The Positive Way

WAVESTONE

RETOURS D'EXPÉRIENCE ET BONNES PRATIQUES **POUR PROTÉGER ET MAINTENIR EN CONDITION DE SÉCURITÉ LES SI INDUSTRIELS**

AUTEURS

BENOIT BOUFFARD
benoit.bouffard@wavestone.com

ALI FAWAZ
ali.fawaz@wavestone.com

Depuis plusieurs années, nous accompagnons les changements profonds que vivent les Systèmes d'Information Industriels avec une ouverture à marche forcée et une utilisation de technologie des SI de Gestion de plus en plus fréquente. Le niveau d'exposition et de menace augmentant, il est crucial d'assurer aisément leur maintien en condition de sécurité en coordination avec le Métier.

Quels sont les retours terrain et les bonnes pratiques pour protéger et maintenir en condition de sécurité les SI industriels ?

L'ouverture au SI de gestion, une nécessité mais un vecteur de risques

Historiquement, le SI Industriel n'était pas interconnecté avec le SI de Gestion, par absence de besoin ou par recherche d'une limitation de son exposition. L'essentiel des actions se faisait localement, directement sur les équipements ou à distance avec des moyens spécifiques, avec une gouvernance et des opérations souvent elles-mêmes locales.

L'évolution des besoins Métier et l'optimisation des procédés de production ont fait émerger de nouveaux enjeux moins locaux (supervision à distance, télémaintenance, émergence de l'IoT[1], standardisation et rationalisation des technologies et des compétences, cyber menaces, etc.) dans le but d'accroitre la performance et le confort des opérations. Ces enjeux ont amené un besoin de numérisation et d'interconnexion entre les SI Industriels et les SI de Gestion.

Bien que nécessaires au bon fonctionnement des Métiers, nos échanges avec les opérationnels montrent bien que ces interconnexions ont eu pour conséquence de générer des **risques d'intrusion et de propagation entre ces systèmes d'information :**

- Sur **les opérations et la qualité** avec de potentiels arrêts ou altérations de lignes de production entraînant des impacts financiers, d'image voire humains ;
- Sur **la sécurité des installations** en cas de compromission grave d'outils de production pouvant avoir des impacts sur l'humain ou l'environnement.

La mitigation de ces risques d'intrusion et de propagation et de leur conséquence nécessite de mettre en place des activités et mesures de sécurité en différentes étapes :

1. La cartographie du SI Industriel ;
2. La mise en place d'une architecture réseau sécurisée ;
3. Le durcissement puis le maintien en conditions de sécurité des différents systèmes dans la durée ;
4. Enfin, la mise en place de moyens de détection d'incident et de réaction.

Les autorités se sont par ailleurs penchées sur le sujet et imposent ces mesures, et d'autres encore, sur les périmètres les plus sensibles.

Des interventions parfois distantes et potentiellement fréquentes (patch management, revue de compte, contrôle d'intégrité, etc.), d'équipes plus éloignées des opérations, peuvent alors être nécessaires et se heurter à un modèle opérationnel historique pensé pour privilégier la continuité et l'intégrité des opérations, la qualité, l'hygiène et la sûreté, tout en minimisant les disruptions.

Comment mettre en place ces mesures sans pour autant perdre de vue la finalité du SI industriel : faire fonctionner un procédé physique de façon nominale ?

1. IoT i.e. Internet of Things

1. La cartographie, un prérequis au traitement des risques de cybersécurité sur les SI Industriels

Afin d'évaluer les risques et maîtriser les impacts potentiels des mesures, la première action à mener est de **construire une cartographie SI** des installations industrielles permettant :

- De connaître les systèmes à administrer et à maintenir à jour ;
- D'identifier les utilisateurs (exploitants, mainteneurs, etc.) et donc les interlocuteurs à impliquer lorsqu'un changement est nécessaire, pour en maîtriser les impacts opérationnels ;
- D'évaluer les impacts potentiels de nouvelles vulnérabilités et failles de sécurité en matière de sûreté, d'opérations et de qualité.

Retour d'expérience

Notre retour d'expérience montre que la cartographie d'un SI peut être longue. Il s'agit alors, pour commencer, d'identifier les macro-systèmes de son SI industriel puis d'en prioriser la cartographie fine. Une **analyse de ces macro-systèmes** va ainsi permettre de **les ordonner dans différentes catégories** :

1. Les composants ayant un rôle de qualité ou de sûreté ;
2. Les systèmes de supervision et de maintenance de ces mêmes composants qualité / sûreté ;
3. Les autres systèmes industriels

La priorisation prend également en compte le niveau d'exposition (interconnexion, accès à distance, exposition sur internet) de ces systèmes.

Une fois que le processus de cartographie est lancé, il faut également formaliser la **procédure de mise à jour de cette même cartographie** en définissant une fréquence de mise à jour par degré de criticité puis s'atteler au traitement des risques.

Ce chantier conséquent va donc requérir **un dialogue et une collaboration étroite avec les automaticiens et les membres de l'ingénierie.**

Il est à noter que ce chantier de cartographie peut se révéler plus long et complexe que pour une cartographie habituellement effectuée par une DSI. En effet, les SI Industriels ne sont pas totalement comparables à un SI classique et plusieurs de leurs spécificités rendent leur cartographie difficile :

- Les équipements peuvent être isolés derrière des systèmes de filtrage bloquant leur découverte ou tout simplement éteints sur de longues périodes (cas d'un poste utilisé uniquement sur une production en batch annuel) ;
- La gouvernance autour de ces équipements a historiquement été portée localement sans forcément utiliser les mêmes normes et outils que ceux des DSI.

