrôle d'accès, alarmes etc.) robustes.

Par conséquent, il ne sera pas nécessaire de poursuivre l'analyse des macro-scénarios **S2** et **S3** pour l'Attaquant retenu.

Sur notre exemple, nous obtenons le résultat suivant :

- **D1.1** : **Immuniser** les Administrateurs contre les compromissions par le recrutement, la formation et la vigilance entre administrateurs ; **Dissuader** un Administrateur indélicat par la surveillance ; **Limiter** les possibilités d'administration externes ; **Bloquer** les opérations d'administration non spécifiées ou non autorisées dans le contexte ; **Rétablir** rapidement les situations nominales en cas d'incident

E. Atelier 4 : scénarios opérationnels

Outre la partie industrielle (**OT**), ce modèle introduit principales fonctionnalités informatiques (**IT**) utiles pour faire fonctionner les systèmes de pilotage des unités de production ou offrir des services de support à distance.

De plus, pour assurer la cohérence du modèle on prend également en compte les services d'administration et de maintenance de nouvelles fonctionnalités **IT** pour faire fonctionner les systèmes de pilotage des unités de production ou offrir des services de support à distance.

Il faut préciser que ces services supplémentaires accroissent la surface d'attaque : les nouveaux chemins vers les composants névralgiques doivent donc impérativement être pris en compte dans les raffinements ultérieurs des scénarios.

Cependant, comme ils n'interviennent pas dans le scénario **S1.1**, nous ne les étudierons pas plus avant dans ce papier.

De plus, pour assurer la cohérence du modèle, on prend également en compte les services d'administration et de maintenance de nouvelles fonctionnalités.

Les fonctions essentielles de l'ICS, présentées dans l'atelier 1, sont alors implémentées :

- Le pilotage du système est réalisé par des composants BPCS qui prennent les entrées des capteurs et des instruments de processus et fournissent une sortie basée sur les fonctions de contrôle, conformément à la stratégie de contrôle de conception approuvée.

- La fonction de sécurité est assurée par des Systèmes Instrumentés de Sécurité (SIS) ; ils sont composés de capteurs, de solveurs logiques et d'éléments de contrôle finaux conçus pour protéger le personnel, l'équipement et l'environnement en amenant le processus à un état sûr.

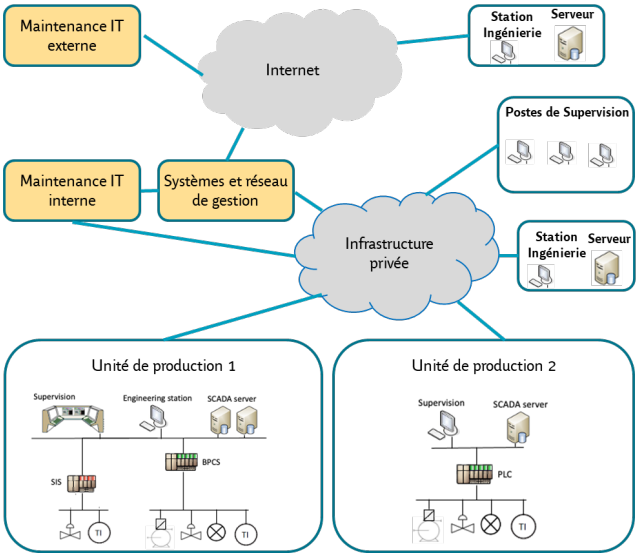

Fig 17. Système industriel

Pour les biens supports, aux composants standard des systèmes IT (postes de travail, serveurs, routeurs …) s'ajoutent des éléments spécifiques :

- Station(s) de supervision
- Station(s) d'ingénierie
- Serveur d'historique
- Serveur de données de pilotage (configuration, programme automates …)
- Automates (PLC), systèmes embarques de contrôle
- Automates des sécurité (SIS)

Les deux derniers types sont des systèmes particuliers utilisant des protocoles de communication spécifiques (dits protocoles industriels) qui présentent des vulnérabilités et induisent une surface d'attaque directe sur le système physique piloté.

