Les systèmes industriels face à la question cyber

Un état des lieux de la cybersécurité industrielle

Vincent Nicaise
Industrial Partnership and Ecosystem Manager (Stormshield)

Si les systèmes industriels ont connu des jours heureux à l'abri des cyber-attaquants, cela fait maintenant plus d'une dizaine d'années qu'ils sont la cible régulière d'offensives cyber. Pour appréhender au mieux la fragilité de ces systèmes, cet article fait un état des lieux de la cybersécurité industrielle.

Des systèmes industriels au cœur de notre quotidien

Les systèmes industriels font référence aux systèmes informatisés qui réalisent de manière automatique des traitements, à partir d'informations collectées par des capteurs, ayant pour effet des actions sur des organes physiques. Souvent invisibles, ces systèmes sont pourtant omniprésents dans notre quotidien. On résume ces systèmes d'information industriels en « réseaux OT » pour « *Operationnal Technology* », par opposition aux réseaux IT pour « *Information Technology* », plutôt destinés à la bureautique et à la gestion commerciale et financière de l'entreprise. Ces réseaux OT ont été conçus pour durer de 10 à 40 ans et souvent mis en œuvre bien avant que l'on considère les risques de cyberattaque pour ces systèmes. La plupart n'intègre donc aucun concept d'architecture sécurisée, aucun mécanisme de protection, ni même une organisation prenant compte ces risques.

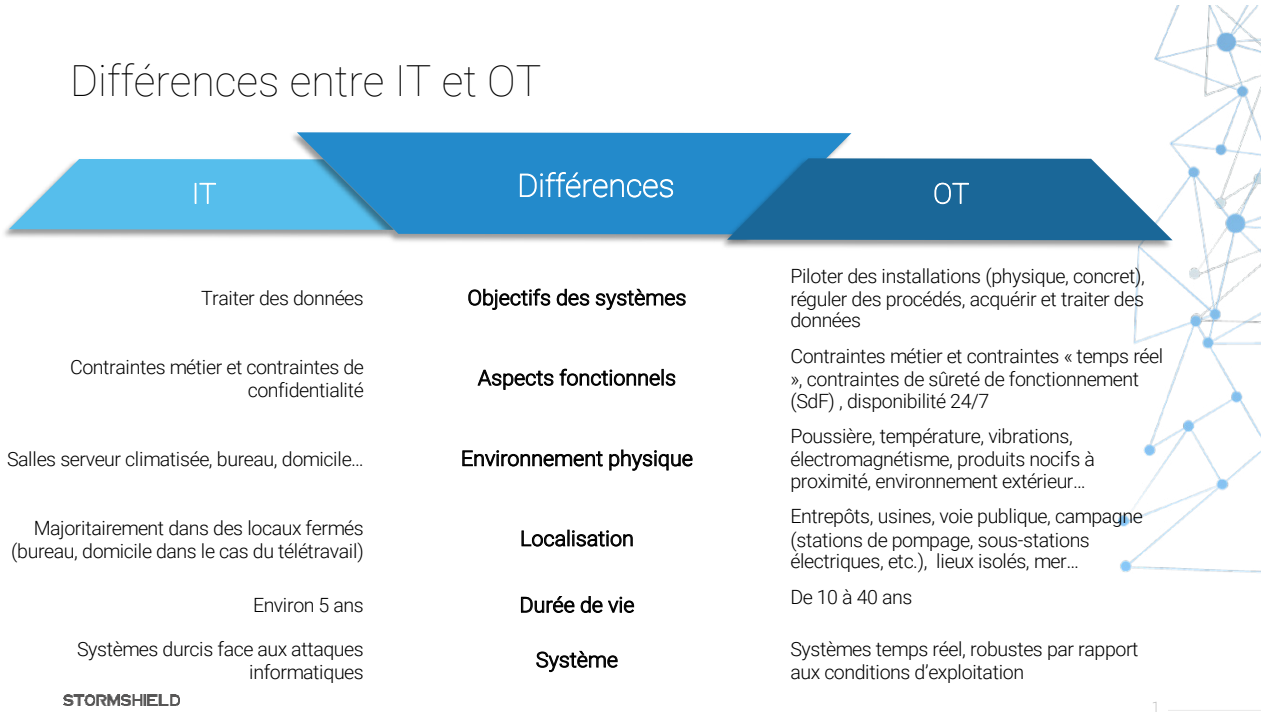

Figure 1 : Différences entre réseaux IT et OT.

Pourtant, les systèmes industriels sont au cœur des domaines sensibles de l'énergie, de l'eau, du transport, de la ville connectée ou encore de l'industrie. Ils pilotent des processus critiques qui, s'ils sont atteints, peuvent avoir un impact fort sur le tissu économique, l'écologie et même la nation. Et le risque s'amplifie fortement avec le développement des technologies du numérique.

