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

Evaluation du niveau de sécurité d'un système OT et architecture sécurisée

OT System security level assessment and secured architecture

LARDJAM Abdellah
SERMA Safety & Security
Bordeaux
a.lardjam @serma.com

DUFRESNE Michel
SERMA Safety & Security
Paris
m.dufresne @serma.com

DEOLA Adrien
SERMA Safety & Security
Toulouse
a.deola@serma.com

I. LES RESUMES

FR : Les entreprises qui intègrent actuellement des technologies opérationnelles sont conscientes des opportunités qu'elles offrent aux exploitants d'installations industrielles. Ces opportunités permettent d'augmenter la productivité, réduire les coûts et d'assurer le partage en temps réel d'informations entre divers systèmes industriels et d'entreprise.

Malgré ces opportunités, il existe une préoccupation croissante concernant les cyberattaques. Les infrastructures industrielles sont devenues des cibles pour des cybercriminels déterminés et des entités hostiles étrangères. Ces acteurs malveillants constituent une menace réelle pour les processus industriels, les systèmes qui les supervisent et les systèmes de Sûreté (Safety)

Les opérateurs et les ingénieurs se retrouvent donc pris entre la nécessité d'isoler les systèmes industriels et les demandes des gestionnaires qui souhaitent une interconnexion avec les systèmes informatiques et internet.

Face à ce dilemme, comment les entreprises peuvent-elles évaluer le niveau de sécurité de leurs systèmes de contrôle industriel tout en assurant une certaine isolation entre les technologies de l'information (IT) et les technologies opérationnelles (OT), en tenant compte à la fois des menaces numériques et physiques?

L'objectif de cet article est de proposer une approche visant à évaluer les niveaux de sécurité des systèmes industriels et à concevoir une architecture intrinsèquement sécurisée. Cette méthodologie permet d'intégrer des considérations de sécurité dès les premières étapes de conception, assurant ainsi une protection robuste et proactive des infrastructures industrielles

EN: Companies that are currently integrating operational technologies are aware of the opportunities they offer to industrial plant operators. These opportunities include increasing productivity, reducing costs, and ensuring real-time information sharing between different industrial and business systems.

Despite these opportunities, there is growing concern about cyber-attacks. Industrial infrastructure has become a target for determined cyber criminals and hostile foreign entities. These malicious actors pose a real threat to industrial processes, the systems that monitor them and security systems.

Operators and engineers are therefore caught between the need to isolate industrial systems and the demands of managers to connect them to IT systems and the Internet.

Faced with this dilemma, how can companies assess the level of security of their industrial control systems while ensuring a degree of isolation between information technologies (IT) and operational technologies (OT), considering both digital and physical threats?

The aim of this article is to propose an approach aimed at assessing the security level of industrial systems and designing an intrinsically secure architecture. This methodology makes it possible to integrate security considerations from the earliest design stages, thereby ensuring robust and proactive protection of industrial infrastructures.

II. MOTS CLEFS

Convergence IT/OT, EBIOS RM, IEC62443, ''Défense en profondeur, Safety, Niveau de sécurité (Security Level : SL)

III. INTRODUCTION

Les systèmes de contrôle industriels (ICS) modernes remplissent des fonctions vitales dans les systèmes critiques, telles que la distribution d'énergie électrique, la distribution de pétrole et de gaz naturel. Ils sont également au cœur des dispositifs médicaux, des systèmes d'alarmes et de la gestion des transports.

Ces systèmes de contrôle sont de plus en plus interconnectés, intégrant des technologies de l'information (IT) et des technologies opérationnelles (OT). Cette convergence expose les infrastructures critiques à des risques accrus de cyberattaques, qui peuvent non seulement perturber la production, mais aussi compromettre la sécurité des travailleurs, des installations et de l'environnement.

De ce fait, l'évaluation de la cybersécurité d'un système industriel est d'une importance capitale dans le contexte actuel où les menaces numériques sont en constante évolution.

Pour les nouveaux systèmes, intégrer l'évaluations de cybersécurité dès les premières étapes de la conception permet de construire des systèmes robustes et résilients. Cette approche proactive, connue sous le nom de "Security by Design", vise à identifier et à atténuer les vulnérabilités potentielles avant même que le système ne soit déployé. Pour les installations existantes, cette évaluation est souvent confrontée à des défis qu'il faut relever tels que l'hétérogénéité des infrastructures, l'obsolescence des équipements et la convergence IT/OT qui augmentent la surface d'attaque.

Dans les deux cas, l'évaluation de la cybersécurité des installations industrielles va permettre de mettre en place des mesures de protection adéquates, cela va compléter les autres expertises (Safety, IT) en fournissant une couche de protection essentielle contre les menaces numériques et va permettre aux entreprises de réduire significativement les risques de compromission et assurer une continuité opérationnelle optimale.

IV. ETAT DE L'ART

Aujourd'hui, les entreprises industrielles se tournent souvent vers des solutions de cybersécurité prêtes à l'emploi, négligeant parfois l'importance de l'évaluation basée sur l'analyse des risques de leurs installations existantes. L'état de l'art en matière de cybersécurité OT souligne l'importance de cette évaluation pour identifier les vulnérabilités spécifiques aux environnements industriels. Les normes telles que l'IEC 62443 offrent des directives pour définir les exigences de sécurité et implémenter des mesures de protection adaptées. Une approche rigoureuse inclut la segmentation du réseau en zones de sécurité et conduits pour limiter les impacts en cas de cyberattaque, ainsi que l'utilisation de systèmes de surveillance continue.

V. CONVERGENCE IT/OT

A. IT et OT : COMPRENDRE CES DEUX SYSTEMES

La Technologie de l'Information (IT : Information Technology) : La technologie de l'information (IT) englobe l'ensemble des composantes liées aux ordinateurs, allant du matériel aux logiciels, en passant par la gestion des réseaux, le stockage des données et la sécurité informatique. Elle constitue un pilier essentiel pour le traitement de l'information, la communication efficace et l'automatisation des processus au sein des organisations. [6]

La Technologie Opérationnelle (OT : Operation Technology) : La technologie opérationnelle (OT) englobe les équipements matériels et logiciels utilisés pour surveiller et contrôler les processus physiques dans les environnements industriels. Contrairement à l'informatique (IT) qui gère les données et les systèmes informatiques, l'OT se concentre sur la gestion des équipements tels que les machines de production, les capteurs et les systèmes de contrôle automatisés. [6]

La différence entre ces deux technologies : L'informatique (IT) se concentre sur la gestion de l'information numérique, tandis que la technologie opérationnelle (OT) prend en charge le fonctionnement des équipements physiques et des processus industriels. Étant donné que l'informatique (IT) est principalement axée sur le stockage, la récupération, la manipulation et la transmission des informations numériques, **la confidentialité** des données devient une préoccupation essentielle. Ainsi, la sécurité informatique est cruciale dans toute organisation pour garantir la sécurité et le contrôle des données.

