LIVRE BLANC

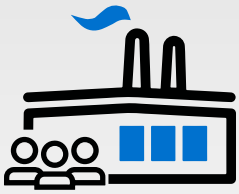
Sécuriser l'Industrie 4.0

Perspectives & impacts sur les environnements OT

Synthèse

Le concept d'Industrie 4.0 favorise la modernisation des environnements technologiques industriels (OT - Operational Technologies) pour améliorer l'efficacité des processus métiers et agréger davantage de données décisionnelles, à partir de systèmes autrefois cloisonnés, mais désormais interconnectés. Cependant, la convergence de ces systèmes présente un impact majeur en termes de sécurité. En effet, 9 entreprises sur 10 ont subi une intrusion qui a pesé sur leur productivité, leurs revenus, leur image de marque, leurs éléments de propriété intellectuelle ou leur sécurité physique.[1] La majorité (70 %) des acteurs industriels interrogés déclare que la cybersécurité des systèmes industriels compte parmi les 5 principaux risques commerciaux pour leur entreprise.[2]

La transformation digitale et la dépendance accrue aux données sont des tendances universelles. Selon McKinsey, le COVID-19 a accéléré le changement : l'adoption du digital a affiché, en seulement 8 semaines, une croissance équivalente à celle qu'elle aurait connue en 5 ans.[3] Dans de nombreux secteurs d'activité, comme la production industrielle notamment, la transformation digitale devrait se poursuivre. Si les cyberattaques constituent une réelle menace, nombre d'industriels sont à la recherche de solutions pour juguler les risques de sécurité à l'heure de l'Industrie 4.0.



Plus de 80 % des acteurs industriels s'attendent à ce que le budget de leur entreprise consacré à la sécurité des technologies OT progresse au cours du prochain exercice fiscal.[4]

Industrie 4.0 et convergence entre OT et IT

La transformation digitale des acteurs industriels est motivée par la promesse de cette quatrième révolution industrielle qu'est l'Industrie 4.0. La première révolution industrielle était la mécanisation, la deuxième la production de masse et les chaînes de montage utilisant l'électricité, et la troisième l'adoption des ordinateurs et de l'automatisation. Aujourd'hui, l'Industrie 4.0 renforce l'automatisation avec des systèmes alimentés par des données et le machine learning. Cette évolution a conduit à la convergence des réseaux technologiques industriels (OT) et des réseaux informatiques (IT).

Les environnements OT hébergent souvent des systèmes de contrôle industriel (ICS) qui pilotent le fonctionnement d'équipements ou de machines. Ils sont généralement gérés à l'aide d'automates programmables (PLC) et peuvent inclure des systèmes SCADA (contrôle de supervision et acquisition de données) qui servent d'interface utilisateur graphique pour les systèmes ICS. Si l'OT contrôle les équipements, c'est l'IT qui contrôle les données. L'IT s'attache à garantir la confidentialité, l'intégrité et la disponibilité des systèmes et données, tandis que l'OT se concentre sur la sécurité et la haute disponibilité des machines.

L'industrie 4.0 implique d'intégrer l'automatisation et les échanges des données dans les technologies et processus de fabrication, notamment l'Internet des objets (IoT), l'Internet des objets industriels (IIoT), le cloud computing, l'informatique cognitive, l'intelligence artificielle (IA) et les systèmes cyber-physiques (CPS). Cependant, l'Industrie 4.0 accentue les défis qui émergent de la convergence entre réseaux OT et IT. Avec leurs équipes et systèmes de contrôle spécialisés et leurs technologies héritées souvent obsolètes, les réseaux OT connaissent un risque plus marqué, la conséquence directe d'une connectivité plus large. Cette interconnexion des systèmes internes avec des ressources situées hors de murs des usines a modifié l'ensemble de l'écosystème de sécurité OT, laissant les experts IT et OT se démener pour protéger à la fois l'infrastructure de l'entreprise et l'environnement de production.

Industrie 4.0 et sécurité

L'un des principaux objectifs de l'Industrie 4.0 est d'aligner les processus industriels et les processus business, afin que l'outil de production opère de concert avec les réalités du terrain. L'agrégation de données provenant de sources diverses et externes accentue le risque d'intrusion de hackers et l'exposition à des campagnes visant à perturber les ressources digitales et physiques. Traditionnellement, les réseaux OT étaient sécurisés car cloisonnés des réseaux IT, ce qui isolait les équipements et technologies OT vulnérables et fragiles des réseaux IT d'entreprise. L'intention était de les protéger de la plupart des attaques ciblant l'infrastructure IT.