La volonté d'optimiser la productivité de ces systèmes, notamment par l'interconnexion avec d'autres systèmes d'information comme les réseaux IT ou encore Internet mais aussi le déploiement d'objets connectés, a pour effet une augmentation de la surface d'attaque et donc un besoin accru en termes de cybersécurité.

Une cybersécurité spécifique aux systèmes industriels

La cybersécurité appliquée aux systèmes industriels doit prendre en compte leurs spécificités techniques et organisationnelles. En effet, il n'est pas question de dupliquer les bonnes pratiques de l'IT sans l'adapter à un contexte industriel et opérationnel, souvent complètement différent. Pour cela, il est important de bien comprendre ces différences et d'en tenir compte lors de la définition de la politique de sécurité (figure 1).

Des spécificités techniques

La conception, l'intégration et la maintenance d'une installation industrielle est bien souvent très coûteuse. Pour rentabiliser cette investissement, l'exploitation est prévue sur plusieurs dizaines d'années. Cette longue durée de vie implique notamment des difficultés à devoir maintenir les composants du système qui, à terme, deviennent obsolètes. En effet, si aujourd'hui les fabricants d'automates travaillent à ajouter des fonctions de sécurité essentielles ainsi qu'à intégrer la cybersécurité dans les cycles de développement logiciel, le fameux « *cybersecurity-by-design* », il n'en demeure pas moins que les installations dites « *legacy* » doivent faire avec des produits pas ou peu cyber-sécurisés. S'ajoute à cette faiblesse fonctionnelle, la difficulté à patcher ces équipements pour des raisons de continuité opérationnelle. En effet, pour des systèmes dont la disponibilité et la continuité de service est l'objectif essentiel, mettre hors service un automate dans le cadre d'une mise à jour logicielle face à une nouvelle vulnérabilité n'est pas une opération facile. Dans certains cas, la conduite du process s'effectue en 24/7 et la fenêtre de maintenance planifiée, organisée et réduite à son essentiel.

Cette difficulté d'intervention est aussi valable pour tout chantier de sécurisation du système, de modification d'architecture ou d'intégration de produits et logiciels de cybersécurité. Et cela, notamment car la localisation des systèmes industriels rend impossible le déploiement de solutions de cybersécurité tel qu'elles sont mises en oeuvre dans les réseaux IT. Il faut s'adapter au contexte industriel et par exemple prévoir des équipements de cybersécurité durcis avec diverses capacités de connectivité et une adaptabilité à la source d'alimentation.

En ce qui concerne les flux de communications, les systèmes industriels utilisent des protocoles propres aux marques d'automates, au contexte opérationnel ou encore aux types de processus. Ainsi, le protocole BACnet sera par exemple privilégié dans un contexte de gestion technique de bâtiment, l'IEC-61850 dans le domaine de l'énergie et

le S7 pour l'utilisation d'automates Siemens. Tous ces protocoles ont été conçus il y a déjà plusieurs dizaines d'années, et ne prévoient donc pas de mécanismes de sécurité.

Certains protocoles quant à eux tentent à évoluer vers plus de sécurité : OPC UA, annoncé comme le protocole de l'industrie 4.0 et des nouveaux usages industriels, intègre par exemple une sécurisation des communications via des certificats. Mais cette évolution est encore fragile ; dans les faits, le déploiement et la gestion du cycle de vie de ces certificats sont rarement mis en œuvre parce que trop contraignants à gérer dans le temps.

Car le temps est bien au cœur des enjeux de l'industrie 4.0, où les automates se basent sur des systèmes temps réel et où la maîtrise des temps de cycle et de réponse s'avère primordiale. Alors que les échanges inter-automates sont de l'ordre de quelques octets et sont séquencés à la milliseconde, la latence n'est pas acceptable à ce niveau sous peine d'impacter le processus. Cette exigence de quasi instantanéité nécessite la mise en œuvre de mécanismes de cybersécurité performants et ultra-fiables qui garantissent de ne pas perturber les échanges et qui doivent être également capables de comprendre les protocoles et de détecter les échanges illégitimes dans les communications.

Des spécificités organisationnelles

Pour de nombreux systèmes industriels qui pilotent des systèmes critiques, il existe une réglementation stricte. Cette réglementation permet notamment de s'assurer de la sécurité fonctionnelle ainsi que des intervenants et des utilisateurs. On retrouve par exemple : la directive machine pour les OEM, le standard FDA pour les secteurs de l'agroalimentaire et de l'industrie pharmaceutique, ou encore les standards de l'AIEA et les normes IEC pour le secteur nucléaire. Les étapes de mise en conformité sont souvent fastidieuses, complexes et coûteuses. Modifier les procédures et les architectures ou ajouter des équipements demande forcément de repasser les étapes de certification. Il peut donc être très contraignant et coûteux de cybersécuriser un système déjà certifié. Pour les nouveaux projets, il est essentiel d'intégrer la cybersécurité dès les phases d'avant-projet pour s'assurer de sa bonne prise en compte.