2. La mitigation des risques sur le SI Industriel par la mise en place d'une architecture de sécurité

La sécurité n'étant pas un sujet nouveau, il parait donc logique de vouloir suivre les principes d'architecture et de sécurité des SI de Gestion pour les SI Industriels tout en les adaptant à leurs spécificités :

- Réduire les risques de propagation et d'intrusion en assurant **un cloisonnement** du SI Industriel et en restreignant les accès ;
- Sécuriser l'administration du SI en mettant en place **une architecture d'administration dédiée** ;
- Équiper les administrateurs avec **les outils adéquats** pour intervenir sur l'ensemble du parc industriel ;
- Intégrer dès le départ, lorsque cela est possible, **l'intervention des mainteneurs externes.**

Ces quatre principes **sont les pierres angulaires de la sécurisation de l'architecture d'un SI Industriel.**

Le cloisonnement, le début de la réduction de l'exposition

Les SI de Gestion et Industriels n'ont, par essence, pas les mêmes buts : l'un sert à faire fonctionner une entreprise (messagerie, gestion, outils collaboratifs…) tandis que l'autre sert à opérer des procédés physiques. Théoriquement, ils devraient être cloisonnés et seuls certains flux autorisés. Cependant, le retour terrain montre que cela est rarement le cas.

Comme dans toute démarche de sécurisation d'un SI, il convient **d'adopter le principe de strict nécessaire** afin de limiter l'exposition aux cybermenaces. Les interconnexions entre la Gestion et l'Industriel ne doivent répondre qu'à des besoins spécifiques comme par exemple :

- L'envoi des ordres de productions aux SCADA[2] ;
- Le transfert des fichiers de FAO[3] aux machines à commandes numériques ;
- La remontée des données de productions pour garantir un pilotage des opérations.

Une bonne pratique courante consiste à mettre en place une DMZ[4] comprenant un filtrage des flux à l'aide d'un pare-feu mais aussi avec une solution de partage de fichiers qui correspond à un besoin Métier. Ce partage de fichier peut être sécurisé via la mise en place d'une analyse antivirale systématique des fichiers déposés avant de pouvoir être récupérés côté Industriel.

Le SI Industriel se doit également d'être cloisonné en son sein afin de réduire le risque de propagation. Pour ce faire, nous pouvons suivre le principe de zones et conduits tel que décrit dans la norme IEC 62443.

En pratique, nous pouvons **effectuer ce cloisonnement en plusieurs étapes :**

- Lister les fonctions Métier avec différents niveaux de sûreté ;
- Rassembler les fonctions de même niveau de forme de zones (avec potentiellement une zone « *legacy* » et ses sous-zones) ;
- Mettre en place les règles de sécurité par zone en fonction de leurs besoins tels que décrits dans la norme IEC 62443 ;
- Vérifier que les interconnexions (conduits) entre les différentes zones respectent les règles de sécurité ;
- Migrer les applications – la mise en conformité des applications peut être longue et difficile et il peut ici être opportun de procéder par analyse de risques pour prioriser et piloter, et de lister les non-conformités et les plans de remédiation associés. De même la migration elle-même peut être complexe pour s'assurer de ne pas impacter les opérations.

Ici une approche par étapes associée à des phases d'observation peut être pertinente :

- Avant la migration d'applications industrielles dans leurs zones cibles : pour vérifier qu'un changement d'adresse IP n'amène pas d'impact sur les opérations (IP codée en dur, IP configurée dans un actif donné…) ;
- Après la migration et avant l'activation des règles de filtrage, là encore pour vérifier que le filtrage lui-même n'amènera pas d'impact sur les opérations.

2. SCADA i.e. Supervisory Control And Data Acquisition ou système de contrôle et d'acquisition de données.
3. FAO i.e. Fabrication Assistée par Ordinateur.
4. DMZ i.e. *Demilitarized Zone*.

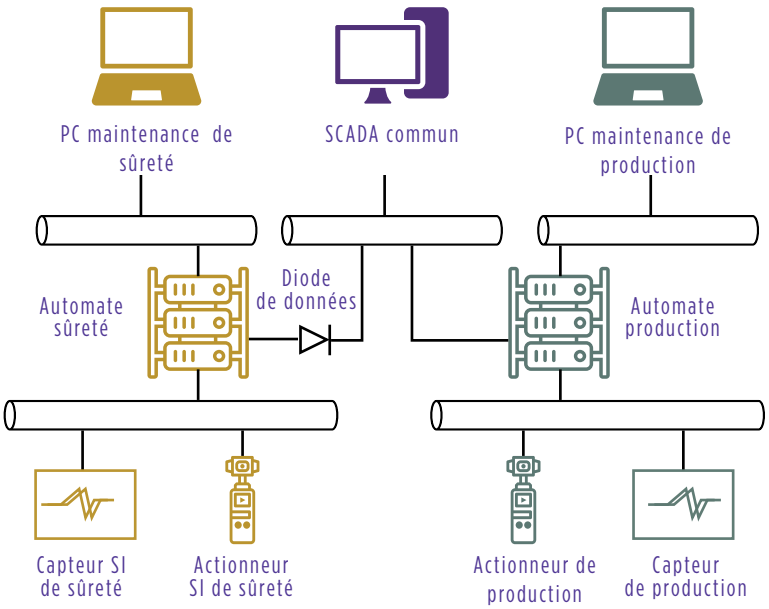
La particularité des SI de sûreté

Les SI de sûreté sont les SI industriels permettant de mettre en condition de sûreté les systèmes industriels de production. Ils ont longtemps été mécaniques, puis pneumatiques, électriques avant d'être numérisés. On comprend donc l'importance d'en assurer spécifiquement l'intégrité. Un dernier chantier de cloisonnement peut donc être envisagé pour le permettre. Cependant, il est souvent observé sur le terrain que l'existant peut être un frein et donc rendre ce chantier complexe. Lorsqu'elle est réalisée de manière stricte, la séparation permet de réduire les risques de propagation, d'avoir des niveaux de sécurité distincts entre SI de production et SI de sûreté en fonction de leurs niveaux de risques. Elle a par contre l'inconvénient de nécessiter un système SCADA dédié et est donc coûteuse et non ergonomique pour les opérations.