1) Elaborer les Scénarios opérationnels

Pour déterminer les scénarios opérationnels nous procédons à un raffinement supplémentaire en appliquant, non plus une grammaire abstraite, mais la base du MITRE : ATT@CK-ICS (Fig. 18).

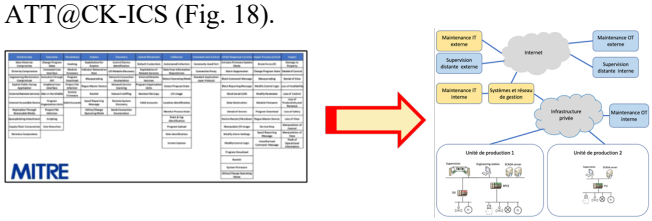

Fig. 18 Application d'ATT@CK-ICS

Nous obtenons une série de scénarios raffinant **S1.1**, en traduisant chacune de ses étapes en une ou plusieurs tactiques ATT@CK combinées, puis en déclinant chaque tactique en techniques, à condition que la séquence obtenue soit bien cohérente du point de vue logique.

Comme ATT@CK est une typologie de cyberattaques, certaines étapes du scénario stratégique étudié ne seront pas traduites mais on vérifie que les post-conditions de ces étapes singulières couvrent les préconditions des techniques ATT@CK sélectionnées pour l'étape suivante.

Voici le détail de l'un des scénarios ainsi traduits :

Scénario S1.1.3 :

0. Recrutement d'un Administrateur

1. TA108 (Initial Access) ▸ T0866 (Exploitation of Remote Services)

2. TA0104 (Execution) ▸ T0807 (Command-Line Interface) ; TA011 (Collection) ▸ T0868 (Detect Operating Mode)

3. TA0104 (Execution) ▸ T0807(Command-Line Interface) ; TA0104 (Execution) ▸ T0858 (Change Operating Mode)

4. TA0107 (Inhibit Response Function) ▸ T0800 (Activate Firmware Update Mode)

5. T0879 (Damage to Property)

Fig. 19 Exemple de scénario opérationnel

La technique permet, en basculant le SIS dans le mode d'activation du *firmware*, de bloquer sa fonction de contrôle.
Par ailleurs, on peut modéliser plusieurs autres scénarios en produisant des variantes, par exemple pour l'étape (3) :

(3.1) … ; TA0106 (Impair Process Control) ▸ T0836 (Modify Parameter)

(3.2) … ; TA0106 (Impair Process Control) ▸ T0855 (Unauthorized Command Message)

Fig 20. Variantes du scénario opérationnel

2) Vraisemblance des scénarios opérationnels

Cette étape vise à évaluer les scénarios opérationnels sachant que EBIOS-RM incite l'analyste à écarter les scénarios stratégiques jugés peu pertinents durant l'atelier 3 sans définir précisément la notion de pertinence ; aucun scénario opérationnel n'est alors associé à ces scénarios stratégiques.

Nous pensons, qu'un scénario ne doit pas être écarté sans un argument rigoureux, nous allons donc évaluer TOUS les scénarios générés jusqu'alors, sans nous limiter aux seuls scénarios opérationnels produits dans l'étape précédente.

Nous avons donc deux situations distinctes :

(1) Pour les scénarios d'attaque complètement couverts par les modes de défense proposés (e.g. **S2**, **S1.3**), il s'agit d'évaluer l'efficacité réelle des implémentations de ces modes de défense dans le système industriel concret ; En effet, les modes de défense (e.g. **D2**) sont autant d'exigences supplémentaires qui complètent les spécifications du système et rentrent dans son processus de développement.

(2) Pour les scénarios opérationnels il faut comparer les techniques ATT@CK avec le profil capacitaire de l'Attaquant retenu.

