PROTÉGER LE FUTUR CONNECTÉ

QUELS SONT LES ENJEUX DE LA CYBERSÉCURITÉ DANS L'INDUSTRIE ?

LIVRE BLANC 2023

SERMA
SAFETY & SECURITY

contact-S3@serma.com
www.serma-safety-security.com

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. Que ces attaques visent à voler des secrets industriels ou à saboter la production, ces acteurs malveillants constituent une menace réelle pour les processus industriels et les systèmes qui les supervisent.

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 gérer la convergence des technologies de l'information (IT) et des technologies opérationnelles (OT) tout en maintenant une certaine isolation ?

Dans ce livre blanc, les experts de SERMA Safety and Security expliquent comment la méthode d'évaluation et de sécurisation des systèmes OT développée par SERMA Safety and Security offre un cadre pour faire face aux attaques qui menacent la sécurité des installations industrielles.

**Les technologies opérationnelles font référence aux outils et systèmes utilisés dans les installations industrielles pour gérer les opérations de production, surveiller les processus et maintenir le bon fonctionnement des équipements.*

Quels sont les enjeux de la cybersécurité dans l'industrie ?

C'est avec le souhait d'intégrer des technologies de pointe (IoT, intelligence artificielle, robotique) dans les environnements industriels traditionnels que les systèmes de contrôle industriel (ICS) connectés, les sondes, capteurs et autres réseaux (ZigBee, Bluetooth, LoRaWAN, WIFI, 4G/5G) se sont multipliés.
Si sur le papier ces évolutions permettent des avancées technologiques majeures, elles apportent leurs lots de problématiques au quotidien : élargissement de la surface d'attaque, multiplication des maintenances et mises à jour, augmentation du nombre d'entreprises sous-traitantes...

L'OT, comme l'IT, est soumis à un nombre important de vulnérabilités. Rien que sur l'année 2021, 637 vulnérabilités ont affecté des systèmes de contrôle industriel sur le territoire français selon le rapport de l'éditeur Claroty. Au niveau mondial, ce n'est pas moins de 797 vulnérabilités qui ont été publiées, impactant par la même occasion 82 constructeurs. Ces vulnérabilités sont diverses et touchent à la fois la couche logicielle et le firmware, ne laissant ainsi aucune option de remédiation pour des équipements anciens qui ne sont plus supportés par les constructeurs.

Pour faire face à cet enjeu, l'OT ne doit plus être considéré comme le parent pauvre de l'IT traditionnel. Au travers de l'application stricte des standards et bonnes pratiques de cybersécurité, une acculturation des équipes aux environnements de production doit se faire en intégrant le risque cyber dans leur quotidien.
Cette étape peut être réalisée au travers de la désignation et de la montée en compétences d'un référent cybersécurité présent sur le site de production ou par l'équipe SSI elle-même.
Une vision convergente IT/OT doit s'appliquer en intégrant les spécificités de chaque environnement opérant ainsi un même niveau de sécurité que l'on soit dans des environnements on-premise ou dans le cloud.

01 | IT ET OT : COMPRENDRE CES DEUX SYSTÈMES

La Technologie de l'Information | IT

La technologie de l'information (IT) englobe tout ce qui concerne les ordinateurs, du matériel aux logiciels, ainsi que la gestion des réseaux, du stockage de données et de la sécurité informatique. Elle est essentielle pour permettre aux organisations de traiter l'information, de communiquer efficacement et d'automatiser divers processus. L'IT joue un rôle central dans la productivité et la compétitivité des entreprises modernes, en garantissant que leurs systèmes informatiques fonctionnent de manière optimale.

En résumé, l'IT est la clé de voûte de la gestion de l'informatique au sein des entreprises, et elle a un impact significatif sur leur réussite et leur efficacité opérationnelle.