Fig. 1. Critères de sécurité entre IT et OT.

Dans le domaine de l'OT, **la protection** et **la disponibilité** des équipements et des processus industriels prédominent. Il s'agit de traiter les systèmes physiques, tels que les machines de production et les capteurs, qui doivent maintenir des paramètres stables, tels que la température, la pression ou la vitesse de rotation. Cette exigence de stabilité implique un contrôle méticuleux pour assurer le bon fonctionnement des processus industriels.

B. CONVERGENCE IT/OT

La convergence des systèmes d'information (IT) et des systèmes industriels (OT) représente un virage crucial dans le paysage technologique des entreprises, en particulier dans le secteur industriel. Jusqu'à récemment, ces deux domaines étaient étanches, tant sur le plan technique qu'organisationnel. Cependant, la transformation numérique des entreprises a imposé un changement de paradigme, nécessitant une convergence entre IT et OT.

Fig. 2. Convergence IT / OT.

Plusieurs facteurs ont contribué à ce besoin croissant de rapprochement entre IT et OT. Parmi eux, la nécessité de décloisonner les données pour en optimiser l'utilisation occupe une place centrale. Cependant, ce décloisonnement et la convergence des systèmes engendrent des défis accrus en matière de cybersécurité, une préoccupation majeure pour les dirigeants.

La convergence technologique permet désormais aux systèmes de couvrir de manière transparente les deux mondes, facilitant l'intégration des technologies OT dans l'IT et vice versa. Ainsi, les technologies OT intègrent de plus en plus d'éléments d'IT, tels que les serveurs OPC, le cloud computing et machine learning, tandis que les technologies IT s'étendent vers l'OT, avec des avancées telles que la virtualisation des automates et une accessibilité accrue des technologies par le biais des fournisseurs IT.

C. COMPOSANT D'UN SYSTEME OT

Un système OT est généralement composé d'éléments numériques et physiques qui interagissent à travers un réseau de communication, pour permettre la collaboration des éléments informatiques pour contrôler et commander les entités physiques. Très souvent, les éléments de l'OT sont exploités par des logiciels spécifiques, comme les logiciels SCADA. [1]

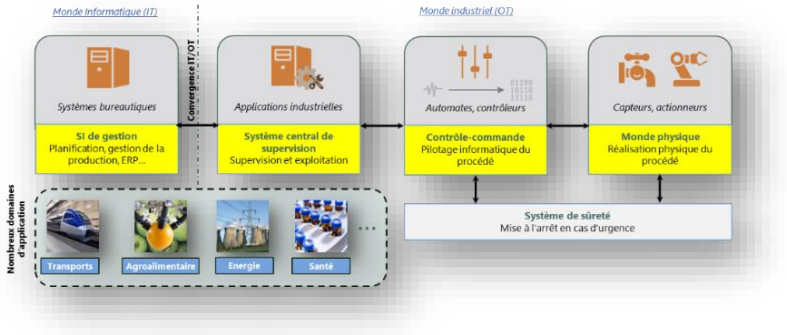

Fig. 3. Composants d'un système OT.

Un système opérationnel (OT) est composé de plusieurs éléments essentiels qui interagissent pour surveiller, contrôler et automatiser les processus physiques dans un environnement industriel. Voici les composants principaux d'un système OT :

a) Capteurs et actionneurs : Ce sont des dispositifs physiques qui captent les données à partir de l'environnement (température, pression, niveau, etc.) ou qui agissent sur celui-ci en fonction des instructions reçues du système de contrôle.

b) Système de contrôle : Il s'agit du cœur du système OT, comprenant des automates programmables (PLC), des unités de contrôle distribué (DCS) ou des systèmes de contrôle commande. Ce système reçoit les données des capteurs, les traite et envoie des instructions aux actionneurs pour réguler les processus industriels.

c) Réseaux de communication : Les réseaux industriels permettent la transmission des données entre les différents composants du système OT, notamment les capteurs, les actionneurs et le système de contrôle. Ces réseaux doivent être robustes, sécurisés et adaptés aux contraintes industrielles.

d) Supervision et gestion : Les interfaces homme-machine (IHM) et les logiciels de supervision permettent aux opérateurs de surveiller et de contrôler les processus industriels en temps réel. Ils offrent également des fonctionnalités de diagnostic, d'analyse et de gestion des alarmes.

e) Stockage de données : Les systèmes OT incluent souvent des bases de données ou des systèmes de stockage pour enregistrer les données historiques des processus industriels. Ces données sont utilisées pour l'analyse rétrospective, la génération de rapports et l'optimisation des performances.

Ensemble, ces composants forment un écosystème complexe qui garantit le bon fonctionnement des processus industriels tout en assurant la fiabilité et l'efficacité des opérations.

D. CYBERSECURITE INDUSTRIELLE : DES STANDARDS ET DES BONNES PRATIQUES

1) Défense en profondeur

Une notion importante dans la protection des installations industrielles contre les attaques est basée sur le fait qu'elle requiert la participation de tous les acteurs : l'exploitant, l'intégrateur et le fournisseur. En général une seule mesure ne sera pas suffisante pour atteindre un certain niveau de protection. Il est nécessaire de mettre en œuvre plusieurs mesures coordonnées qui représenteront autant de barrières, de lignes de défense contre l'attaquant. Cette stratégie, appelée défense en profondeur (Defense in Depth) a été appliquée dans le domaine militaire depuis très longtemps. De ce fait, la défense en profondeur (DEP) est un concept dans lequel une série de mécanismes défensifs sont superposés afin de protéger des données et des informations précieuses. Si un mécanisme échoue, un autre intervient immédiatement pour déjouer une attaque. [1], [3]

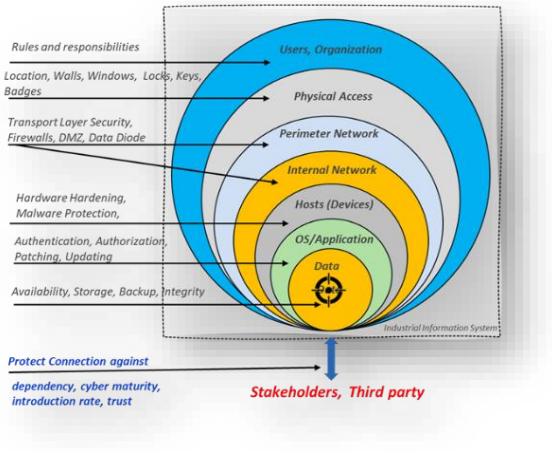

Fig. 4. Défense en profondeur.