Dans notre exemple (**S1.1.3**), les phases 2 à 5 reposent sur l'abus de pouvoir d'un administrateur, leur vraisemblance ne dépend donc pas des caractéristiques spécifiques des composants techniques.

Compte-tenu de l'analyse faite au §IV.D.3, il sera dès lors nécessaire de développer le mode de défense **D1.1** en renforçant le contrôle des actions d'administration.

F. Atelier 5 : système de cyberdéfense

Dans cette partie, nous nous limitons à l'étape 3 de l'atelier 5, dédié à la mise en œuvre des mesures de sécurité.

1) Développement des modes de défense de haut niveau

Comme nous l'avons vu, plusieurs éléments de défense ont été spécifiés dans les étapes précédentes ; il faut alors analyser la rigueur et la profondeur de leurs implémentations.

Par exemple, dans le cas du mode de défense **D2**, il s'agit de garantir que les flux transitant entre le domaine de maintenance interne et les unités de production sont convenablement protégés par un VPN utilisant des algorithmes de chiffrement robustes, avec des clés de taille suffisante, et supporté par des passerelles de communication certifiées ou agréées.

2) Sélection des mesures de défense opérationnelles

Il reste alors à déterminer les mesures de défense complémentaires pour couvrir les scénarios raffinés jusqu'au niveau opérationnel.

Nous déterminons les mesures concrètes en appliquant les bases de défense du MITRE (e.g. D3FEND) sur les scénarios opérationnels (Fig. 21).
Le MITRE, qui propose aujourd'hui plusieurs bases ([9, 10, 12]) a lancé des travaux de mise en cohérence dans un même référentiel de défense.

Fig. 21 Application de D3FEND

Le MITRE a défini explicitement les applications des techniques des bases de défense sur les techniques des bases d'attaque ; par conséquent la sélection des techniques de défense applicable est immédiate.

Dans le cas de notre exemple, on obtient le résultat suivant

0. Cf. mesures de Contre-ingérence

1. Pas de mesure spécifique à cette phase

2. Pas de mesure spécifique à cette phase

3. M0800 - Authorization Enforcement pour limiter les possibilités des administarteurs distants dans certaines conditions
   CM2144 - Monitor Platform Status pour contrôler le contexte d'utilisation

4. M0800 - Authorization Enforcement pour limiter les possibilités des administarteurs distants dans certaines conditions
   CM2144 - Monitor Platform Status pour contrôler le contexte d'utilisation
   D3-NTF Network Traffic Filtering pour isoler l'unité de production du domaine d'administration distante en cas de suspicion

5. M0805 - Mechanical Protection Layers pour placer le système dans état sûr en cas d'incident

Fig. 22 Application des bases de défense du MITRE

Les différentes bases de défense proposent quelques mesures pour le scénario **S1.1.3** qui devront s'appuyer sur une définition très rigoureuse des différentes situations de maintenance en spécifiant, pour chacune d'elles, les opérations licites et les modalités d'exécution autorisées.

V. Conclusion et perspectives

La méthode EBIOS est une méthode très riche qui peut être complexe à mettre en œuvre, tout particulièrement dans le cas des systèmes industriels ou la Sûreté de Fonctionnement doit aussi être prise ne compte.

Dans cet article, nous avons montré qu'un certain nombre de *stéréotypes* peuvent être identifiés pour ces systèmes industriels, et qu'il est possible d'en dégager les éléments d'un (futur) guide générique pour la mise en oeuvre de EBIOS sur les ICS.

L'approche proposée vise à atteindre un niveau de rigeur compatible à celui de la Sûreté de Fonctionnement pour la modélisation des cyber-attaques conduisant à des événements redoutés, puis la sélection des mesures de défense.
Pour ce faire, elle s'appuie sur des bases de connaissance et une grammaire précise qui permet de construire graduellement les scénarios d'attaques dans les ICS puis de leur opposer des scénarios de défense adaptés.