Bonne pratique

Une séparation laissant de la place à un SCADA commun permet d'assurer l'ergonomie du SI Industriel tout en réduisant les risques de propagation du SI de production vers le SI de sûreté par l'installation d'une diode.

Schéma de cloisonnement SI Industriel / SI de Sûreté (SIS)



L'administration, point névralgique de l'architecture réseau

L'administration d'un SI est essentielle pour garantir sa disponibilité et sa sécurité. **Dans un programme de sécurisation d'un SI, il convient de prendre en compte les objectifs que l'on souhaite atteindre** afin d'obtenir le modèle le plus adapté. Dans notre cas, les bonnes pratiques que nous observons sur le terrain consistent à :

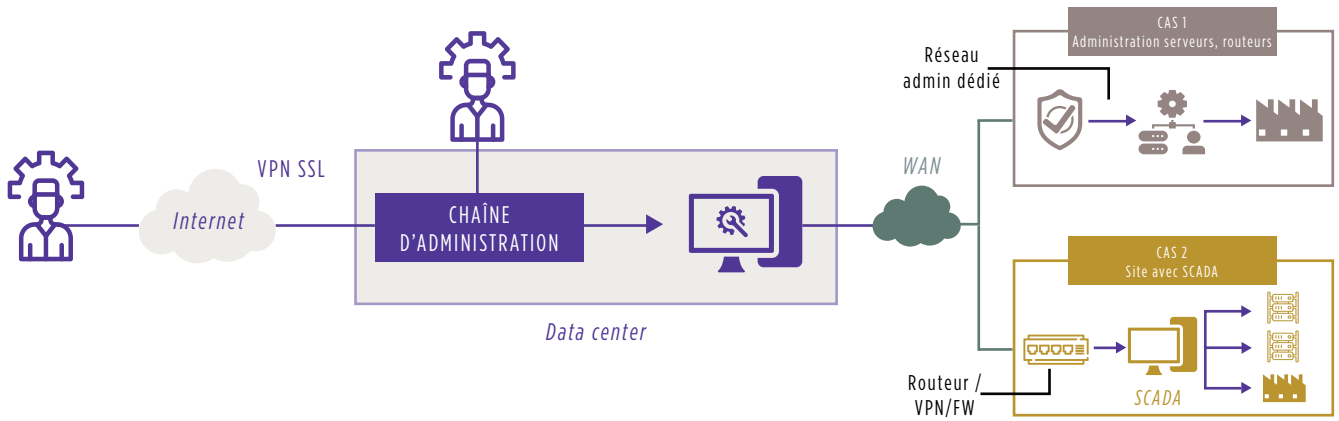
- **Créer un réseau d'administration isolé du réseau de production et étendu à la fois en central et localement** pour protéger les flux d'administration afin d'éviter des pertes d'intégrité sur des flux de pilotage d'opérations sensibles ;
- **Protéger les équipements d'administration** pour éviter une prise de contrôle directe de ces éléments critiques par un attaquant ;
- **Homogénéiser au maximum les pratiques et standardiser les équipements** afin de faciliter les déploiements d'une architecture d'administration sécurisée voire centralisée, et le maintien dans le temps du niveau de sécurité – cela pouvant se faire en mutualisant les ressources dans une équipe centrale et dédiée.

Attention, nous ne traitons ici que l'administration de l'infrastructure des SI Industriels. L'administration des automates, par exemple, est faite par le Métier pour ce qui est de la configuration et passera par le poste de configuration et de maintenance dédié, en cas de besoin de mise à jour.

La première étape consiste à créer la structure du réseau d'administration isolé et étendu. Cet objectif peut être atteint au travers des mesures suivantes :

- Dans une optique d'optimisation et de mutualisation des ressources, **le réseau d'administration est construit autour d'un ou plusieurs datacenters**, notamment pour assurer le DRP[5].
- Afin de réduire le risque de propagation par rebond depuis un site infecté, le réseau WAN[6] mis en place entre le datacenter et les sites industriels peut être configuré en ***hub and spoke***[7] pour assurer une isolation entre chaque site.
- Pour pouvoir garantir l'intégrité et la confidentialité des flux d'administration, ceux-ci doivent être isolés au sein d'une **VRF[8] spécifique** ou d'un réseau **VPN[9] d'administration** entre le datacenter et chaque site. La mise en place de ce réseau dédié à l'administration se fait notamment par l'utilisation d'équipements télécom, de sécurité et d'interfaces dédiées sur les serveurs.
- Pour les sites les plus importants, le risque d'intrusion depuis le LAN[10] utilisateur peut être réduit par la mise en place d'un **LAN d'administration accessible uniquement depuis le LAN d'administration du datacenter**. Une telle architecture doit cependant prévoir **une solution de résilience** dans le cas où le WAN venait à être coupé pour permettre aux sites d'y accéder directement mais aussi pour les équipements qui ne sont tout simplement pas maintenables à distance.
- Les entreprises ayant de nombreux sites peuvent également utiliser **un boitier standardisé** embarquant toutes les fonctions de sécurité nécessaires à l'interconnexion d'un site. Cela facilite en effet la configuration et le maintien en conditions de sécurité.

Schéma d'interconnexion d'un site standard ou avec SCADA



5. *Disaster Recovery Plan* i.e. Plan de Reprise d'Activité.
6. WAN i.e *Wide Area Network*.
7. Réseau *Hub and Spoke* i.e. Réseau en étoile autour du data center.
8. *Virtual Routing and Forwarding* i.e. un plan de routage virtuel.
9. VPN i.e. *Virtual Private Network*.
10. LAN i.e. *Local Area Network*.