Cette approche multicouche augmente la sécurité d'un système dans son ensemble et s'attaque à de nombreux vecteurs d'attaque différents.

Les différentes couches du modèle de défense en profondeur sont succinctement décrites ci-après :

a) Couche Organisationnelle : Cette couche implique la mise en place d'un système de gestion de la sécurité et l'établissement de politiques de sécurité claires et de procédures opérationnelles standard (SOP) pour guider les pratiques de sécurité dans toute l'organisation. Cela comprend la sensibilisation à la sécurité, la formation des employés, les processus de gestion des incidents et la gouvernance de la sécurité.

b) Couche des Accès Physiques : Cela inclut les mesures de sécurité telles que les clôtures, les caméras de surveillance, les contrôles d'accès physique aux installations, etc.

c) Couche des réseaux (Internes et externes) : Cette couche comprend les pares-feux, les passerelles VPN, les routeurs, les commutateurs, les systèmes de prévention des intrusions (IPS) et les politiques de liste de contrôle d'accès (ACL) configurés pour filtrer et contrôler le trafic entrant et sortant.

d) Couche des dispositifs (Hosts) : Cette couche se concentre sur la sécurisation des équipements individuels, des appareils et des systèmes qui composent l'infrastructure OT comprenant notamment le durcissement, la suppression des applications/protocoles/services inutilisés, la fermeture des ports logiques inutiles et la protection des ports physiques.

e) Couche des Applications : Cela concerne la sécurisation des applications spécifiques utilisées dans les systèmes OT, comme les logiciels de contrôle industriel (Exemple : Application SCADA) et les interfaces homme-machine (IHM), pour prévenir les vulnérabilités et les failles de sécurité.

f) Couche des données : La sécurité au niveau de cette couche vise à protéger les données du système OT en incluant, par exemple, la cryptographie, la sauvegarde pour garantir l'intégrité et la disponibilité des données.

La norme **IEC 62443** adresse tous les aspects d'une stratégie de défense en profondeur.

2) Description générale de la norme IEC 62443

a) Champ d'application de la norme IEC 62443

La norme IEC 62443 est le référentiel spécifique à la sécurité des systèmes OT notamment les ICS (Industrial Control Systems), elle définit le cadre de cyberdéfense des systèmes industriels, pour tous types de centres de production (station d'épuration, fabrication électronique, usine pharmaceutique, automobile fonderie, raffinerie, etc.).

Les systèmes de contrôle industriel (ICS) englobent une gamme variée de technologies et d'infrastructures essentielles au bon fonctionnement des industries. Ils comprennent notamment les : [1]

- *Systèmes de Supervision et Acquisition de Données (SCADA) :* Ces systèmes permettent la surveillance et le contrôle à distance des processus industriels en collectant des données sur le terrain.
- *Systèmes de Contrôle Distribués (DCS) :* Les DCS sont des systèmes informatiques utilisés dans les processus industriels pour surveiller et contrôler les équipements distribués dans une usine ou une installation.
- *Automates Programmables Industriels (PLC, RTU) :* Sont des dispositifs électroniques programmables utilisés pour automatiser les processus de production et de contrôle dans les usines et les installations industrielles. Ils exécutent des séquences d'instructions pour contrôler les machines et les équipements.
- *Systèmes de Gestion des Bâtiments (BMS)* : Ces systèmes sont utilisés pour surveiller, contrôler et optimiser les équipements et les services dans les bâtiments commerciaux et industriels, tels que le chauffage, la ventilation, la climatisation, l'éclairage, etc.
- *Systèmes de Sécurité Instrumentée (SIS) :* Ces systèmes sont conçus pour détecter et réagir aux situations dangereuses dans les installations industrielles en mettant en œuvre des mesures de sécurité telles que l'arrêt d'urgence des équipements.

b) Structure de la norme

La norme IEC 62443 se répartit en quatre parties, chacune d'entre elles regroupant plusieurs documents :

- *Partie 1 :* Regroupe les documents destinés aux concepts généraux, à la terminologie et aux méthodes.
- *Partie 2 :* Spécifie uniquement des mesures organisationnelles.
- *Partie 3 :* A un contenu beaucoup plus technique, elle décrit la méthode et les moyens pour structurer l'architecture de la solution en zones et canaux de communication (conduits).
- *Partie 4 :* Est spécifiquement destinée aux équipements faisant partie de systèmes de contrôle industriels.

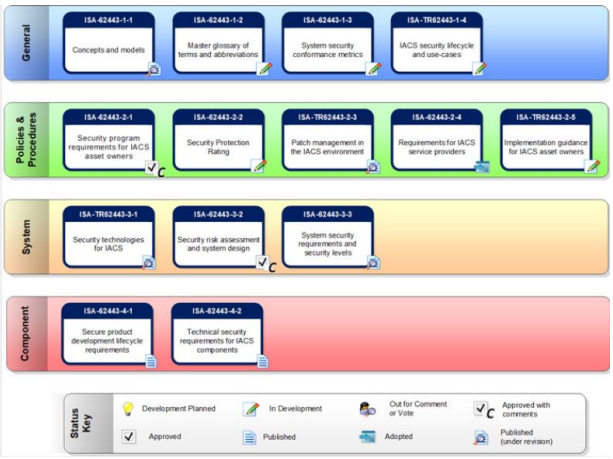

Fig. 5. Les séries de la norme IEC 62443.

La série de normes IEC 62443-3-3 est cruciale pour la mise en place des contrôles de sécurité dans un système de contrôle industriel. Elle établit sept (07) exigences fondamentales (Foundational Requirements : FR) en matière d'intégrité des données, de disponibilité des ressources, de temps de réaction à un événement ou encore de contrôle de l'accès et de l'utilisation. [10]

TABLE I. EXIGENCES FONDAMENTALES

Foundational Requirement	Associated Process
FR1 – Identification, Authentication, and Access control	User authentication and authorisation
FR2 – Use Control	Enforcement of roles and responsibilities
FR3 – System Integrity	Prevent unauthorized manipulation.
FR4 – Data Confidentiality	Use of encryption
FR5 – Restrict Data Flow	Network segmentation
FR6 – Timely Response to Event	Audit logs
FR7 – Resource Availability	System backup and recovery

Comme le montre l'exemple du tableau ci-dessous, pour chacune des exigences fondamentales, il existe un certain nombre d'exigences de sécurité technique (SR) et d'améliorations (RE) spécifiques, qui sont classées en quatre (04) niveaux de sécurité (SL) en fonction de la criticité de la menace.