De ce fait, nous pensons qu'une telle méthode permet de pallier à de nombreuses limitations inhérentes à EBIOS RM, en particulier l'absence de bases pour construire les scénarios opérationnels ou encore l'introduction très (trop ?) tardive des éléments de défense.
L'idée de notre approche est de systématiser au maximum, par le truchement des grammaire d'attaque et défense inspirées des principes de la lingustique fonctionnelle systémique ([21]), la construction des scénarios afin de les rendre autant que possible reproductible par des experts différents.

Ceci étant dit, il ne faut pas sous-estimer la difficulté intrinsèque de l'anticipation des manœuvres d'un attaquant que l'on ne pourra jamais totalement prévoir. Sur ce point particulier, nous commençons à réfléchir à inclure dans cette méthode les idées développées dans [22].

Sur un plan concret, la démarche que nous avons élaborée doit être mise en œuvre dans le cadre d'un processus structuré de maîtrise des risques et une première version de cette méthode a été employée par la RATP sur un métro automatique (ce travail a été présenté dans [23]) ; nous pensons qu'elle peut être généralisée à de nombreux types de systèmes industriels dès lors que leurs spécificités respectives peuvent être correctement représentées dans les modèles sur lesquels nous nous appuyons.

D'autre part cette méthode nécessite bien évidemment le support d'outil pour être déployée sur de grands systèmes industriels. Malheureusement les outils EBIOS RM actuellement labellisés par l'ANSSI ne permettent pas de l'appliquer parce qu'ils ne peuvent pas manipuler les graphes qui reproduisent les cartes successives du système et fondent nos différentes analyses.

Une des suites possibles du travail que nous présentons dans cette communication cosisterait alors à spécifier un outil adapté, en s'incrivant dans une approche de type *model-based* pour maîtriser la suite de modèles anstraits et leurs raffinements tout en s'appuyant au maximum sur les nombreux modules open sources développés autour des bases de connaissance du MITRE.

References

[1] L. Pièrre-Cambacédès, "Des relations entre sûreté et sécurité," PhD Thesis, Télécom ParisTech, 2010.

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

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

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

[5] https://fr.wikipedia.org/wiki/IEC_62443

[6] https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final

[7]https://www.ssi.gouv.fr/guide/la-cybersecurite-des-systemes-industriels/

[8]https://collaborate.mitre.org/attackics/index.php/Main_Page

[9] https://engage.mitre.org/

[10] https://d3fend.mitre.org/

[11] J. Caire , HADES : Hologrammes d'Attaque et Défense pour Evaluer la Sécurité , non publié

[12] https://csrc.nist.gov/publications/detail/sp/800-160/vol-2-rev-1/final

[13] US Air Force, "Cyber Vision 2025", 2013

[14] J. Caire et S. Conchon, "Le Continuum de Sécurité", Congrès Lambda-Mu 22, 2020

[15] M. Vego "Joint Operational Warfare", 2009

[16] J.-M. Flaus, Cybersécurité des systèmes industriels,

ISTE-, 2019

[17] K. Jabbour, The Science of Mission Assurance, 2012

[18] Afnor - CN Cybersécurité, Normes volontaires et approches innovantes pour la Cybersécurité, 2019

[19] A. Villemeur, Sûreté de fonctionnement des systèmes industriels, Eyrolles, 1988

[20] E. Morin, Introduction à la pensée complexe, Le Seuol, 2014

[21] A. Sliva et al., Hybrid Modeling of Cyber Adversary Behavior in Social, Cultural and Behavioral Modeling, Springer, 2017.

[22] J. Caire et S. Conchon, Sécurité : comment gérer les surprises ?, Congrès Lambda-Mu 20, 2016

[23] : J. Peres et al., Maîtrise des risques liés aux aspects de cybersécurité et de sécurité ferroviaire, Congrès Lambda-Mu 21, 2018