La Technologie Opérationnelle | OT

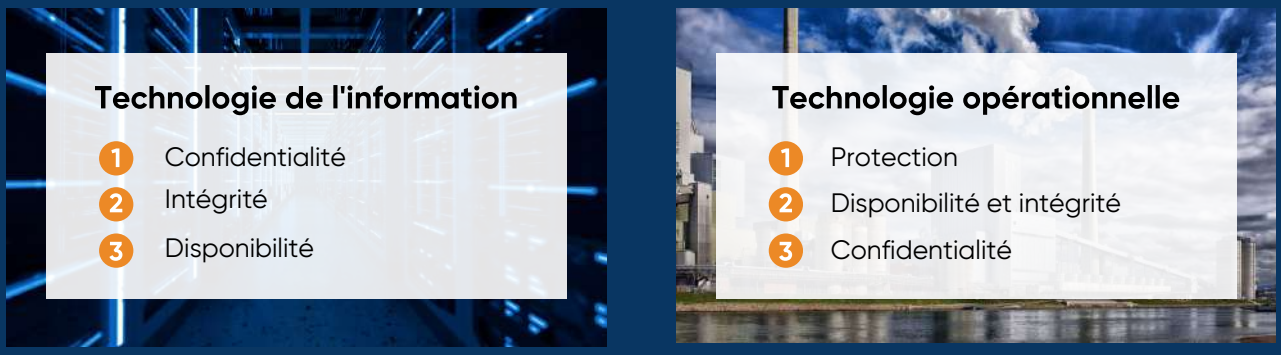
La technologie opérationnelle (OT) se réfère aux équipements matériels et logiciels utilisés pour surveiller et contrôler les processus physiques dans des environnements industriels. Contrairement à l'informatique (IT) qui gère les données et les systèmes informatiques, l'OT se concentre sur la gestion des équipements tels que des machines de production, des capteurs et des systèmes de contrôle automatisés. Elle est essentielle pour assurer le bon fonctionnement des processus industriels, la sécurité des installations et la qualité des produits.

L'OT peut nécessiter une intervention humaine pour prendre des décisions critiques, comme l'ajustement de la température dans une usine ou l'arrêt d'une machine en cas d'urgence. En résumé, l'OT joue un rôle crucial dans la surveillance et le contrôle efficaces des processus physiques dans le secteur industriel.

La différence entre ces deux technologies

L'IT s'occupe de l'information, tandis que l'OT prend en charge les machines. Ainsi, le premier gère le flux d'informations numériques, tandis que le second assure le fonctionnement des processus physiques et des mécanismes utilisés pour les exécuter.

Puisque l'IT implique principalement le stockage, la récupération, la manipulation et la transmission d'informations numériques, la confidentialité des données constitue une préoccupation majeure. La sécurité informatique devient cruciale dans chaque organisation afin de garder ses données en sécurité et sous contrôle.

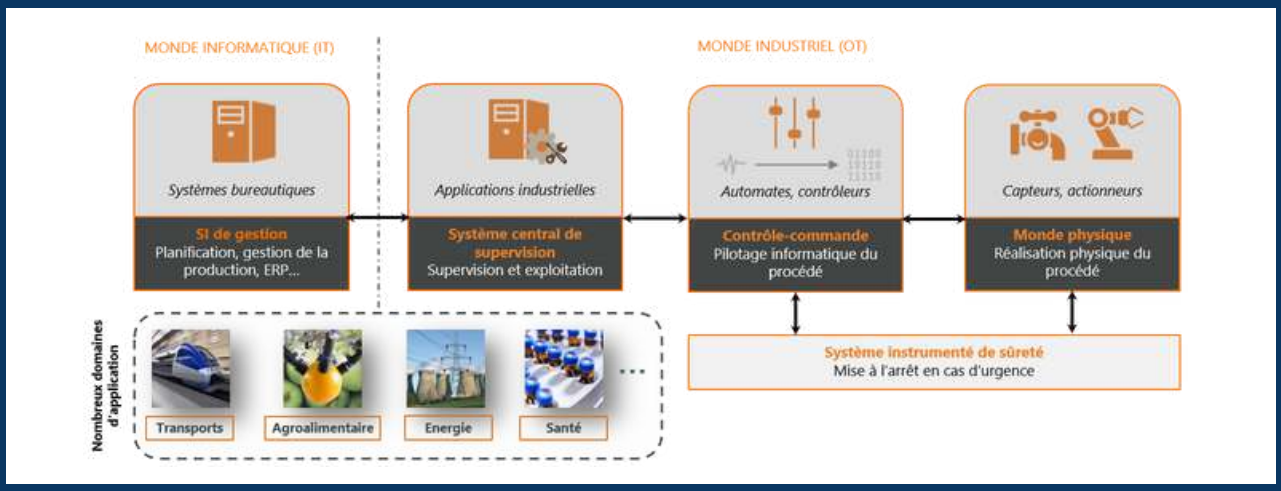


Source : SERMA Safety & Security
Figure 1 : Critères de sécurité entre IT et OT

Dans le domaine de l'OT, la protection et la disponibilité des équipements et des processus dominent. Le traitement des systèmes physiques qui doivent maintenir des valeurs stables, telles que la température et la vitesse de rotation, exige un contrôle méticuleux.