"Sujet particulièrement complexe, la cybersécurité industrielle peut toutefois s'appuyer sur de nombreux référentiels, publiés par différents acteurs du domaine (agences gouvernementales et européennes, organismes de normalisation, associations professionnelles…). "

Pour ce qui concerne l'organisation des intervenants et utilisateurs des systèmes industriels, ils sont particulièrement nombreux. Ils peuvent être internes à l'entreprise (exploitant, opérateur, mainteneur…) mais aussi (et très souvent) externes à celle-ci (fournisseur d'équipements industriels, intégrateur…). Il faudra alors appréhender les rôles de chacun et en tenir compte dans l'organisation de la cybersécurité à mettre en œuvre.

Par ailleurs, les exploitants de systèmes industriels font appel à de nombreux prestataires qui interviennent, remplacent, modifient les architectures. Au fil des années, l'exploitant peut ainsi perdre la maîtrise dans son propre système, ne sachant plus exactement quels sont les composants et quels sont les flux de communications sur le réseau. S'ajoute à cela le manque de considération de la cybersécurité pour certains intervenants extérieurs qui, par négligence, peuvent créer un terrain propice à une intrusion malicieuse.

Une série de référentiels pour la cybersécurité industrielle

Sujet particulièrement complexe, la cybersécurité industrielle peut toutefois s'appuyer sur de nombreux référentiels, publiés par différents acteurs du domaine (agences gouvernementales et européennes, organismes de normalisation, associations professionnelles…). Ces documents permettent aux responsables de la cybersécurité, aux équipes d'exploitation ainsi qu'à la filière conception-intégration-maintenance de pouvoir l'appréhender plus facilement. Ils pourront ainsi définir les objectifs de sécurité, identifier l'effort à fournir et comparer les moyens mis en œuvre vis-à-vis de l'état de l'art.

S'il existe une multitude de référentiels, tous n'ont pas le même objectif ni la même cible : certains seront généralistes tandis que d'autres seront spécialisés ; certains seront transverses et d'autres seront spécifiques à un métier ; enfin, certains seront dédiés à l'organisation tandis que d'autres seront orientés vers la mise en œuvre opérationnelle. Il y a cependant des lectures incontournables auxquels il est bon de se référer.

Les mesures détaillées de l'ANSSI

En France, l'ANSSI a publié en 2014 « Les mesures détaillées », qui reste encore aujourd'hui un excellent document. En français et en libre accès, il est compréhensible et adapté à la fois pour la filière SSI et la filière métier puisqu'il s'adresse aux acteurs participant à la conception, la réalisation, l'exploitation et la maintenance des systèmes industriels. Il présente leurs contraintes et spécificités ainsi que les mesures de sécurité organisationnelles et techniques à mettre en œuvre pour tout ou partie d'une installation selon trois classes de risques. Plus la zone à sécuriser comporte un risque fort, plus les exigences sont élevées. Malgré l'excellente qualité de ce document, sa portée reste très européenne, voire plutôt franco-française.