La deuxième étape consiste à brancher les équipements d'administration et les équipements à administrer sur ce réseau en les protégeant d'une compromission.

Lorsqu'elle est réalisée de manière stricte, la séparation permet de réduire les risques de propagation, d'avoir des niveaux de sécurité distincts entre SI de production et SI de sûreté en fonction de leurs niveaux de risques. Elle a cependant l'inconvénient de nécessiter un système SCADA dédié et est donc coûteuse et non ergonomique pour les opérations.

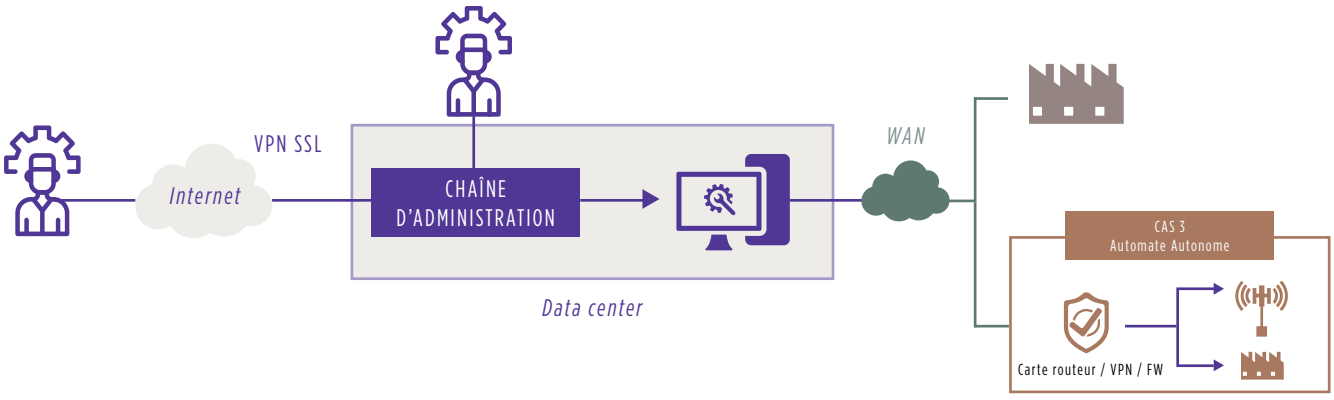
Pour les sites constitués d'un seul équipement, les fonctions de filtrage et de terminaison VPN peuvent être assurées par une **carte routeur** parfois directement ajoutée à l'automate.

Les **équipements non maîtrisés**, du fait de leurs contraintes industrielles, doivent être isolés dans des **VLAN[11] spécifiques** dont l'accès est filtré par un pare-feu pour permettre des actions d'administration à distance si nécessaire.

Il arrive également d'avoir **une partie du SI complètement déconnectée pour des raisons diverses**. Ce SI étant déconnecté, il ne présente pas de risques SSI mais uniquement un risque métier. Son état déconnecté abaisse cependant son niveau d'exposition et de ce fait le risque d'intrusion. Il est opportun de réaliser une analyse de risques pour décider de la façon de procéder. Les moyens seront alors adaptés en allant d'une simple procédure d'administration locale jusqu'à la mise en place d'une infrastructure d'administration dédiée, celle-ci pouvant se révéler coûteuse.

Ces différentes briques réseau permettent ainsi aux administrateurs centraux d'accéder aux équipements. Il faut cependant leur donner accès aux outils nécessaires.

Schéma d'interconnexion d'un site autonome



11. VLAN i.e Virtual Local Area Network, ou Virtual LAN

L'outillage des administrateurs : comment prévoir leurs besoins tout en garantissant la sécurité ?

La gestion des SI de Gestion et Industriel étant généralement distincte, **l'outillage mis en œuvre est dédié**, bien qu'il puisse s'appuyer sur des produits identiques. La mise en place de cet outillage va permettre de répondre à plusieurs objectifs :

- **Assurer le contrôle d'accès** sur les interfaces d'administration pour réduire la probabilité d'obtention de capacités d'attaque et d'utilisation frauduleuse des outils ;
- **Tracer les actions des administrateurs** pour réduire les impacts potentiels d'une attaque en se créant des moyens de détection et réaction et en assurant la facilité d'investigation a posteriori.

Cela se traduit par la mise en œuvre d'une chaîne d'administration.

La diversité des équipements d'un SI Industriel peut cependant nécessiter des clients lourds spécifiques ou des protocoles non supportés par le bastion pour leur administration. Afin de limiter le risque d'infection lié à la connexion de machines non maîtrisées sur le SI, un poste d'administration dédié sur lequel sont installés ces outils peut être mis en œuvre. L'accès à ce poste peut se faire depuis le bastion en RDP[14] par exemple. Les flux utilisant des protocoles obsolètes devront quant à eux être encapsulés dans un tunnel VPN IPSEC[14] pour atteindre leurs cibles.