02 | COMPOSANTS D'UN SYSTÈME 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 de contrôler et commander les entités physiques. Très souvent, les éléments de l'OT sont exploités par des logiciels spécifiques, comme les logiciels SCADA.

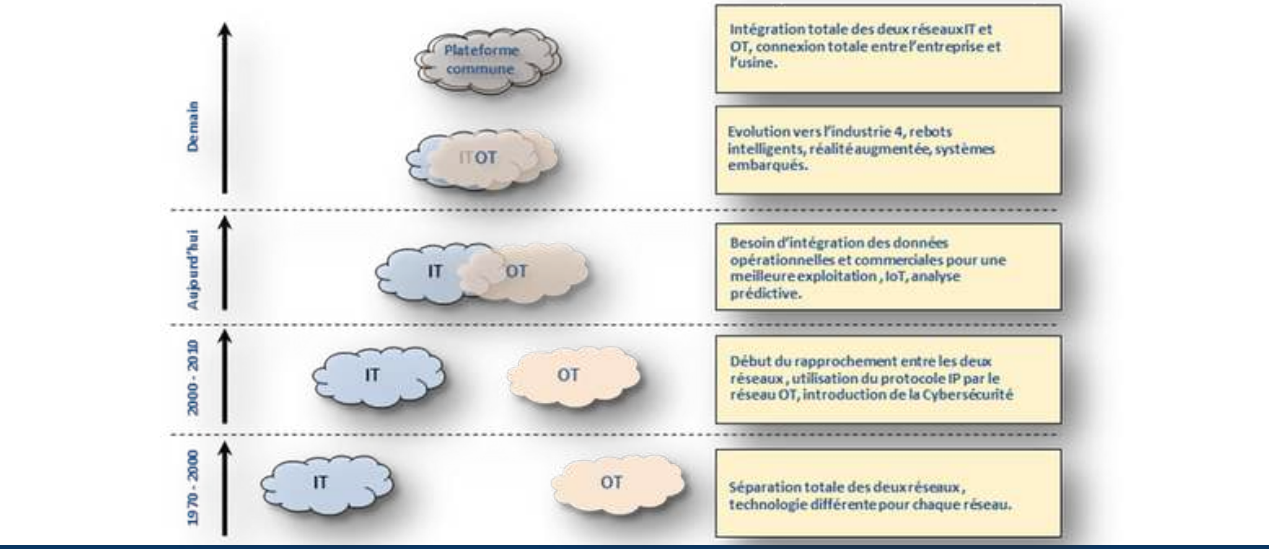


Source : SERMA Safety & Security
Figure 2 : Composants d'un système OT

Comme le montre la figure ci-dessus, un système OT est composé d'une part d'un système de traitement de l'information, composé de postes de travail, de serveurs et d'équipements réseau, de systèmes de stockage et de sauvegarde, et d'autre part d'un ensemble d'équipements spécifiques permettant d'agir avec le monde physique par la réception des grandeurs mesurées (telles que la température, la pression ou la présence d'un objet), et l'application des commandes de contrôle (telles que l'ouverture d'une vanne, la mise en action d'un vérin ou l'ouverture et la fermeture d'un circuit).

03 | CONVERGENCE IT | OT

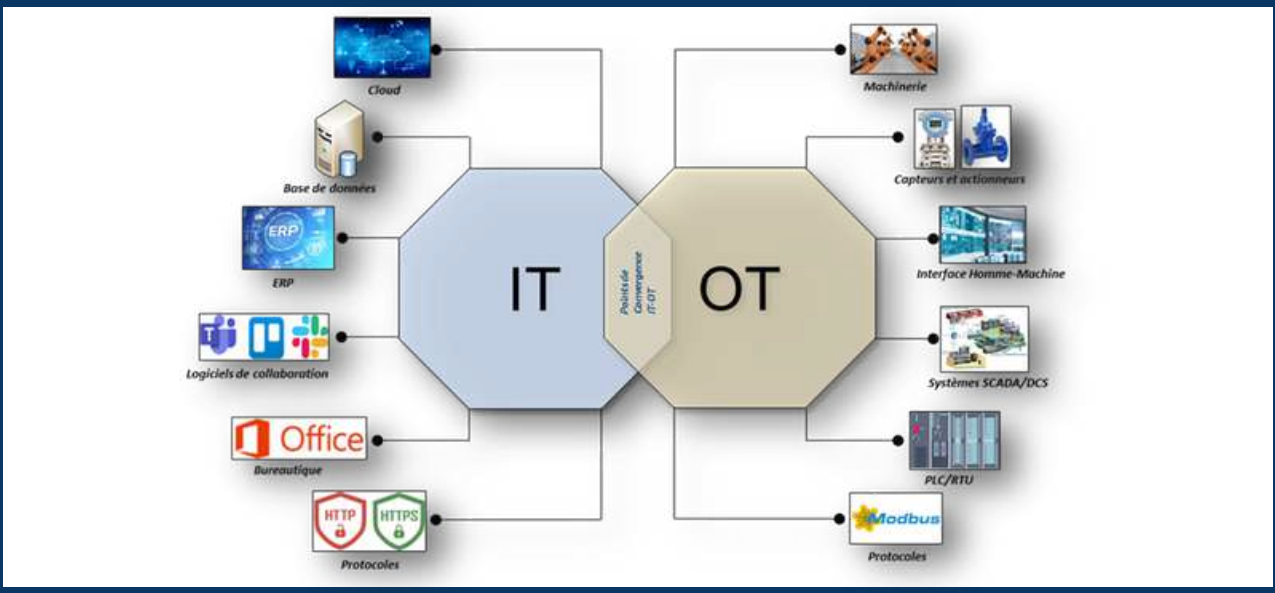
Le rapprochement entre le monde du système d'informations d'entreprise en charge principalement du traitement des données de l'entreprise et le monde des systèmes industriels regroupant les opérations couvrant les installations physiques de production « industrielle » de l'entreprise, est aujourd'hui une évidence.