FR 1 – Identification and Authentication Control (IAC)					
SR 1.1 – Human user identification and authentication		SL1	SL2	SL3	SL4
	RE (1) Unique identification and authentication		SL2	SL3	SL4
	RE (2) Multifactor authentication for untrusted network			SL3	SL4
	RE (3) Multifactor authentication for all network				SL4
SR 1.2 – Software process and device identification and authentication			SL2	SL3	SL4
	RE (1) Unique identification and authentication			SL3	SL4
SR 1.3 – Account management		SL1	SL2	SL3	SL4
	RE (1) Unified account management			SL3	SL4
SR 1.4 – Identifier management		SL1	SL2	SL3	SL4

Fig. 6. Exemple des exigences de sécurité système.

Le niveau de sécurité (SL), est une mesure de la robustesse et de la résilience d'un système OT face aux cybermenaces.

Les SL sont utilisés pour évaluer les besoins en matière de cybersécurité d'un système OT et pour concevoir des contre-mesures appropriées. Les différents niveaux de sécurité correspondent aux différentes catégories de cyberattaques.

La norme IEC 62443 définit quatre niveaux de sécurité principaux, numérotés de SL1 à SL4, avec SL1 étant le niveau le plus bas de sécurité et SL4 le plus élevé. Chaque niveau de sécurité correspond à un ensemble spécifique de mesures de sécurité.

- **SL1 :** Ce niveau correspond généralement aux systèmes OT les moins critiques, où la cybersécurité n'est pas une préoccupation majeure. Les mesures de sécurité à ce niveau sont limitées.
- **SL2 :** Les systèmes OT de niveau SL2 sont plus critiques, mais les conséquences de failles de sécurité sont gérables. Des mesures de sécurité supplémentaires sont mises en place pour protéger ces systèmes.
- **SL3 :** Les systèmes OT de niveau SL3 sont considérés comme critiques, et des mesures de sécurité robustes sont nécessaires pour les protéger. Les conséquences d'une faille de sécurité sont significatives.
- **SL4 :** Les systèmes OT de niveau SL4 sont les plus critiques, souvent utilisés dans des environnements hautement sensibles, comme les centrales nucléaires, les installations Oil & Gas, ou les infrastructures de transport essentielles. Les mesures de sécurité à ce niveau sont extrêmement rigoureuses.

Les SL ont été réparties en trois types différents : (Voir Annexe A de la série IEC 62443-3-3 pour davantage de détails) :

- **Target (SL-T):** représente le niveau de sécurité cible que l'on souhaite atteindre ;
- **Achieved (SL-A) :** représente le niveau de sécurité réellement atteint par rapport au niveau cible ;
- **Capability (SL-C) :** représente le niveau de sécurité actuel du système OT.

VI. METHODOLOGIE

A. EVALUATION ET SECURISATION D'UN SYSTEME OT

La cybersécurité étant un domaine en constante évolution, il est essentiel de planifier la mise en œuvre des mesures de sécurité en identifiant les besoins de l'entreprise, les risques, les mesures de sécurité appropriées et les protocoles de suivi.

Pour ce faire, SERMA Safety and Security a développé une méthodologie pragmatique prenant en compte les besoins en matière de sécurité d'information industrielle. Cette méthodologie permet d'évaluer et de sécuriser un système OT en s'appuyant sur :

- L'analyse de risque en utilisant la méthode EBIOS Risk Manager ;
- La norme IEC 62443 et spécifiquement IEC 62443-3-2 et IEC 62443-3-3 et éventuellement la IEC 62443-2 pour la mise en plan d'un plan de cybersécurité organisationnel (CSMS) ;
- D'autres référentiels et normes internationales à savoir NIST et la famille ISO 27000 ;
- Les bonnes pratiques de la sécurité industrielle recommandées par l'ANSSI ;
- L'approche de la défense en profondeur ;

Comme le montre la figure, cette méthodologie qui se nomme ''CERMA'' (Cybersecurity Evaluation and Risk MAnagement) passe par les étapes suivantes :

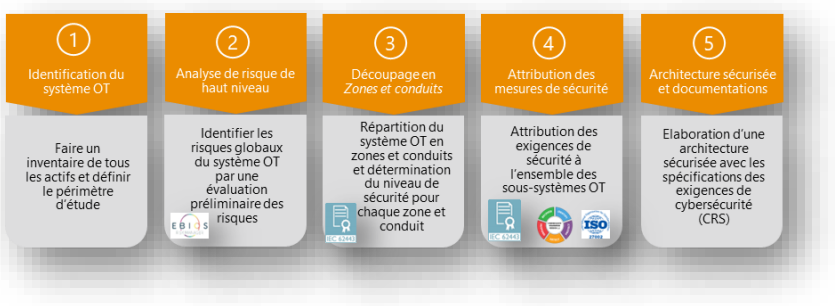

Fig. 7. Méthodologie d'évaluation et de sécurisation d'un système OT.

ETAPE 1 : Identification du Système OT : L'identification des actifs, qui représentent généralement les éléments de valeur au sein d'un système OT, est une étape cruciale pour la gestion de la sécurité et la protection des données. Cette étape se déroule comme suit : réaliser un inventaire physique et logique, créer des diagrammes d'architecture, identifier les données et les processus clés qui sont gérés par le système OT, consulter les documents techniques et les documents de conception, réaliser des entretiens avec les parties prenantes, analyser les flux de données qui circulent à travers le système OT, identifier les accès aux différents composants du système et les autorisations accordées, cartographier le réseau OT pour identifier les périphériques connectés et leur relation les uns avec les autres et classifier les actifs selon leur criticité afin de hiérarchiser les mesures de sécurité.

ETAPE 2 : Analyse de risque de haut niveau : Comme le prévoit la norme IEC 62443-3-2, l'objectif de l'analyse de risque de haut niveau (High Level Risk Assessment) est d'acquérir une première compréhension du risque le plus défavorable pour une entreprise en cas de compromission de son système OT. Ce risque est généralement évalué en termes d'impact sur la santé, la sécurité, l'environnement, l'interruption des activités, la perte de production, la qualité des produits, les aspects financiers, juridiques et réglementaires, la réputation, etc.

Cette évaluation permet de hiérarchiser les évaluations détaillées des risques et facilite le regroupement des actifs en zones et en conduits au sein du système OT.

Pour cette étape, nous utilisons la méthode **EBIOS Risk Manager** (EBIOS : Expression des Besoins et Identification des Objectifs de Sécurité).

Cette méthode recommandée par l'ANSSI, permet d'apprécier les risques numériques et d'identifier les mesures de sécurité à mettre en œuvre pour les maîtriser.