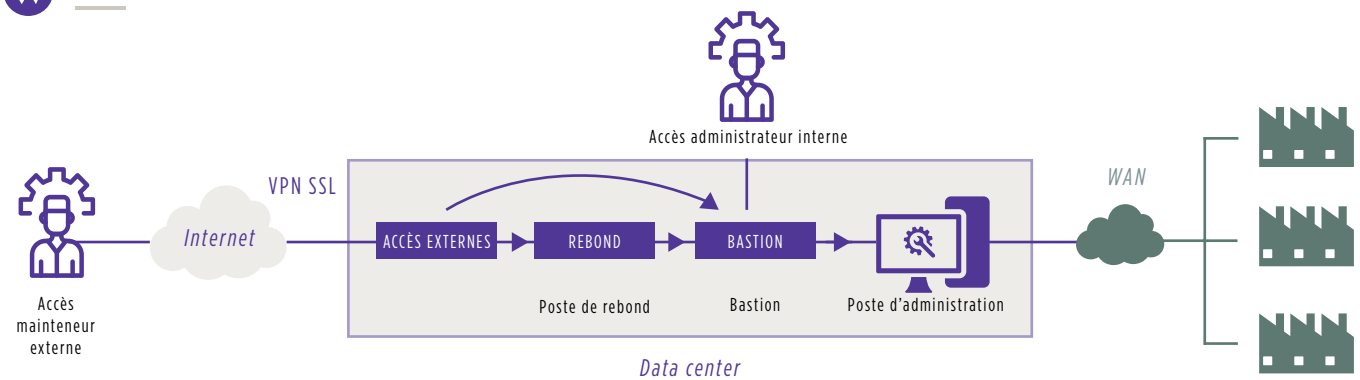
Afin de centraliser les accès et de maintenir un contrôle fin sur les autorisations, **un bastion d'administration** doit être mis en place. Les comptes génériques sont joués par le bastion et protégés dans son coffre-fort numérique. Le bastion assure également la traçabilité des actions et diminue le risque de vol de comptes à privilèges génériques. Le bastion peut également sécuriser les flux d'administration en réalisant de la translation de protocole (Telnet[12] vers SSH[13] par exemple).

Pour les équipements ayant un niveau de maturité sécurité suffisant (gestion fine des droits, traçabilité, comptes nominatifs), il peut être envisagé d'assurer leur administration directement sans passer par un bastion (ce peut notamment être le cas pour des équipements télécom).

La mise en place d'un poste d'administration dédié, où seront installés les outils nécessaires au Métier, nécessite la mise en place d'un processus d'installation de ces outils afin de maintenir le niveau de sécurité de ce poste mais aussi de connaître la liste des outils déployés sur le SI.

Que l'administration soit réalisée au travers d'un bastion standardisé ou d'un poste d'administration dédié, la résilience de la solution doit être assurée.

Schéma de principe de la chaîne d'administration



12. Telnet i.e Terminal Network, Telecommunication Network, ou encore Teletype Network
13. SSH i.e Secure Shell
14. RDP i.e Remote Desktop Protocol

La prise en compte des mainteneurs externes

Enfin, **il est primordial de sécuriser l'accès des tiers mainteneurs** afin de limiter les risques provenant d'accès abusifs ou non cadrés (infection du SI après installation d'un outil non validé, perte de donnée liée à un tiers malicieux, indisponibilité des équipements…).

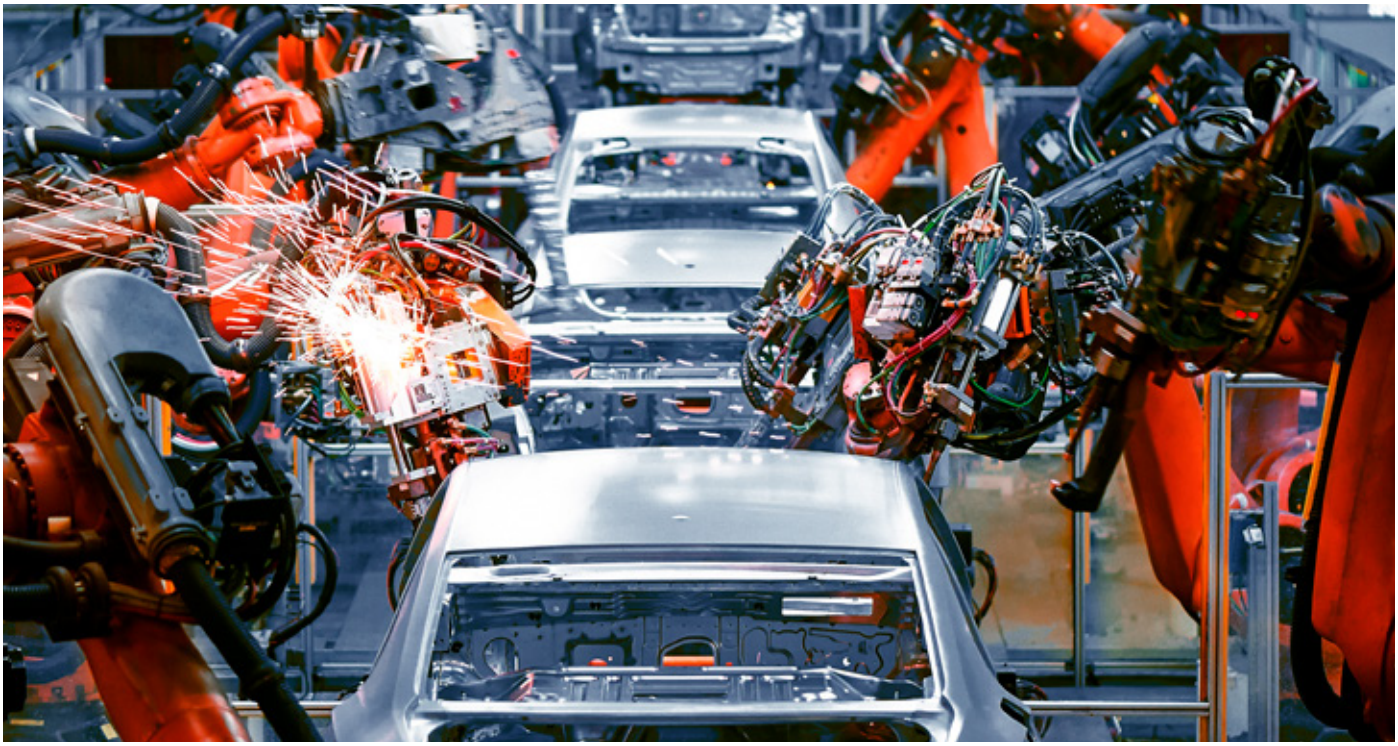
La mise en œuvre **d'un point d'accès externe** avec **une authentification forte** est nécessaire afin de garantir l'identité des utilisateurs. Ce point d'accès permet aux mainteneurs d'accéder à un poste de rebond maîtrisé et durci par le client tout en assurant la traçabilité des actions. Sur ce point, les clients les plus avancés mettent en œuvre des solutions permettant de ne donner accès au SI que durant la durée de l'intervention et cela uniquement après validation interne.