Source : SERMA Safety and Security

Figure 3 : Convergence progressive dans le temps par l'utilisation de technologies IT dans les systèmes industriels

Les grands acteurs industriels ont déjà engagé une réflexion sur la convergence entre l'univers de l'IT (« Information Technology »), reposant sur l'intelligence logicielle et sur des standards très ouverts, et le monde de l'OT (« Operations Technology ») qui dépend de dispositifs physiques (capteurs, automates, superviseurs…) ayant privilégié les technologies propriétaires.



Source : SERMA Safety and Security

Figure 4 : Les points de convergence entre l'OT et l'IT

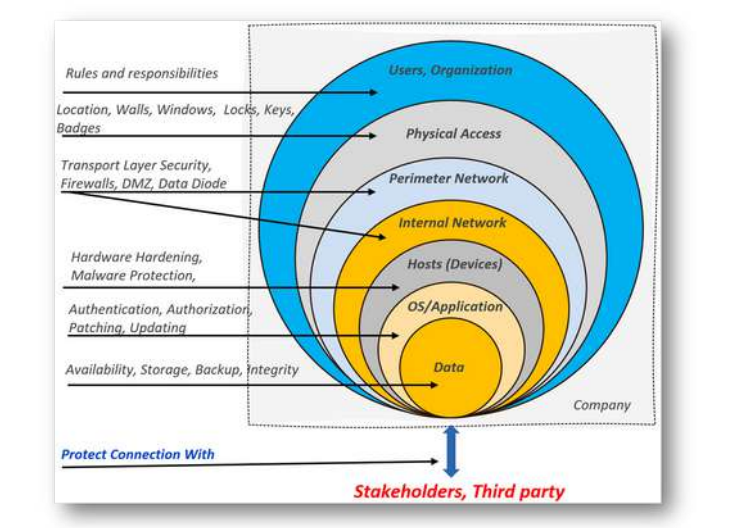
Cette convergence conduit à un nouveau défi en termes de cybersécurité. L'arrivée des applications industrielles dans les infrastructures du système d'information a entrainé une prise de conscience du besoin de synergie.

Quelles sont les démarches à adopter pour répondre à ces enjeux ?

Pour répondre à ces enjeux de cybersécurité, les entreprises industrielles peuvent s'appuyer sur des standards et des bonnes pratiques

01 | DÉFENSE EN PROFONDEUR

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.



Source : SERMA Safety and Security
Figure 5 : Défense en profondeur (defense in depth)