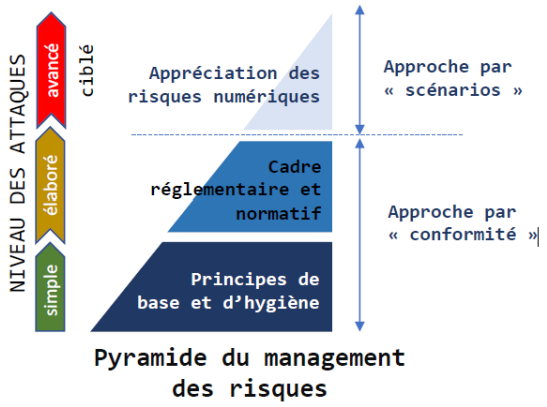

Fig. 8. Pyramide du management des risques.

Comme le montre la figure, cette méthode est symbolisée par la pyramide du management du risque numérique, elle vise à obtenir une synthèse entre « conformité » et « scénarios », en positionnant ces deux approches complémentaires là où elles apportent la plus forte valeur ajoutée.

Cette méthode se base sur la norme ISO 27005 portant sur la gestion des risques de sécurité de l'information et se déroule en cinq (05) ateliers qui font référence à des sessions de travail collaboratives organisées pour mener à bien l'analyse des risques :

a) ***Atelier 1*** *:* *Cadrage et socle de sécurité :* Ce premier atelier vise à identifier l'objet de l'étude, les participants aux ateliers et le cadre temporel. Au cours de cet atelier, nous recensons les missions, valeurs métier (biens essentiels) et biens supports relatifs à l'objet étudié. Nous identifions les événements redoutés associés aux valeurs métier et évaluons la gravité de leurs impacts. Nous définissons également le socle de sécurité et les écarts.

b) ***Atelier 2*** *:* *Sources de risque :* Dans le deuxième atelier, nous identifions et caractérisons les sources de risque (SR) et leurs objectifs de haut niveau, appelés objectifs visés (OV). Les couples SR/OV jugés les plus pertinents sont retenus.

c) ***Atelier 3*** *:* *Scénarios stratégiques* *:* Dans l'atelier 3, nous allons acquérir une vision claire de l'écosystème et établir une cartographie de menaces numériques de celui-ci vis-à-vis de l'objet étudié. Ceci va nous permettre de bâtir des scénarios de haut niveau, appelés scénarios stratégiques. Ils représentent les chemins d'attaque qu'une source de risque est susceptible d'emprunter pour atteindre son objectif. Ces scénarios se conçoivent à l'échelle de l'écosystème et des valeurs métier de l'objet étudié. Ils sont évalués en termes de gravité.

d) ***Atelier 4*** *:* *Scénarios opérationnels* *:* Cet atelier fonctionne un peu comme le précédent, si ce n'est qu'il cherche à proposer une solution opérationnelle pour répondre aux différents risques en fonction du chemin d'attaque qui a été constaté.

e) ***Atelier 5*** *:* *Traitement du risque* *:* Le dernier atelier consiste à réaliser une synthèse de l'ensemble des risques étudiés en vue de définir une stratégie de traitement du risque. Cette dernière est ensuite déclinée en mesures de sécurité inscrites dans un plan d'amélioration continue. Lors de cet atelier, nous établissons la synthèse des risques résiduels et définissons le cadre de suivi des risques.

Cette analyse de risque préliminaire va permettre de hiérarchiser les impacts dans le système OT et par conséquent, de répartir le système en zones et conduits.

ETAPE 3 : Découpage en zones et conduit et attribution du niveau de sécurité (SL): À la suite de l'analyse de risque de haut niveau (High Level Risk Assessment), nous procédons à la décomposition du système OT en zones et conduits tel que décrit dans la norme IEC 62443-3-2 pour segmenter et isoler les différents sous-systèmes d'un système OT.

Une zone : est définie comme un regroupement de biens logiques ou physiques qui partagent des exigences de sécurité communes basées sur des facteurs tels que la criticité et les conséquences.

Un conduit : représente toute donnée passant d'une zone à une autre, quel que soit le moyen utilisé pour le transfert des données (communication réseau, dispositif amovible, etc.). [9]

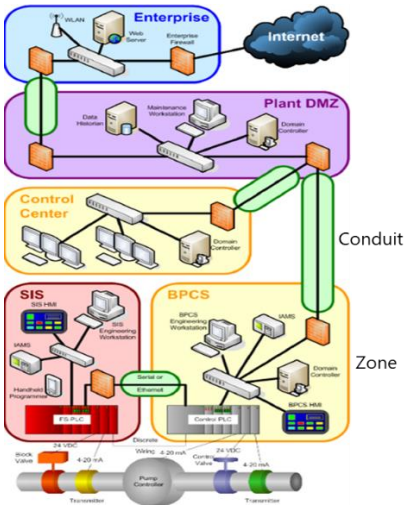

Fig. 9. Répartition d'un système OT en zones et conduits. [9]

Pour partitionner le système OT en zones et en conduits les critères suivants doivent être pris en compte : Risque pour les actifs en termes d'intégrité, de disponibilité et de confidentialité, type d'interfaces ou de connexions avec les autres parties du système (par exemple sans fil), emplacement physique, exigences en matière d'accès, fonction opérationnelle, les responsabilités organisationnelles pour chaque actif, l'aspect de la sûreté (Safety), le cycle de vie du produit, l'obsolescence.

Le découpage en zones procède de deux logiques complémentaires : d'une part celle de la défense en profondeur visant à circonscrire les conséquences d'un dommage et à opposer à une menace des remparts successifs, d'autre part celle de la défense des accès à la périphérie de préférence à un durcissement de chacun des constituants, approche plus difficile et plus onéreuse.

Les zones ne sont jamais isolées. Elles sont reliées, soit au monde extérieur, soit à une autre zone par un ou plusieurs conduits qui regroupent des canaux de communication, réels (réseaux et équipements associés) ou équivalents (conduits de compensation : connexions USB ou autres).

Une attention particulière doit être portée aux SIS (Safety Instrumented System), aux systèmes sans fil et aux équipements mobiles ou nomades (ordinateurs portables, tablettes, smartphones). Ces systèmes peuvent faire l'objet d'une zone spécifique. Une zone démilitarisée (DMZ) peut également être introduite lorsqu'il est nécessaire d'introduire une zone tampon par laquelle passeront toutes les communications vers une zone sensible telle que la zone de contrôle.