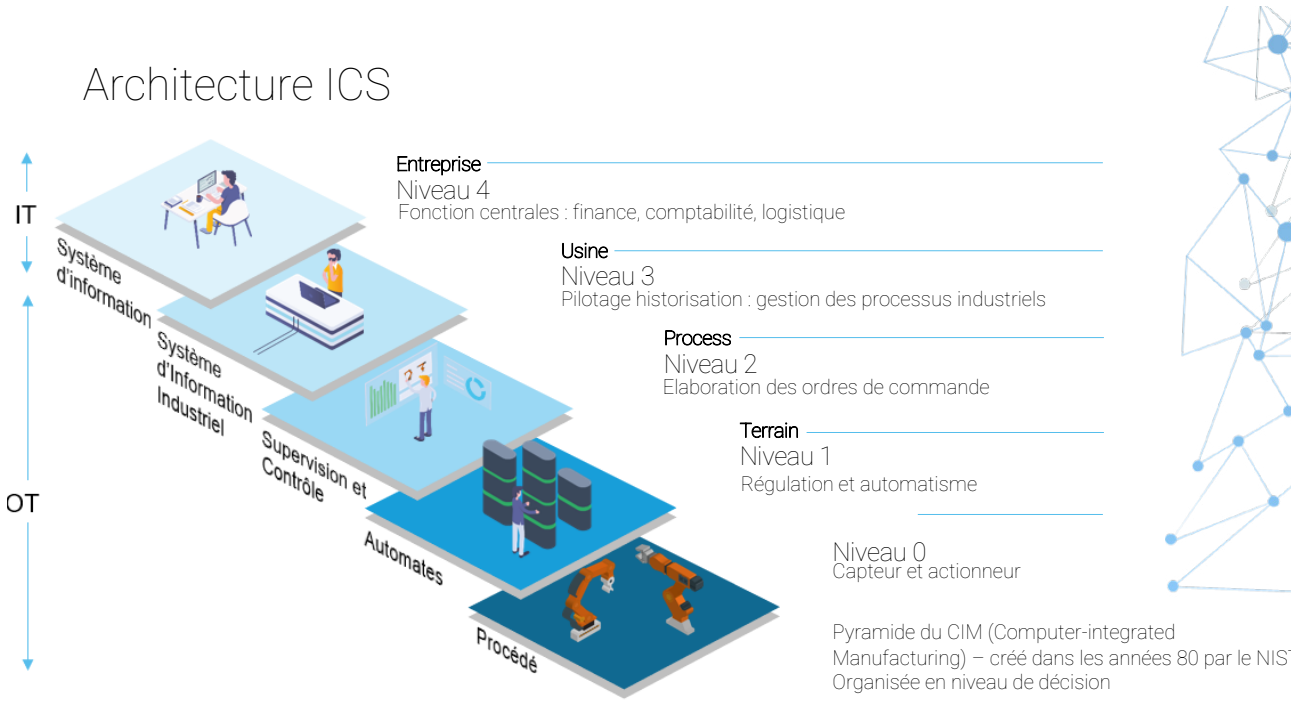

Figure 2 : Architecture des systèmes IACS.

Le référentiel NIST SP800-82

Aux États-Unis, le NIST (*National Institute of Standards and Technology*) consacre une série de référentiels concernant la sécurité (la série SP-800), dont le référentiel SP800-82 qui traite spécifiquement des systèmes industriels. Le document propose une approche structurée en cinq parties :

- Présentation des différents éléments faisant partir d'un système de contrôle industriel ;

- Gestion et analyse de risques des ICS ;

- Aide à la création d'un programme de sécurité spécifique aux systèmes industriels ;

- Définition des architectures, des composants réseaux et de communication (firewalls…) ;

- Détail des mesures de sécurité à mettre en œuvre.

Le référentiel prévoit également une annexe de plus de 130 pages qui reprend notamment le concept à trois niveaux de sécurité, permettant d'adapter la sécurité au niveau de criticité du processus étudié.

La norme IEC-62443

La norme IEC-62443 initiée par l'ISA, est quant à elle en passe de devenir le standard international dédiée à la sécurité informatique des IACS (*Industrial Automation and Control Systems*). Elle a la particularité d'être transverse à tout processus industriel : de l'usine de chocolat au site de production pharmaceutique. Elle est composée de plusieurs documents, regroupés en quatre parties :

- **« General 62443-1 » :** qui regroupe les documents destinés aux concepts généraux, à la terminologie et aux méthodes. Il définit notamment un glossaire ;

- **« Policies & procedures 62443-2 » :** qui spécifie les mesures organisationnelles et s'adresse aux exploitants et mainteneurs des solutions d'automatisation. Il contient également des recommandations dans le cadre des corrections et mises à jour des composants du système, en respectant les spécificités des infrastructures critiques industrielles ;

- **« System 62443-3 » :** dédié aux moyens opérationnels de sécurité des systèmes industriels. Il fournit une évaluation actuelle des différents outils de cybersécurité, décrit la méthode et les moyens pour structurer leur architecture en zones et dresse un état des lieux des techniques de protection contre les cyberattaques. C'est certainement le volet le plus intéressant puisqu'il présente les éléments d'une cyberdéfense en profondeur ;

- **« Component 62443-4 » :** destiné aux équipementiers de solutions de contrôle-commande : automates, RTUs, station de travail, composants réseaux, logiciels d'application. Cette partie décrit d'une part les exigences de sécurité pour ces équipements et présente les bonnes pratiques de développement d'un produit.

À noter que l'IEC-62443 est certifiante pour des fournisseurs de services d'intégration et de maintenance, des systèmes de contrôle, des composants ainsi que des fournisseurs de produits sur l'aspect procédure de développement (figure 2).

Figure 3 : Mesures cyber organisationnelles.

Les mesures de cybersécurité pour les systèmes industriels

Sécuriser les systèmes industriels nécessite une complémentarité entre mesures de sécurité organisationnelles et techniques qu'il conviendra d'adapter au contexte auquel il s'applique : métier, processus, architecture, organisation, localisation…

Ci-dessus, une vue macro des mesures les plus essentielles à prendre en compte sur un chantier de sécurisation (figure 3).

Des mesures de sécurité organisationnelles

La cybersécurité des systèmes industriels nécessite la mise en œuvre de mesures organisationnelles qui ont vocation à proposer des procédures indispensables à la politique de sécurité du système. Ces mesures doivent être prises en compte par l'ensemble des acteurs : informaticiens, responsables de la sécurité, responsables du métier, responsables de l'exploitation et de la maintenance ou encore des administratifs.