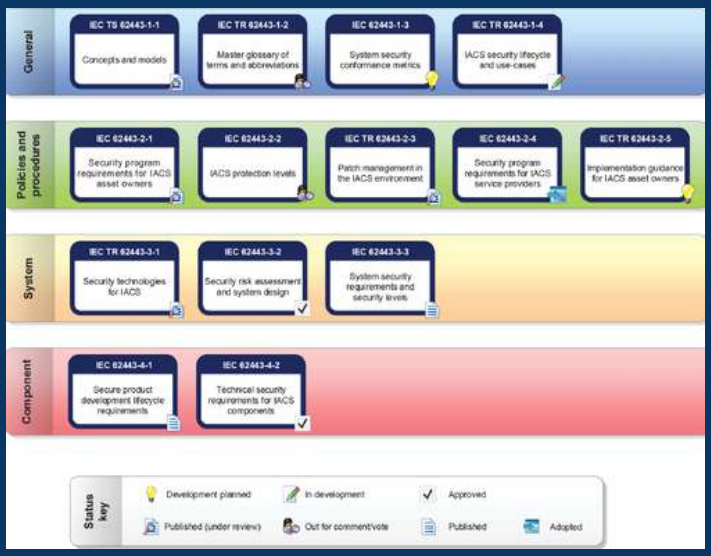
Cette approche multicouche augmente la sécurité d'un système dans son ensemble et s'attaque à de nombreux vecteurs d'attaque différents.

Pour mettre en œuvre ce concept, **SERMA Safety and Security a développé la démarche "CERMA" en se basant notamment sur :**

- Proposition de mesures de sécurité organisationnelles (Politiques de sécurité, Procédures, PCA...)
- Evaluation de la maturité cyber d'un système OT (analyse de risque et détermination du niveau de sécurité (SL : Security Level))
- Répartition du système OT en zones et conduits
- Application des contrôles de sécurité selon les normes IEC62443, NIST, ISO27001 et ISO27002
- Proposition des architectures sécurisées.

02 | NORME IEC 62443

La norme IEC 62443 est le référentiel spécifique à la cybersécurité industrielle, elle définit le cadre de cyberdéfense des systèmes industriels, pour tous type de centre de production (station d'épuration, fabrication électronique, usine pharmaceutique, automobile fonderie, raffinerie, ...).
Les premiers travaux sur la norme IEC 62443 ont débuté au sein du groupe de travail ISA SP99 et se poursuivent actuellement dans le cadre d'une coopération entre la IEC et l'ISA.



Source : IEC 62443
Figure 6 : Les séries de l'IEC 62443

Comme le montre cette figure, la série de normes IEC 62443 se compose de quatre domaines principaux, qui sont représentés comme suit :

1. IEC 62443-1 : Information Générale
2. IEC 62443-2 : Procédures et politiques de sécurité
3. IEC 62443-3 : Exigences de sécurité relatives aux systèmes
4. IEC 62443-4 : Exigences de sécurité relatives composants

La norme IEC 62443 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.

FOUNDATIONAL REQUIREMENT	ASSOCIATED PROCESS
FR1- Identification, Authentification, and Access control	User authentification 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

Source : IEC 62443
Figure 7 : Exigences fondamentales

Comme le montre l'exemple du tableau ci-dessous, pour chacune des exigences fondamentales existent un certain nombre d'exigences de sécurité technique (SR) et d'améliorations (RE) spécifiques classées selon quatre (04) niveaux de sécurité 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

Source : IEC 62443
Figure 8 : 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 menaces cybernétiques.
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, SL1 étant le niveau de sécurité 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 installation 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 : (Voir Annexe A de la norme IEC62443-3-3 pour plus de détail)

- 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.

Comment SERMA Safety and Security évalue et sécurise un système OT ?

La cybersécurité étant un domaine en constante évolution, il est essentiel de planifier la mise en oeuvre 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 de ces clients, 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 IEC62443 et spécifiquement IEC62443-3-2 et IEC62443-3-3 et éventuellement la IEC62443-2 si le Client souhaite un plan de cybersécurité organisationnel (CSMS) ;
- D'autres normes internationales à savoir NIST et ISO27000 ;
- Les bonnes pratiques de la sécurité industrielle recommandées par l'ANSSI.
- L'Approche de la défense en profondeur ;

Cette méthodologie appelée ''CERMA'' (Cybersecurity Evaluation and Risk MAnagement) comprend les étapes suivantes :

Source : SERMA SAFETY AND SECURITY

Figure 9 : Méthodologie d'évaluation et de sécurisation d'un système OT

01 | DESCRIPTION EN DÉTAIL DES CINQ ÉTAPES 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, si possible, le réseau OT pour identifier les périphériques connectés et leur relation les uns avec les autres ;
- Classifier les actifs selon leur criticité afin d'hiérarchiser les mesures de sécurité.