Il faut cependant noter que l'accès à distance n'est pas conforme avec les exigences de la LPM[15] qui imposent d'avoir un poste durci dédié pour l'administration et isolé d'Internet (également nécessaire pour une administration depuis l'interne).

Les **postes de configuration et de maintenance**, dédiés au site et aux automates, doivent quant à eux faire l'objet d'un suivi particulier pour être mis à jour et rester en conditions de sécurité, notamment pour ce qui est des outils déployés.

Il peut toutefois arriver qu'un fournisseur refuse de passer par des postes de maintenance locaux dédiés, ou des rebonds avec accès distant sécurisé, pour diverses raisons. Il conviendra alors d'identifier des solutions permettant d'allier la sécurité du SI Industriel, les besoins du Métier et les contraintes des fournisseurs.

Pour aller plus loin, on peut s'intéresser au Groupe de Travail de l'ANSSI[16] sur la Cybersécurité des Systèmes Industriels et à son **référentiel PIMSEC**[17] qui recommande un certain nombre d'exigences de sécurité à appliquer contractuellement à ses prestataires intervenants sur le SI Industriel.



15. Loi de Programmation Militaire servant à identifier et sécuriser les organisations et les SI d'importance vitale.
16. ANSSI i.e. Agence Nationale de la Sécurité des Systèmes d'Information.
17. PIMSEC i.e. Référentiel d'exigences de sécurité pour les prestataires d'intégration et de maintenance de Systèmes Industriels.

3. La couverture des risques dans la durée

Le durcissement des équipements

En complément d'une architecture et d'un outillage d'administration sécurisés, il convient d'élever le niveau de sécurité de chaque équipement en appliquant un principe de strict nécessaire. Un guide de **durcissement** générique peut être créé et adapté à chaque technologie identifiée lors de la cartographie du SI Industriel. Celui-ci permet de remédier à une partie des vulnérabilités présentes au niveau des configurations et des systèmes.

L'utilisation de solutions complémentaires peut également apporter un surplus de sécurité :

- Les **antivirus** connectés au réseau ou non (impliquant une mise à jour manuelle) vont couvrir les postes industriels contre les virus les plus communs ;
- La mise en place de règles strictes sur les **pare-feux locaux** des machines va empêcher les communications, et donc intrusions, sur les ports inutilisés, et filtrer l'origine des flux en fonction des protocoles utilisés, permettant de mieux détecter des tentatives d'attaques ;
- **Des solutions de gestion des comptes administrateurs locaux** (par exemple LAPS pour Windows) peuvent enfin permettre de gérer les comptes administrateur natifs des postes de manière centralisée et individualisée.

Il arrive cependant qu'il ne soit plus possible de durcir un équipement du fait de sa vétusté, il faut alors travailler avec le Métier sur **la gestion de l'obsolescence** des équipements, sur leur éventuel remplacement et en dernier recours sur les capacités à les isoler du reste du SI. **Des bloqueurs de configuration** pourront également permettre, sur des postes vétustes, de restreindre l'installation et l'utilisation de composants à ceux uniquement nécessaires.

Il est important de rappeler que le SI Industriel souffre de certaines vulnérabilités, mais est avant tout l'outil de production du Métier. Le dialogue avec ces équipes est donc primordial à la compréhension de l'utilisation qu'ils en font afin de résoudre ces vulnérabilités en limitant les conséquences au maximum pour le métier.

Le maintien en condition de sécurité

Lorsque les équipements atteignent le bon niveau de sécurité, il faut prévoir son maintien dans le temps. **Différents scénarios de gestion des correctifs de sécurité ou « patchs »** peuvent être définis pour répondre également aux besoins du Métier (disponibilité, intégrité) et synchronisés avec la maintenance industrielle :

1. **Intégration dans les processus nominaux d'exploitation** (par exemple : les processus de qualification / qualité d'une installation peuvent imposer que les équipements soient à jour). La mise à jour et l'administration des équipements tireront ainsi profit des arrêts industriels d'autant plus si une re-certification est nécessaire.
2. Préparation d'un **processus de mise à jour « à chaud »** en cas de faille de sécurité critique et d'un processus d'isolation préventif d'une ligne de production le temps que le procédé puisse être interrompu ;
3. **Identification des équipements redondants** ou périphériques sur lesquels une intervention avec simple information des responsables de sites est possible.

Plusieurs points durs peuvent être rencontrés ici :

Le processus standard qualité doit idéalement :

- Prévoir que les projets délivrent les procédures de maintien en condition de sécurité avant la mise en production, tout comme les politiques de sécurité ;
- Être aligné avec les équipes sécurité sur l'évaluation de l'impact en intégrité d'un changement liés à des opérations de maintien en condition de sécurité ;

Le marché est hétérogène sur ces points :

- Dans les structures les moins matures, patcher les systèmes est encore optionnel dans le processus de qualité et les projets ne délivrent pas encore les procédures de maintien en condition de sécurité de manière standard ;
- Dans d'autres, plus matures, une procédure opérationnelle standard de la qualité prévoit qu'un patch de cybersécurité doit être appliqué conformément à sa procédure d'application (délivrée par un projet) et qu'il n'altère pas l'intégrité de fonctionnement des systèmes industriels ni leur éventuelle certification.