Connaissance du système industriel

Les systèmes industriels ont la réputation d'être des systèmes d'information dont il est difficile de connaître les composants et l'environnement d'exploitation. Il est essentiel d'acquérir une connaissance précise et complète du système pour pouvoir lui appliquer les mesures de sécurité dont il fait l'objet.

Dans ce cadre, il est essentiel d'adresser les points suivants :

• Définition d'une une chaîne de responsabilités de la cybersécurité permettant le fondement d'une bonne gouvernance.

• Cartographie pour la connaissance complète de l'ensemble des éléments du système d'information à travers une cartographie physique, logique et applicative. Cette cartographie doit être suivie et mise à jour régulièrement. Elle s'intègre dans une démarche générale de gestion des risques permettant de disposer d'une vision commune et partagée du système au sein de l'établissement afin de faciliter la prise de décision, d'identifier les systèmes critiques et exposés, de réagir et prévoir efficacement les scénarios de défense en cas d'attaque et d'identifier les fonctions nécessaires à la gestion de crise.

• Réalisation d'une analyse de risque. Celle-ci permettra d'identifier et d'évaluer le danger au regard des probabilités d'occurrence, dans une approche fédérative entre sûreté de fonctionnement [1] et cybersécurité. Les critères de cette analyse devront être ceux du risque industriel c'est-à-dire le risque sur l'information, les personnes, l'environnement, les installations mais aussi l'investissement, la capacité de production ou le rendu de service.

Plan de sauvegarde

Un plan de sauvegarde doit également être mis en place afin de disposer des données participant au bon déroulement d'un Plan de Reprise d'Activité (PRA) qui intervient après une attaque. Les données à sauvegarder concernent les équipements serveurs, postes informatiques, équipements terrain (automates, capteurs, actionneurs), équipe- ●●●

1 La sûreté de fonctionnement est l'aptitude d'un système à remplir une ou plusieurs fonctions et à ne pas présenter de dangers pour les utilisateurs et l'environnement.

ments réseau et autres équipements de sécurité. Elles peuvent aller du fichier d'installation logicielle à la base de données de configuration. En ce qui concerne la conception, l'exploitation et la maintenance des systèmes industriels, une documentation détaillée doit être rédigée et sauvegardée afin de maîtriser avec exactitude l'exploitation des processus. Cette documentation intègre notamment les analyses fonctionnelles, les schémas d'architecture et plans d'adressage. Ce plan et cette documentation doivent prendre en compte un suivi des sauvegardes à chaque modification de ces éléments.

Maîtrise des intervenants

Il est essentiel de pouvoir gérer les intervenants en fonction de leurs fonctions et périmètres d'intervention. Cette gestion implique notamment une maîtrise fine des accès aux locaux, aux réseaux, aux données ainsi qu'à l'utilisation d'équipements électroniques. Ces données d'accès doivent être conformes aux bonnes pratiques de gestion des identifiants. Par ailleurs, le facteur humain étant souvent la porte d'entrée d'une cyberattaque, il convient de sensibiliser et de former les intervenants aux bonnes pratiques de cybersécurité. Cette sensibilisation devra être suivie dans le temps. Enfin, les interventions sur les systèmes industriels doivent faire l'objet d'une procédure organisée et tracée décrivant l'ensemble des aspects essentiels à l'intervention, ainsi que l'identité de l'intervenant, la période et le périmètre d'intervention.

Intégration de la cybersécurité dans le cycle de vie du système industriel

La cybersécurité doit faire partie intégrante des projets, de la phase de spécification à la phase d'exploitation notamment pour des programmes de création, extension et refonte des systèmes. Un volet sur la cybersécurité doit ainsi être intégré au cahier des charges et dans les phases de spécification. Il faudra alors prévoir l'ensemble des mesures techniques nécessaires à la sécurité du système ainsi que l'ensemble des procédures permettant le maintien de son niveau de sécurité. Pour les systèmes les plus critiques, le cahier des charges devra prévoir une clause exigeant la fourniture de logiciels et matériels labellisés sur le plan de la cybersécurité.

> **"La cybersécurité doit faire partie intégrante des projets, de la phase de spécification à la phase d'exploitation notamment pour des programmes de création, extension et refonte des systèmes."**

Le système devra également faire l'objet d'une analyse de risque. Au niveau de la phase de conception, une attention particulière sera apportée à la complexité du système qui devra être réduite afin de minimiser le risque cyber.

Les rôles des différents intervenants seront définis et de telle sorte que les privilèges soient réduits au strict nécessaire. Les administrateurs auront des droits et des accès dissociés des autres intervenants sur le système. Avant la mise en exploitation du système, une vérification du niveau de sécurité est recommandée. Pour les systèmes les plus critiques, une homologation ainsi qu'une autorisation d'exploitation est demandée.