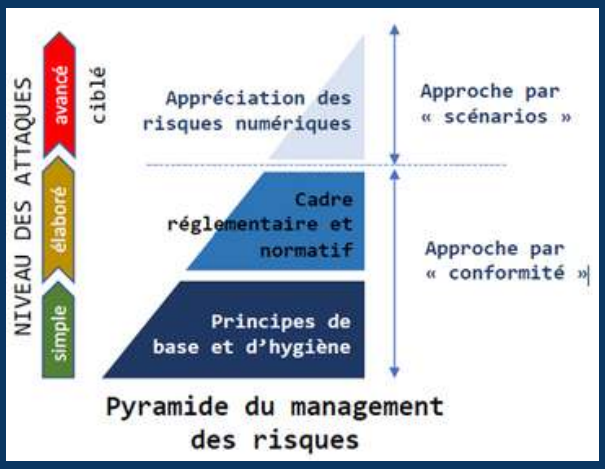
ETAPE 2 : ANALYSE DE RISQUE DE HAUT NIVEAU

Comme le prévoit la norme **IEC62443-3-2**, 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, **SERMA Safety and Security** utilise la méthode **EBIOS Risk Manager.**
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 maitriser.



Source : ANSSI

Figure 10 : 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 et se déroule en cinq ateliers :

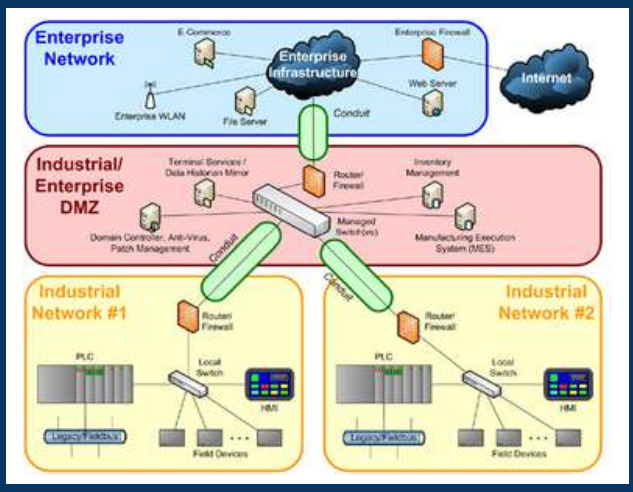
- **Atelier 1 :** Définir le cadrage et le socle de sécurité (Approche par conformité) ;
- **Atelier 2 :** Définir les sources de risque (couple SR/OV) ;
- **Atelier 3 :** Définir les scénarios stratégiques et les chemins d'attaques (Approche par scénarios)
- **Atelier 4 :** Définir le mode opératoire ou technique du chemin d'attaque établi dans l'atelier 3.
- **Atelier 5 :** Traiter le risque

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 CONDUITS ET ATTRIBUTION DU NIVEAU DE SÉCURITÉ (SL)

À la suite de l'analyse de risque de haut niveau (High Level Risk Assessment), SERMA Safety & Security procède à la décomposition du système OT en zones et conduits.

La norme IEC 62443-3-2 introduit les concepts de "zones" et de "conduits" 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.).



Source : IEC 62443

Figure 11 : Répartition d'un système OT en zones et conduit

Les critères suivants doivent être pris en compte pour partitionner le système OT en zones et en conduits :

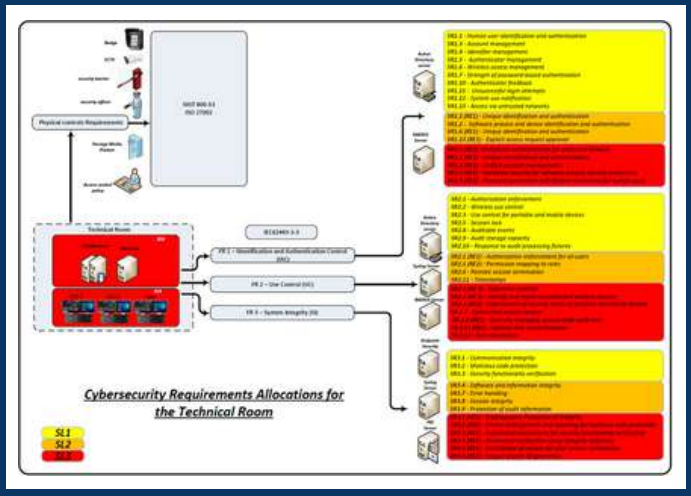
- Risque pour les actifs en termes d'intégrité, de disponibilité et de confidentialité ;
- Type d'interfaces ou de connexions avec les autres parties du système (par exemple sans fil) ;
- Emplacement physique ;
- Exigences en matière d'accès ;
- Fonction opérationnelle ;
- Responsabilités organisationnelles pour chaque actif ;
- Aspect de la sûreté de fonctionnement ;
- Cycle de vie du produit, l'obsolescence.