Enfin, pour aller plus loin, quelques astuces peuvent permettre de réduire les impacts potentiels des mises à jour :

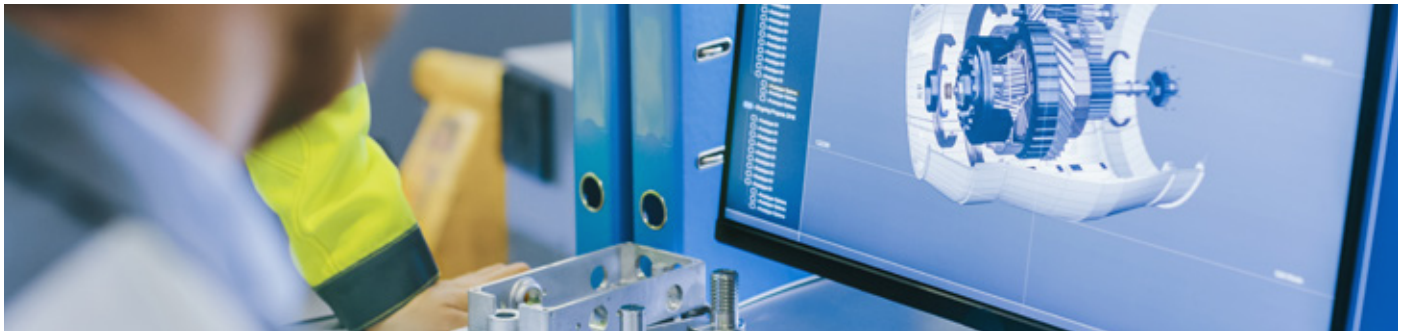
- L'identification des éléments d'architecture d'un système industriel nécessaires aux opérations ou aux fonctions de support des opérations peut permettre de définir des éléments d'architecture permettant de réduire les pertes de disponibilité ou de données lors d'opérations de patch (haute disponibilité, cold spare, redondance des données / traces à chaud, mise en tampon temporaire des données et traces, backup hors ligne…) ;
- L'installation silencieuse de patchs sur les couches basses des systèmes, associée à des redémarrages des chaines de production entre deux batchs, lorsque cela est possible, permet de réduire autant que possible le temps de l'opération de patch sur le temps de maintenance effectivement disponible (uniquement le temps de redémarrage compte) ;
- La création d'une infrastructure de sauvegarde régulière (à chaque redémarrage) peut faciliter les rollbacks en cas de problème.

Afin de mettre en place ces process de patch, la cartographie réalisée précédemment doit faire apparaître **un inventaire précis des équipements** devant inclure :

/ L'identification des équipements, leur type, localisation et nombre ;
/ Les procédés industriels pour lesquels ils sont utilisés et la criticité associée ;
/ La version du système d'exploitation et/ou firmware, les outils et la configuration déployés dessus ;
/ Les besoins en termes de cybersécurité au regard des procédés supportés ;
/ La disponibilité de redondance, de mise en tampon des données et de cold spare ;
/ La fréquence de patch requise et l'historique de patch.

Le maintien du niveau de sécurité ne se base pas uniquement sur l'application de correctifs de sécurité sur les équipements. Il convient également de :

/ Définir le processus de mise à jour des **solutions de sécurité installées** sur les équipements coupés du réseau ;
/ Installer des **solutions de nettoyage de média amovibles** qui restent très présents sur les sites industriels – certains produits ont l'avantage d'être portables et donc d'analyser le média pendant le déplacement à l'intérieur du site industriel ;
/ Assurer la **sauvegarde des configurations** des équipements et leurs **intégrations au DRP** afin de garantir une remise en route post-incident qui réponde aux besoins de disponibilité ;
/ Mettre en place un **suivi de l'IAM[18] industriel** afin d'avoir un contrôle d'accès physique et logique robuste. Cette action permettra aussi d'automatiser de nombreuses actions fastidieuses de revue de comptes parfois encore faites à la main.



18. IAM i.e. *Identity and Access Management.*

4. La détection des incidents de cyber sécurité

Les mesures citées précédemment permettent de réduire la probabilité d'occurrence des risques et donc d'augmenter la disponibilité des équipements pour le Métier. Il faut néanmoins se préparer au pire et avoir les outils nécessaires à **la détection d'un incident** pour le remédier au plus vite et garantir un temps d'interruption réduit au maximum.

La mise en place de la détection

La première étape à réaliser est l'activation des fonctions IDPS[19] sur les équipements réseau afin d'assurer **un premier stade de détection et potentiellement de blocage automatique.**

Il s'agit ensuite d'assurer **la collecte d'informations** en déployant un concentrateur sur site. Les logs des équipement réseau et serveurs pourront ainsi être envoyés aux SIEM[20] existants ou dédiés dans lesquels se feront **corrélation et détection**. Les SOC[21] et CERT[22] peuvent alors réaliser les opérations d'analyse, détection et éventuellement de réaction sur incident en se basant sur des scénarios classiques.

Il est à noter que l'envoi de logs peut être consommateur de ressources en termes de bande passante, un filtrage peut être réalisé directement au niveau du concentrateur pour n'envoyer que les informations pertinentes aux SIEM.

L'anticipation de risques spécifiques

Cependant, la détection basée sur des scénarios classiques n'apportera que peu de valeur aux métiers. La prise en compte de l'ensemble des sources (PC, Linux, UNIX…) et la mise en place de sondes dédiées aux SI Industriels capables de s'interfacer avec des systèmes SCADA peut permettre d'améliorer le système de détection. Toutefois, ces solutions peuvent s'avérer coûteuses.