Par la suite, le maintien en condition de sécurité doit prévoir des audits réguliers du système afin de convenir de la bonne marche des fonctions de sécurité mises en œuvre ainsi que de l'organisationnel associé. Toutes les modifications d'applications, de fichiers de configuration de l'ensemble des composants du système doivent être tracées. Les changements entre les versions doivent être clairement identifiés.

En parallèle, une veille liée au risque cyber doit être organisée et suivie dans le temps. À cet effet, les CERT nationaux ainsi que ceux des fabricants et éditeurs de logiciels doivent être consultés pour permettre une application des mesures adaptées aux tendances et failles identifiées.

Enfin, la gestion de l'obsolescence sera centrale ici puisque les équipements et logiciels utilisés sur le système peuvent faire l'objet d'obsolescence laissant de nouvelles portes d'accès aux cyber-attaquants. Il convient de prévoir en amont cet aspect en l'intégrant dans les contrats signés avec les fournisseurs et en établissant un plan de gestion d'obsolescence des composants.

Sécurité physique et contrôle d'accès aux locaux

Une politique de gestion des accès aux locaux doit être mise en œuvre pour permettre un accès approprié aux intervenants légitimes à s'introduire dans les locaux. Une recommandation de vigilance particulière sera adressée aux prestataires et intervenants externes.

Réaction en cas d'incident

Le PRA (Plan de reprise d'activité) doit prévoir par anticipation les mécanismes pour reconstruire et relancer le système. Le PCA (Plan de continuité d'activité) doit permettre de prévoir une stratégie qui limite l'impact d'un incident quitte à ce que le service soit dégradé.

En cas d'infection et de paralysie du réseau, les procédures devront prendre en compte les aspects de cybersécurité et s'assurer de dégrader *a minima* la continuité opérationnelle.

Une procédure de gestion de crise efficace permettra de faire face à une crise ainsi qu'à l'analyse *a posteriori*. Cette analyse permettra de tirer les enseignements afin d'améliorer les procédures et les moyens techniques dans une vision prospective. Cette gestion décrira le plan d'action et prévoira une procédure d'escalade afin de traiter l'incident au bon niveau de responsabilité.

Des mesures techniques de sécurité

Les solutions techniques à déployer sur les systèmes industriels sont nombreuses et tiennent compte désormais des spéci-

Figure 4 : Mesures techniques cyber.

ficités de l'OT. Il convient de s'adapter aux contextes avec une approche de défense en profondeur où chaque fonction de sécurité est un rempart nécessaire au blocage ou au ralentissement d'une offensive cyber (figure 4).

Authentification des intervenants

L'authentification doit permettre la mise en œuvre des règles assurant l'identification des utilisateurs, comptes et rôles avec pour objectif d'en maîtriser les privilèges. Les comptes à haut privilège de type « administrateur » seront ainsi traités avec la plus grande attention car c'est le type de compte le plus convoité pour un cyber-attaquant. L'authentification permettra également l'accès sécurisé aux composants du système industriel à travers la mise en place de mécanismes de gestion de mots de passe. Une attention particulière sera apportée à la robustesse des mots de passe et à leur renouvellement.

Sécurisation et cloisonnement de l'architecture du système industriel

Les systèmes industriels possèdent très souvent des architectures « à plat » où tout équipement est en mesure de discuter avec un autre. En termes de cybersécurité, cela revient à augmenter la surface d'attaque de l'ensemble du réseau ; il faudra entreprendre une segmentation de celui-ci pour limiter et bloquer le cyber-attaquant dans sa démarche s'il est déjà introduit sur le système d'information. Pour mettre en œuvre cette segmentation, il convient de découper le système industriel en zones regroupant les actifs qui ont des exigences de sécurité communes. On établira ensuite des conduits entre ces zones pour lesquels il sera appliqué une politique de filtrage des communications entre les zones.

L'interconnexion avec le réseau IT étant monnaie courante, il faudra également mettre en œuvre un cloisonnement entre ces deux systèmes d'information. La réalisation d'une matrice de flux précise devra être entreprise afin d'identifier les flux légitimes et permettre une politique adaptée. Enfin, l'interconnexion entre le système industriel et Internet ou les sites distants devront se limiter au strict essentiel. L'utilisation d'un pare-feu permettra ici une politique de sécurité fine et adaptée. En complément, les réseaux d'administration devront être cloisonnés physiquement des autres systèmes d'information ou logiquement à l'aide d'un tunnel VPN. Plusieurs éléments à noter ici : l'ANSSI recommande l'utilisation de pare-feux qualifiés pour les interconnections entre le réseau OT et Internet. Elle a d'ailleurs publié le guide « *Recommandations pour choisir des pare-feux maîtrisés dans les zones exposées à Internet* » pour accompagner les entreprises dans les architectures et les bonnes pratiques, tandis que l'IEC-62443 propose un concept éprouvé de segmentation réseau, avec des exigences parfaitement adaptées au contexte.