ETAPE 4 : Implémentation des mesures de sécurité : L'analyse des risques, associée à la segmentation du système en zones de sécurité, nous offre la possibilité de déterminer un niveau de sécurité cible (SL-T) pour chaque zone et conduit. Cette démarche se traduit par un vecteur contenant sept composantes, chacune représentant l'une des exigences fondamentales en matière de cybersécurité (FR1 à FR7) telles que définies dans la norme IEC 62443-3-3 (voir chapitre ‘’Structure de la norme IEC 62443’’). [10]

En fonction des risques identifiés, ces exigences doivent être respectées à des niveaux variables, allant de 1 à 4 selon la norme IEC 62443-3-3. Chaque exigence fondamentale est accompagnée d'un ensemble de critères définis par cette série de normes. Ces critères permettent d'évaluer le respect des exigences et d'attribuer une note correspondant au niveau atteint. [10]

En comparant les niveaux cibles (SL-T) et les niveaux réalisés (SL-A), nous pouvons repérer les éventuelles lacunes et les localiser précisément. C'est sur ces points que doit se concentrer en priorité l'effort de mise en œuvre de contre-mesures, dans le but d'atteindre, dans la pratique, les niveaux de sécurité définis comme objectifs.

La figure ci-dessous est tirée d'un cas réel. Elle démontre la mise en œuvre des exigences de sécurité pour une salle des équipements techniques avec un niveau de sécurité cible égal à 3 (SL3-T).

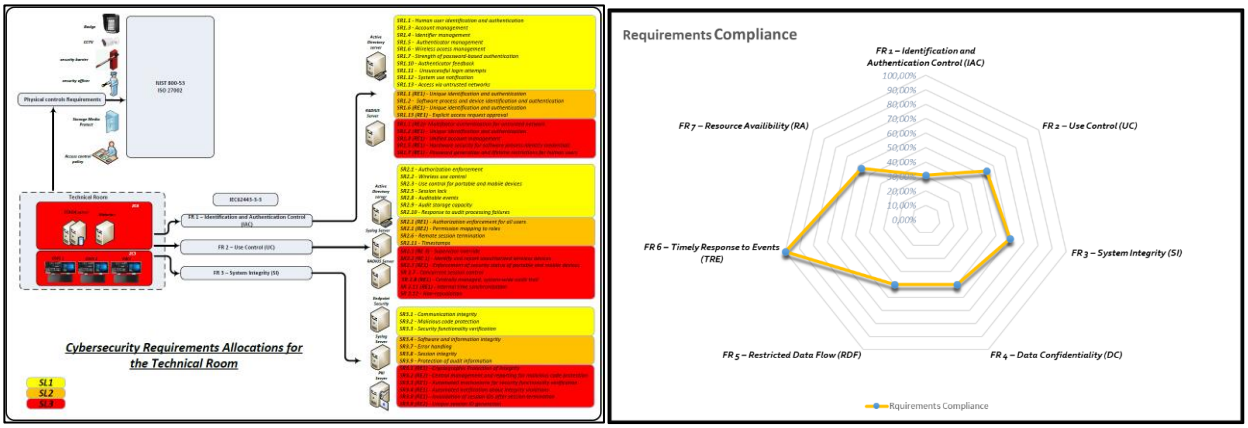

Fig. 10. Exemple d'attribution et de conformité des exigences de sécurité.

Le but est de déterminer le niveau de sécurité cible SL-T du système OT et établir un écart (gap analysis) entre le SL-T et le niveau de sécurité atteint SL-A comme le montre cette figure :

Cette étude d'écart va nous permettre d'avoir un ''tableau de bord'' qui met en exergue la conformité du système OT avec les exigences de la nome IEC 62443.

Si le système OT ne peut pas répondre aux exigences de sécurité définies, cela peut être dû à diverses raisons telles que des limitations techniques (par exemple, des exigences contradictoires de l'ingénierie du système ayant une priorité plus élevée), l'obsolescence des équipements ou des limitations de ressources. Dans de telles situations, il est possible de proposer des mesures compensatoires visant à minimiser le risque encouru.

ETAPE 5 : Architecture sécurisée et documentations : Après avoir réalisé les étapes précédentes, l'objectif de cette étape est de définir les règles encadrant les échanges d'information entre les différentes zones ainsi que les mesures de sécurité permettant leur mise en œuvre.

Parmi les règles importantes à prendre en compte pour chaque architecture :

- Les flux entre les différentes zones et les différents conduits doivent être filtrés ;
- Les flux doivent être initiés depuis une zone de criticité élevée vers une zone de criticité moindre ;
- Les flux initiés depuis une zone de moindre confiance ne doivent être à destination que d'une zone présentant un même niveau de criticité.

Le respect de ces règles va impliquer la création de zones intermédiaires aussi appelées « zones démilitarisées » (DMZ). [5]

Ces zones ont un rôle de passerelle sécurisée hébergeant à titre d'exemple des systèmes relais (patch management, signatures antimalware, télémaintenance, etc.) et assurant l'interfaçage sécurisé entre l'environnement de contrôle industriel et « le reste du monde » (par le biais d'un SI de gestion classique généralement).

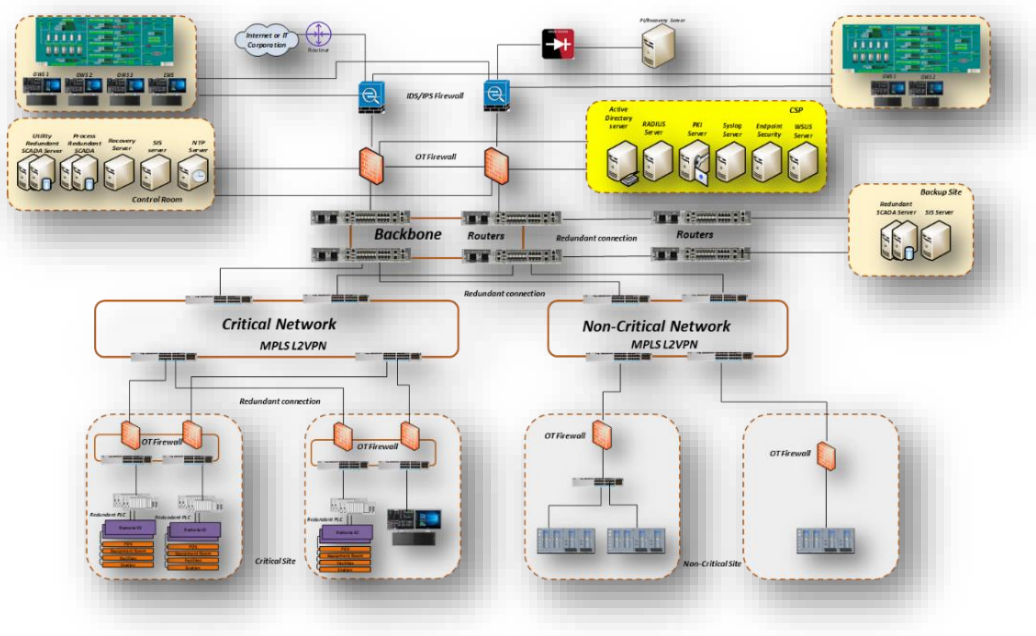

Fig. 11. Exemple d'architecture sécurisée.