À mesure que les entreprises se transforment, les changements apportés au mode d'exploitation de ces réseaux doivent tenir compte des meilleures pratiques de cybersécurité pour protéger un large panel de systèmes et d'applications désormais interconnectés : applications industrielles, systèmes de planification des besoins en matériaux (MRP), automates programmables, interfaces homme-machine (IHM) et autres composants.

Avec des réseaux IT et OT interconnectés, même à un degré limité, les attaques ciblant l'IT s'en prennent désormais à l'OT. Ces attaques contre les infrastructures critiques ont le potentiel de causer des dommages particulièrement lourds. Une panne d'un système industriel dans le secteur de la fabrication pourrait littéralement paralyser la production pendant des heures, détruire des matériaux sensibles en cours de processus, ce qui coûterait des millions de dollars, ou encore exposer les entreprises à des sanctions potentielles pour cause de non-conformité réglementaire. Ce nouvel éventail d'attaques ciblant les systèmes OT peut avoir un impact significatif sur les processus cyber-physiques auxquels les citoyens font confiance. Il est plus que jamais important de comprendre l'impact collatéral d'une attaque : des problématiques de livraison de ressources, la paralysie de systèmes de défense nationale et même les dommages causés à des civils innocents ne sont que quelques-unes des conséquences potentielles d'une attaque.

Près des trois quarts des entreprises font désormais état d'interconnexions, à minima de base, entre IT et OT.[5]

Risques de sécurité OT

L'OT est particulièrement vulnérable aux menaces actuelles et anciennes, compte tenu d'un parc technologique vieux de 20 à 30 ans. Les systèmes de contrôle industriel présentent un risque car ils utilisent souvent des communications non authentifiées ou non cryptées. Les équipements ont généralement un cycle de vie long. Ils proviennent de plusieurs fournisseurs et peuvent utiliser différents protocoles industriels. Un fonctionnement sûr et continu est une priorité, mais une action aussi simple qu'un scan actif peut provoquer des défaillances et perturber l'outil de production, avec de lourdes conséquences à la clé.

Les menaces qui pèsent sur les systèmes cyber-physiques se renforcent et évoluent. Le premier semestre de 2020 témoigne d'un bond d'environ 35 % du volume total des attaques par rapport au second semestre de 2019[6] À mesure que les réseaux OT et IT opèrent leur transformation digitale, l'infrastructure de sécurité gagne en complexité et se fragmente, révélant de nouvelles vulnérabilités et possibilités de piratage des systèmes. De nombreuses entreprises ont multiplié les solutions de sécurité autonomes pour compenser la sécurité moindre résultant du décloisonnement entre environnements IT et OT. Une nouvelle vulnérabilité ou une nouvelle exigence de conformité sera traitée via des mesures complémentaires, ce qui ne facilite pas la visibilité et le partage d'informations de sécurité sur l'ensemble de l'infrastructure de sécurité. Inévitablement, les analystes réseau ne disposent pas d'une visibilité claire et temps réel sur la sécurité de leur environnement réseau OT.

Heureusement, la majorité des industriels considère la sécurité des technologies OT comme l'un des cinq risques métiers les plus importants auxquels ils sont confrontés aujourd'hui, tandis que plus d'un tiers des personnes interrogées (39 %) l'intègre dans leur Top 3 des risques.[7] Ces entreprises, dans leur majorité, semblent agir en fonction de ces préoccupations : l'étude MAPI montre que 83 % d'entre elles prévoient d'augmenter la part du budget d'entreprise allouée à la sécurité OT. Compte tenu des multiples défis qui les attendent alors qu'ils s'efforcent d'intégrer les deux environnements complexes que sont l'IT et l'OT, cet investissement supplémentaire est essentiel.