Accès distants

La télémaintenance, la télégestion et la télémétrie impliquent toutes des échanges à distance depuis l'extérieur du système industriel. Pour éviter les prises en main à distance non désirées, il faudra prévoir une connexion distante sécurisée par un tunnel VPN, une authentification de l'utilisateur ou de son rôle et une journalisation des flux échangés. Il conviendra de maîtriser parfaitement la gestion des liaisons VPN et de veiller à ne pas laisser le tunnel monté

en permanence. Le pare-feu s'avère ici aussi incontournable avec un filtrage protocolaire, ne laissant transiter que les flux nécessaires et autorisés.

Sécurisation des protocoles

Idéalement, les protocoles IT non sécurisés devront être désactivés au profit de protocoles sécurisés. Lorsque cela n'est pas possible d'un point de vue opérationnel, ils devront alors être encapsulés dans un tunnel. Il conviendra de mettre en place une analyse protocolaire pour les flux transitant entre les pare-feux assurant la segmentation afin de n'autoriser que les flux strictement nécessaires.

Détection d'intrusion

Une stratégie de détection d'intrusion peut être mise en œuvre pour alerter d'une attaque sur le système industriel. Une sonde de détection dédiée aux environnements industriels pourra par exemple effectuer une surveillance passive en 24/7 du système et notifier les équipes cyber (équipe SOC IT) de tout comportement malveillant.

Sécurisation des équipements

La sécurisation des équipements industriels peut prendre plusieurs formes, complémentaires entre elles. Idéalement, tous les actifs des systèmes industriels (automates, postes, switch…) devraient durcir leurs configurations. Ceci implique la désactivation de l'ensemble des services et des fonctions matérielles qui ne sont pas nécessaires (ports physiques, comptes par défaut, logiciels inutiles, fonctions de débogage…).

Pour les postes de supervision et d'ingénierie, cela peut passer par un durcissement de l'actif en n'autorisant que les applications métier strictement nécessaires pour gérer les connexions ainsi que les interfaces réseau, dédier le poste à une seule et unique activité et s'assurer qu'il est installé dans un lieu sécurisé où l'accès est contrôlé.

Pour les postes de travail, une solution de scellement de poste peut être déployée. Elle permettra notamment de mettre en place une liste blanche d'applications, de sécuriser les accès au BIOS, à la CPU et aux programmes mais aussi d'assurer l'intégrité et l'authenticité des firmwares, mises à jour logicielles, programmes automates et de tout fichier téléchargé sur le poste.

Gestion des corrections

La gestion des vulnérabilités pour les systèmes industriels doit également s'inscrire dans une démarche globale de *patch management*. Pour des processus fonctionnant en 24/7, il faudra planifier et intégrer cette gestion dans le plan de maintenance et prévoir des processus de solutions correctives ou palliatives après validation et vérification de la non-régression du système avec leur déploiement.

La gestion des médias amovibles et notamment des clés USB est également centrale, puisque ces médias sont encore largement utilisés au sein des systèmes industriels. Une station blanche permettant l'analyse et la décontamination des clés USB pourra par exemple être installée à l'entrée du site pour l'ensemble des employés et des intervenants externes.

Enfin, afin d'assurer la traçabilité des évènements et de faciliter une analyse *post mortem* sur le système suite à un incident, une politique de journalisation des événements de sécurité doit être définie. Seront à prévoir la définition des événements pertinents à tracer, leur conservation (stockage, archivage), les conditions d'analyse, ainsi que les alertes à générer.

Communications sans fil

Sécurité des IIoT

Au sein des systèmes industriels, l'utilisation de réseau filaire est encore privilégiée mais la tendance devrait s'inverser avec l'arrivée de la 5G. Les réseaux sans fil doivent intégrer les fonctions de sécurité d'authentification du point d'accès et de l'actif qui se connecte et le contrôle d'accès réseau. Les équipements qui se connectent devront faire l'objet d'une ségmentation particulière avec des règles de filtrage adaptées (voir IEC-62443 : notion de zones et conduits).

Les IIoT intégrant des mécanismes de sécurité tels que la gestion de certificats (PKI) seront privilégiés pour des aspects d'authentification, non-répudiation et de confidentialité sur le réseau OT mais également pour les communications avec la Data Lake situé dans le *cloud*.

En complément, les enjeux de sûreté et de contrôle d'accès étant omniprésents, la mise en place de certificats X509 pourra également permettre l'authentification des utilisateurs (fabriquant, mainteneur…) qui se connectent aux IIoT.

Lorque les IIoT ne prévoient pas de mécanismes de sécurité, il faudra déporter ses fonctions sur des passerelles *Edge*.