Un simple pare-feu entre le système IT et le système OT s'est avéré insuffisant dans de nombreux incidents de sécurité (attaques sur réseaux électriques ukrainiens, nombreuses diffusions récentes de rançongiciels ayant touché les systèmes industriels, etc.).

En pratique, il doit y avoir à minima une DMZ pour séparer, avec rupture de flux, le système IT et le système industriel OT.

B. MAINTIEN EN CONDITION DE SECURITE (MCS)

Au cours du cycle de vie du système, le niveau de sécurité est amené à décliner. Les sources de cette baisse du niveau de sécurité sont multiples, à titre d'exemple : rapprochement entre les différents métiers, nouveaux outils d'attaques et nouveaux acteurs de menace, découverte de nouvelles vulnérabilités. [7]

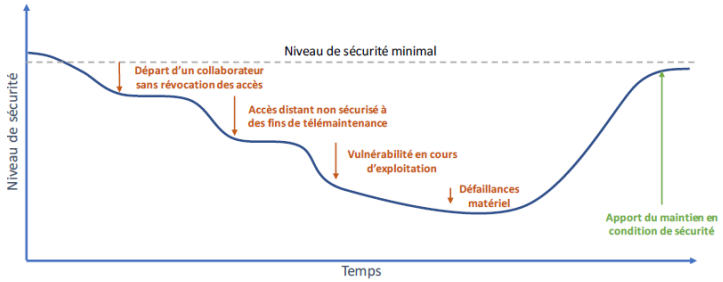

Fig. 12. Evolution du niveau de sécurité d'un système OT dans le temps.

Le maintien en conditions de sécurité est donc un travail à effectuer quotidiennement qui vise à s'assurer que les systèmes respectent les règles et mesures de sécurité préalablement définies (voir les étapes précédentes).

Le MCS est un processus continu et évolutif qui vise à réduire les risques de sécurité, à protéger les systèmes industriels contre les menaces et à assurer la disponibilité opérationnelle continue des systèmes critiques dans un environnement industriel.

Il nécessite une gestion proactive, une planification adéquate et une collaboration entre les équipes de sécurité, les équipes opérationnelles et les parties prenantes de l'entreprise afin d'assurer, notamment, les recommandations suivantes : surveillance continue, mises à jour et correctifs, gestion des Vulnérabilités, tests d'intrusion conditionnel, politiques et procédures, gestion des Incidents, contrôle des accès, gestion de crise, sauvegarde et reprise après incident, formation et sensibilisation.

C. UN MOT SUR LA CONVERGENCE CYBERSECURITE ET SURETE (SAFETY)

Depuis longtemps, les concepts de cybersécurité et de sûreté (safety) étaient traités séparément dans les environnements industriels. La cybersécurité se concentrait sur la protection des systèmes contre les cyberattaques, tandis que la sûreté visait à prévenir les accidents et à garantir le bon fonctionnement des systèmes.

Cependant, avec l'intégration croissante des technologies numériques et automatisées dans les systèmes de contrôle industriel, il est devenu évident que ces deux domaines doivent converger pour assurer une protection complète des infrastructures critiques.

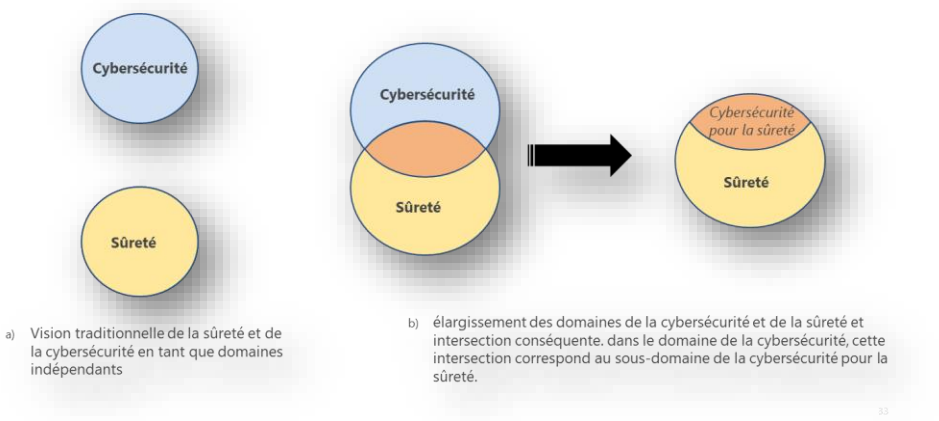

Fig. 13. Convergence Cybersecurité et Safety.

Par exemple, une faille de sécurité informatique dans un système de contrôle industriel (OT) peut entraîner des conséquences graves en termes de Safety, telles que des accidents industriels ou des pannes d'équipement. De même, des défaillances matérielles ou des erreurs humaines dans les systèmes industriels peuvent également créer des vulnérabilités de cybersécurité en exposant les systèmes informatiques à des risques accrus de cyberattaques. [2]

Les méthodes d'analyse des risques et les moyens de prévention des risques accidentels ne sont pas adaptés à traiter et analyser les risques liés à la Cybersécurité. Ces derniers sont rarement évalués et lorsqu'ils le sont, cela se produit dans des processus et des études dissociées des analyses des risques accidentels.

En conséquence, il est devenu essentiel pour les entreprises de prendre en compte à la fois la Cybersécurité et la Safety dans leurs stratégies de gestion des risques afin de protéger efficacement leurs opérations, leurs employés et leurs actifs. Cela nécessite une approche intégrée qui comprend la mise en œuvre de mesures de cybersécurité robustes ainsi que des pratiques solides de la Safety pour assurer la résilience et la continuité des activités dans un environnement industriel de plus en plus complexe et interconnecté.