L'élément clé consistera ici à assurer une montée en maturité et en valeur incrémentale et rapide du SOC. L'utilisation des méthodes Agile est donc tout indiquée, en itérant sur le cycle décrit dans l'encart suivant.

Se préparer à la remédiation

Pour finir, la détection d'un incident ne pourra aboutir à une remédiation efficace que si le Métier est inclus. Tout comme pour les mises à jour d'équipements, il convient donc de revoir les **procédures d'arrêt d'urgence** avec les utilisateurs du SI Industriel. La formalisation d'un **Plan de Réponse à Incident** permet de planifier les actions à mener en cas d'incident cyber-industriel.

Des **exercices de gestion de crise dédiés au SI Industriel** doivent également être menés pour assurer une préparation optimale des équipes et mettre en lumière les éventuels manques.

L'utilisation des méthodes Agile pour la mise en place d'un SOC Industriel est tout indiquée, en itérant sur le cycle suivant :

- Identification d'un événement redouté avec le métier ;
- Analyse de l'architecture du SI Industriel et identification des actifs concernés ;
- Collecte des données permettant de détecter cet événement ;

Les retours terrain montrent que les SOC s'appuient souvent sur des données issues de flux ou d'équipements de sécurité (pare-feu, sondes…). Or on constate que les sources de données « industrielles », encore trop peu exploitées, sont parfois facilement accessibles et peuvent constituer un apport important et complémentaire aux données issues des flux.

- Implémentation du scénario de détection.

19. IDPS i.e. *Intrusion Detection and Prevention Systems.*
20. SIEM i.e. *Security Incident and Event Management.*
21. SOC i.e. *Security Operation Cente.*
22. CERT i.e. *Computer Emergency Response Team.*

5. Une approche progressive et participative garantira le succès de la démarche

La mise en condition de sécurité d'un SI Industriel est un chantier complexe qui ne peut être fait qu'avec le Métier. Il convient donc de travailler avec lui de manière progressive et participative sur chacun des chantiers suivants :

/ **Prendre connaissance de son SI Industriel** en réalisant une cartographie en priorisant les éléments les plus critiques ;

/ **Mitiger les risques sur le SI Industriel** en mettant en place l'état de l'art de l'architecture réseau sécurisée et définir les processus d'administration – les SI de Sûreté, par leur criticité, devront faire l'objet d'une attention particulière ;

/ **Atteindre un niveau de sécurité adéquat** par le durcissement et le maintien en condition de sécurité des équipements dans le temps – des discussions pourront notamment avoir lieu avec les fournisseurs et constructeurs d'équipements ;

/ **Mettre en place les outils nécessaires à la détection d'incident de sécurité**, qui peuvent avoir une influence sur la production, et définir les processus de réaction.

Toutes ces actions ne peuvent pas toujours être menées en parallèle. **La définition d'une feuille de route claire** va permettre la priorisation des différentes actions pour pouvoir maitriser les coûts et maximiser l'apport pour le Métier.

Si ce vaste chantier est souvent initialisé en central, l'enjeu reste de pouvoir embarquer les sites, parfois répartis dans le monde entier, pour assurer une sécurité pérenne dans le temps. Nous observons, en général, une démarche en deux temps :

1. **Un programme cybersécurité pluriannuel** (souvent 3 ans) pour un budget de 10 à 15 millions d'euros visant à :
   - Réaliser l'inventaire des SI Industriels ;
   - Élever le niveau de sécurité du parc existant par la mise en place de protections souvent périmétriques et de filtrage ainsi que la remédiation des vulnérabilités les plus critiques – la définition de procédures est ici nécessaire ;
   - Faire émerger un premier réseau de coordinateurs cybersécurité locaux ;
2. La création d'**une filière cybersécurité industrielle** et de **la gouvernance associée** réunissant :
   - Le cadrage des activités clés à piloter par les acteurs locaux ;
   - La construction participative d'outils pour aider ce réseau de responsable locaux à opérer les activités de cybersécurité sur le contenu ;
   - La construction des moyens de pilotage de la montée en maturité et de gestion du changement (matrices de maturité, outils de modélisation budgétaire par site, définition d'indicateurs de pilotage, services centraux consommables par les sites…).

La mise en place de la gouvernance peut démarrer après le programme et tirer ainsi profit du premier réseau de correspondant sensibilisé à la cybersécurité bâti par le programme.

Une fois construite, il s'agit ensuite de l'animer et de piloter la progression des sites et des systèmes industriels à la fois en termes de niveau de sécurité et de niveau de maturité.

Cette animation réunit en général :

/ Un réseau responsables cybersécurité locaux de 0,5 à 2 ETP[23] par site en charge de réaliser les projets, d'implémenter les activités récurrentes de cybersécurité, d'améliorer continuellement la sécurité et de reporter ;

/ Une équipe centrale de 3 à 10 ETP pilotant globalement et appuyant les responsables locaux notamment en termes d'expertise.

23. Ces chiffres peuvent varier significativement en fonction de la taille de l'entreprise et du nombre de sites locaux, il s'agit d'une moyenne observée dans de grandes organisations internationales que Wavestone accompagne

The Positive Way

WAVESTONE

Dans un monde où savoir se transformer est la clé du succès, Wavestone s'est donné pour mission d'éclairer et guider les grandes entreprises et organisations dans leurs transformations les plus critiques avec l'ambition de les rendre positives pour toutes les parties prenantes. C'est ce que nous appelons « The Positive Way ».

Wavestone rassemble plus de 3 000 collaborateurs dans 8 pays. Il figure parmi les leaders indépendants du conseil en Europe, et constitue le 1er cabinet de conseil indépendant en France.

Wavestone est coté sur Euronext à Paris et labellisé Great Place To Work®.