Sécurité du *Cloud*

Les données qui transitent entre le système industriel et le *cloud* devront

L'auteur

Vincent Nicaise est en charge du développement des partenariats technologiques et commerciaux avec les acteurs de l'automatisme et de la cybersécurité pour Stormshield. Vincent a auparavant contribué à la construction d'une offre de cybersécurité pour l'IoT au sein d'Atos et a développé l'activité commerciale d'une start-up pour une sonde de détection dédiée aux systèmes industriels. Son parcours professionnel lui a permis de travailler durant 20 ans dans l'édition logiciel dont 13 ans dans le domaine de la cybersécurité.

faire l'objet d'un encapsulement des données à travers un tunnel sécurisé de type VPN. La sécurité frontale du *cloud* sera assurée par un pare-feu dont les capacités d'évolution permettront d'adapter les performances et la sécurité à la quantité de données transmises. Un contrôle des accès à distance au *cloud*, une authentification des IoT ainsi qu'une gestion sécurisée des utilisateurs aux applications sera mise en œuvre.

Il conviendra de veiller à une surveillance des activités du service *cloud* ainsi qu'une sécurité opérationnelle (configuration et gestion des changements, gestion des vulnérabilités, surveillance des protections, gestion des incidents, mécanismes de récupération des données en cas de sinistre…). Les points de terminaison (navigateurs web) devront introduire des fonctions de sécurité. Les protocoles de communication entre les points de terminaison et le *cloud* utiliseront des protocoles sécurisés (type HTTPS).

Enfin pour les utilisateurs de services *cloud* externalisés, il sera recommandé de privilégier les fournisseurs labellisés par l'agence nationale, gage de sécurité et de souveraineté numérique. En France, l'ANSSI a mis en place la qualification de sécurité SecNumCloud.

Conclusion

Si l'on constate une recrudescence des cyberattaques ces dernières années sur les systèmes industriels, et notamment le développement des attaques par des logiciels de rançon, les stratégies de sécurisation et les chantiers de mise à niveau semblent encore insuffisantes sur l'ensemble des filières industrielles.

En France, sous la pression des obligations régaliennes, les infrastructures critiques font office de moteur à cette montée en puissance. En effet, ces systèmes industriels sensibles s'équipent et enrichissent leurs équipes de nouveaux profils dotés d'une double compétence cyber et automatisme. Et de plus en plus, les équipes IT et OT tentent à converger au bénéfice d'une meilleure maîtrise de la sécurité des processus.

De son côté, la filière cybersécurité est montée en compétences avec des solutions techniques adaptées et des expertises plus poussées en intégration et conseil. Pour beaucoup d'entreprises et d'organisations, il reste aujourd'hui encore à sensibiliser et convaincre les comités de directions ; c'est peut-être le plus difficile maintenant. ■

Résumé

La cybersécurité appliquée aux systèmes industriels doit prendre en compte leurs spécificités techniques et organisationnelles. En effet, il n'est pas question de dupliquer les bonnes pratiques de l'IT sans l'adapter à un contexte industriel et opérationnel, souvent complètement différent. Il convient de définir une approche de défense en profondeur où chaque fonction de sécurité est un rempart nécessaire au blocage ou au ralentissement d'une offensive cyber.

Si aujourd'hui les fabricants d'automates travaillent à ajouter des fonctions de sécurité essentielles ainsi qu'à intégrer la cybersécurité dans les cycles de développement logiciel, le fameux « *cybersecurity-by-design* », il n'en demeure pas moins que les installations dites « *legacy* » doivent faire avec des produits pas ou peu cyber-sécurisés. Il peut être très contraignant et coûteux de cybersécuriser un système existant. Pour les nouveaux projets, il est essentiel d'intégrer la cybersécurité dès les phases d'avant-projet pour s'assurer de sa bonne prise en compte

En France, l'ANSSI a publié en 2014 « Les mesures détaillées », qui s'adresse aux acteurs participant à la conception, la réalisation, l'exploitation et la maintenance des systèmes industriels. La norme IEC-62443 initiée par l'ISA, est quant à elle en passe de devenir le standard international dédié à la sécurité informatique des IACS (*Industrial Automation and Control Systems*). ■

Abstract

Cybersecurity for industrial systems must take into account their technical and organizational specificities. It requires the adaptation of IT best practices to the industrial and operational context, which is often completely different. A defense-in-depth approach should be defined where each security function is a necessary wall to block or slow down a cyber attack.

Today PLC manufacturers are working to add essential security functions as well as to implement «cybersecurity-by-design»capabilities in their software development cycles.

Nevertheless many "legacy" system have to cope with products which are not very cyber-secure. It can be very complex and costly to cybersecure an existing system.

For new projects, it is essential to integrate cybersecurity from the design phases in order to ensure that security is properly taken into account

In France, ANSSI published «Detailed measures», which define best practices for the design, construction, operation and maintenance of industrial systems. The IEC-62443 standard is becoming the international standard dedicated to IT security for IACS (Industrial Automation and Control Systems). ■