Une fois que le système OT a été décrit en termes de zones et de conduits, des niveaux de sécurité cibles (SL-T) seront individuellement attribués à chaque zones et conduits.

ETAPE 4 : IMPLÉMENTATION DES MESURES DE SÉCURITÉ

Après avoir réalisé l'étape 3, les exigences de sécurité telles que définies dans la norme IEC 62443-3-3 seront appliquées à chaque zone et conduit en tenant compte de leur criticité.

Cette figure (établie par SERMA Safety and Security) montre un exemple de la mise en œuvre des exigences de sécurité pour une salle d'équipements techniques avec un niveau de sécurité cible égal à 3 (SL3-T).



Source : SERMA Safety and Security

Figure 12 : Exemple d'attribution des exigences de sécurité pour une salle technique

SERMA Safety and Security travaille en étroite collaboration avec ses clients pour l'implémentation des mesures de sécurité afin de déterminer le niveau de sécurité cible SL-T du système OT et établit un écart (gap-analysis) entre le SL-T et le niveau de sécurité actuel SL-C.

Source : SERMA Safety and Security
Figure 13 : Conformité des exigences de sécurité

Cette étude d'écart va permettre aux clients d'avoir un ''tableau de bord'' qui met en exergue la conformité de leur système OT avec les exigences de la nome IEC62443.

Si le système OT ne peut pas satisfaire aux exigences de sécurité définies, qui peut être due à des limitations techniques (par exemple, des exigences contradictoires de l'ingénierie du système ayant une priorité plus élevée), des obsolescences ou à des limitations de ressources, SERMA Safety and Security peut proposer des mesures compensatoires afin de minimiser le risque.

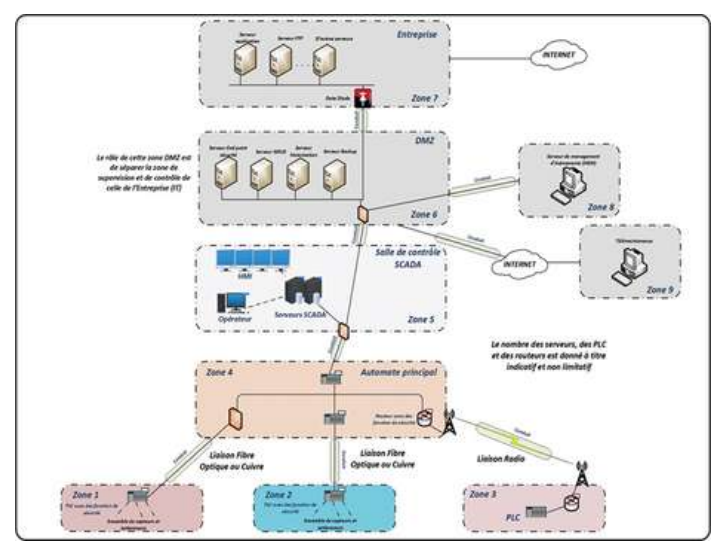
ETAPE 5 : ARCHITECTURE SÉCURISÉE ET DOCUMENTATIONS

L'objectif pour SERMA Safety & Security dans 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.

Plusieurs règles doivent être prises en compte suivant l'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).

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 sécurisée entre l'environnement de contrôle industriel et « le reste du monde » (par le biais d'un SI de gestion classique généralement).



Source : SERMA Safety and Security
Figure 14 : Exemple d'architecture sécurisée

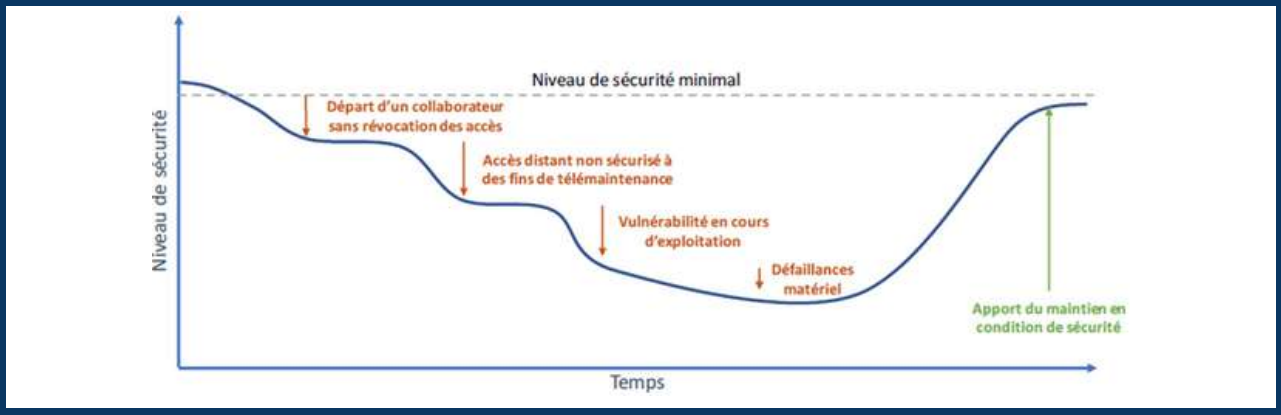
Un simple pare-feu entre le système IT et le système OT s'est avéré insuffisant dans de nombreux incidents de sécurité (attaques sur réseaux électriques ukrainiens, nombreuses diffusions récentes de rançongiciels ayant touché les systèmes industriels, etc.).
En pratique, il doit y avoir à minima une DMZ pour séparer, avec rupture de flux, le système IT et le système industrielle OT.