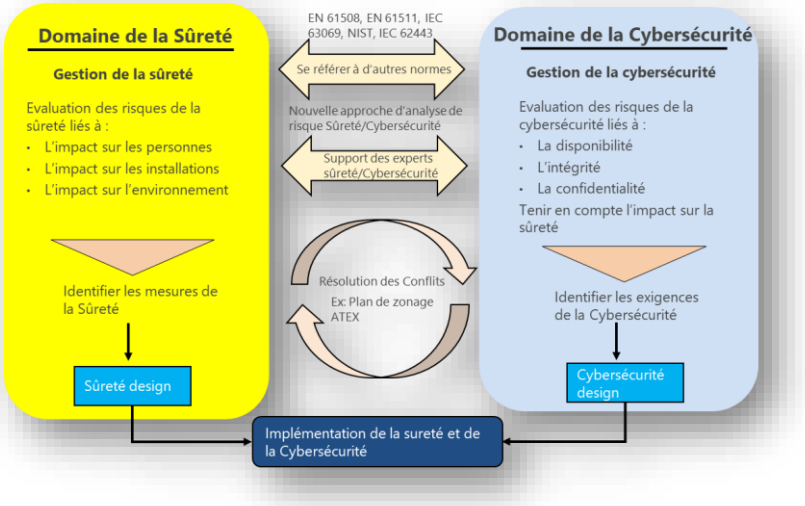

Fig. 14. Collaboration Cybersécurité et Safety

La synergie entre Cybersécurité et Safety dans les environnements industriels exige l'élaboration de méthodes novatrices qui intègrent à la fois le degré de sécurité et le niveau de gravité des installations industrielles. Cela permet de déterminer avec précision le degré de criticité des scénarios de risque et d'élaborer des stratégies de sécurité robustes pour réduire ou éliminer les risques inacceptables.

Cette approche combine une évaluation approfondie des cybermenaces potentielles avec une analyse rigoureuse des dangers liés à la Safety des opérations industrielles. Elle prend en compte la nature interconnectée des systèmes informatiques et des processus physiques, reconnaissant que les vulnérabilités dans l'un peuvent affecter directement l'autre.

En intégrant les deux aspects, les équipes de Cybersécurité/Safety peuvent évaluer de manière plus précise les risques associés aux activités industrielles et développer des contre-mesures adaptées à ces risques. Cela comprend la mise en place de barrières de sécurité technologiques et opérationnelles pour atténuer les menaces potentielles et réduire la probabilité d'incidents graves.

VII. CONCLUSION

La convergence entre les domaines de la technologie de l'information (IT) et de la technologie opérationnelle (OT) représente une évolution majeure dans les environnements industriels contemporains. Cette convergence vise à intégrer les systèmes informatiques traditionnels avec les équipements et les processus physiques utilisés dans la production industrielle, créant ainsi des systèmes interconnectés et interdépendants. Elle reflète une reconnaissance croissante de l'importance de la connectivité entre les systèmes informatiques et les systèmes de contrôle industriels pour améliorer l'efficacité opérationnelle, la flexibilité et la capacité d'innovation des entreprises.

Parallèlement, la convergence entre Cybersécurité et Safety est une autre dimension essentielle de l'évolution des environnements industriels. Elle vise à traiter les risques liés à la cybersécurité et les risques liés à la safety des processus de manière cohérente, afin d'assurer la sûreté et la sécurité des opérations industrielles dans leur ensemble.

En combinant ces deux convergences, les entreprises cherchent à relever les défis complexes de sécurité dans les environnements industriels modernes.

Bien que la pratique de la sécurité by design soit encore rare parmi les entreprises, elle représente la stratégie la plus efficace pour protéger les systèmes industriels contre les cybermenaces. En combinant des normes rigoureuses, des méthodologies d'analyse des risques, des technologies avancées, des pratiques de gestion solides et une approche intégrée de la cybersécurité et de la sûreté, les entreprises peuvent se préparer plus efficacement à faire face aux menaces croissantes. La mise en œuvre de la sécurité dès la phase de conception permet non seulement de créer des systèmes plus robustes mais aussi de réduire les coûts et les efforts nécessaires pour remédier aux vulnérabilités identifiées à posteriori.

VIII.REFERENCES

Livre

[1]. ACKERMAN, P. (2021). Industrial Cybersecurity: Efficiently monitor the cybersecurity posture of your ICS environment Packt Publishing

Thèse

[2]. CHEMALI, R. (2021). Méthodologie orientée sûreté de fonctionnement pour la cybersécurité des systèmes de contrôle-commande; [Thèse de Doctorat, Université de Lille]. https://theses.hal.science/tel-04198264v1

Rapports

[3]. ANSSI. (2018, Décembre). Cybersécurité pour la maintenance des installations industrielles. https://cyber.gouv.fr/publications/la-cybersecurite-des-systemes-industriels

[4]. ANSSI, (2014, Octobre). Mesures détaillées. https://cyber.gouv.fr/sites/default/files/2014/01/securite_industrielle_GT_details_principales_mesures.pdf

[5]. Rockwell Automation. (2022, Mars). Securely Traversing IACS Data across the Industrial Demilitarized Zone Design and Implementation Guide, https://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td009_-en-p.pdf

[6]. Cigref. (2019,Décembre). Convergence IT/OT. Un rapprochement fructueux des systèmes d'information et des systèmes industriels, https://www.cigref.fr/un-rapprochement-fructueux-des-systemes-industriels-et-des-systemes-dinformation-convergence-it-ot

[7]. Clusif. (2021, Février). Guide cybersécurité des systèmes industriels, https://clusif.fr/publications/guide-cybersecurite-des-systemes-industriels-2021/

Normes

[8]. NIST Special Publication 800-82 Revision 2: Guide to Industrial Control Systems (ICS) Security

[9]. IEC 62443-3-2. Juin 2020. Security for industrial automation and control systems – Part 3-2: Security risk assessment for system design

[10]. IEC 62443-3-3. Août 2013. Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels

Sites internet

[11]. America's Cyber Defense Agency. Consulté en avril 2024 sur https://www.cisa.gov/uscert/ics/Recommended-Practices

[12]. Nicaise, V. (2020, Juillet) consulté en avril 2024 sur https://www.stormshield.com/fr/actus/iec-62443-le-standard-incontournable-de-la-cybersecurite-industrielle/

[13]. HAUET, JP. (Octobre, 2016). Processus et normes de cybersécurité dans l'industrie L'IEC 62443 consulté en avril 2024 sur https://archive.g-echo.fr/20161005-hauet-kb.pdf

[14]. KASPERSKY (2021, Octobre) APT Attacks on industrial organizations in H1 2021 consulté en Avril 2024 sur https://ics-cert.kaspersky.com/media/Kaspersky-ICS-CERT-APT-attacks-on-industrial-organizations-in-H1-2021-En.pdf

[15]. NIST (2023, Juillet) Computer security ressource center, consulté en Avril 2024 sur https://csrc.nist.gov/publications/sp

[16]. Industrie du futur . (2020, Décembre) consulté en avril 2024 sur https://industrie-du-futur.info/larchitecture-opc-ua-repond-aux-attentes-des-reseaux-dautomatismes-industriels-daujourdhui/