Toutes les étapes précédemment décrites seront documentées par SERMA Safety and Security.

02 | MAINTIEN EN CONDITION DE SÉCURITÉ (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 et peuvent être sources de nouvelles vulnérabilités :

- Evolution des usages du système d'information via, par exemple, un rapprochement entre les différents métiers.
- Evolution de la menace : nouveaux outils d'attaques et nouveaux acteurs de menace.



Source : Clusif

Figure 15 : 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. Il 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.

Pour ce faire, SERMA Safety and Security accompagne ses clients afin d'assurer les recommandations suivantes :

- Surveillance continue ;
- Mises à jour et correctifs ;
- Gestion des vulnérabilités ;
- Tests d'intrusion conditionnels ;
- Politiques et procédures ;
- Gestion des incidents ;
- Contrôle des accès ;
- Gestion de crise, sauvegarde et reprise après incident ;
- Audit et conformité
- Communication et partage d'informations
- Formation et sensibilisation.

La sécurité informatique est un processus continu et dynamique, plutôt qu'un objectif final et immuable. Atteindre une sécurité totale demeure hors de portée, étant donné que de nouvelles vulnérabilités émergent constamment et que les menaces évoluent sans cesse. Même avec des mesures de sécurité en place, le comportement du personnel peut devenir négligent au fil du temps et des solutions contournant les contrôles peuvent être trouvées. Les faiblesses d'un système subissent des mutations, créant ainsi de nouvelles opportunités pour les attaques.

La sécurité exige un processus continu et une mentalité proactive. "Toute confiance est limitée". C'est en gardant à l'esprit cette maxime que l'on peut aborder la sécurité de manière adéquate. Il est essentiel de considérer que les attaquants pourraient être aussi intelligents et motivés que les défenseurs, voire davantage. Les parties les plus vulnérables d'un système sont souvent les cibles les plus probables. La sécurité peut être progressivement renforcée ou affaiblie par de petites actions et inactions.

La mise en place de mesures de cybersécurité est un processus itératif qui nécessite plusieurs cycles d'amélioration pour parvenir à une mise en œuvre solide et efficace. La sécurité absolue étant hors de portée, l'engagement continu envers la vigilance et l'amélioration demeure le meilleur moyen de protéger les systèmes et les données des menaces en constante évolution.

Pour être accompagné dans ce changement, les acteurs de l’industrie peuvent faire appel à des expertises extérieures comme des profils d’expert en cybersécurité.

CONTACTEZ-NOUS POUR EN SAVOIR PLUS

À PROPOS DE SERMA SAFETY AND SECURITY

SERMA Safety and Security accompagne ses clients pour la sécurité et la sûreté de fonctionnement des produits et systèmes dans les domaines de l'IoT, de l'embarqué, de l'industrie ou des systèmes d'information. L'entreprise bénéficie d'une expertise unique lui permettant d'intervenir sur toute la chaîne de valeur des systèmes : depuis les produits IoT en passant par l'infrastructure réseau et système jusqu'aux applications internes et externes.

SERMA Safety and Security est reconnue pour son excellence technique qui lui vaut d'avoir reçu de nombreuses qualifications et certifications dont CESTI, PASSI RGS, SESIP, FIPS, SBMP, ...

Parallèlement à ces activités, la société propose des formations sur l'ensemble de son périmètre de compétence en sûreté de fonctionnement et cybersécurité. Présente sur 8 sites en France, la société compte plus de 230 collaborateurs et réalise un chiffre d'affaires de plus de 35 millions d'euros. Elle est une filiale du Groupe SERMA.

www.serma-safety-security.com