Avec une pénurie de ressources, des outils technologiques inadéquats, une formation déficiente et l'évolution rapide des menaces, les obstacles à une gestion efficace des menaces sur les réseaux OT sont nombreux. Malgré ces obstacles, les industriels sont prêts à s'investir pour déployer les meilleures pratiques de cybersécurité alors qu'ils adoptent les principes de l'Industrie 4.0. En fait, 94 % des personnes interrogées prévoient de mettre en œuvre de nouvelles solutions pour faire face à leurs risques de sécurité OT.[8]

Gouvernance, risques et conformité

Au-delà de ses fonctionnalités de protection, la sécurité OT invite à se concentrer sur la conformité, l'audit, les équipes, les coûts et la productivité. La conformité ne doit pas être confondue avec la sécurité, bien que les deux disciplines soient liées. La complexité générée par des solutions de sécurité fragmentées est exacerbée par les changements initiés par les instances de réglementation sur les questions de conformité, lors de nouvelles réglementations ou de l'évolution des normes existantes. En l'absence de solutions efficaces dotées de fonctions automatisées de suivi, d'audit et de reporting, les entreprises doivent consacrer beaucoup de temps à l'agrégation de données et à leur corrélation manuelle.

La conformité aux normes définies par les autorités compétentes peut constituer une base de référence pour la sécurité. Aux États-Unis, la plupart des normes relatives aux systèmes ICS sont élaborées et publiées par des autorités sectorielles ayant un intérêt et un engagement envers la préservation des infrastructures critiques. Elles sont souvent requises dans les secteurs industriels, mais ne correspondent pas toujours aux exigences plus générales des systèmes de contrôle industriel.

Les deux frameworks ICS les plus couramment cités sont le National Institute of Standards and Technology (NIST) SP 800-82 et l'International Society of Automation (ISA) 62443. Il convient également de prendre en considération le récent rapport NIST Interagency/Internal Report (NISTIR) 8219, qui se penche sur l'utilisation de la détection des anomalies comportementales dans les réseaux ICS.

44% des entreprises n'assurent aucun suivi, ni reporting de conformité par rapport aux réglementations du secteur.[9]

Les piliers de la sécurité de l'Industrie 4.0

Pour évoluer au rythme de l'Industrie 4.0, les industriels repensent leur architecture existante selon deux axes : simplifier cette architecture et consolider les différents outils de sécurité en place. Ils doivent également s'assurer que les pratiques de sécurité sont adaptées à leurs orientations business, dans le cadre d'une stratégie unique, intégrée et orientée sécurité. Les entreprises doivent évaluer leur situation actuelle, y compris les ressources dont elles disposent. L'étape suivante consiste à analyser leurs processus et à étudier les options qui améliorent l'agilité et la sécurité. Armées de ces informations, elles peuvent rechercher des solutions qui favoriseront la maturité de la cybersécurité OT.

Pilier 1 : dresser un état des lieux de l'existant

Les normes de cybersécurité peuvent aider à orienter et guider les entreprises dans l'élaboration et la mise en œuvre d'une stratégie de sécurité pertinente. Les entreprises sont invitées à prendre en compte des normes établies telles que le NIST ou la norme CEI 62443 pour déterminer où elles en sont et les axes d'amélioration de leur sécurité. En profitant des conseils des experts du secteur, les responsables de la sécurité peuvent affiner leurs connaissances et atteindre les objectifs de sécurité définis pour leur entreprise.

Le framework de cybersécurité du NIST (CSF) fournit un cadre pour standardiser les programmes de sécurité ainsi qu'un langage commun pour améliorer les communications, la compréhension et la collaboration entre les équipes IT et OT. Les industriels peuvent utiliser le NIST CSF pour que leurs initiatives digitales répondent à leurs objectifs métiers et organisationnels, ainsi que pour identifier et mettre en œuvre les changements d'infrastructure nécessaires, qu'ils soient liés aux personnes, aux processus ou à la technologie.

La norme CEI 62443 constitue un autre cadre commun qui peut être utilisé pour gérer les vulnérabilités de sécurité affectant les systèmes industriels de contrôle et d'automatisation. Elle conseille sur le choix des produits qui amélioreront les défenses des systèmes ICS d'une entreprise tout en arbitrant entre coûts et gestion des risques.

Pilier 2 : tenir compte des besoins en ressources humaines

Les acteurs de l'OT doivent dresser un état des lieux de leurs ressources humaines et déterminer les moyens de gérer les différences de culture, d'objectifs et de principes entre les équipes IT et OT. Il s'agit également de prendre en compte les besoins des travailleurs à distance. L'avènement de la pandémie de COVID-19 a encouragé une adoption rapide du télétravail à l'échelle mondiale, avec néanmoins des risques. La sécurisation des télétravailleurs a lourdement pesé sur les systèmes de sécurité, dans un contexte de migration vers le cloud et de prolifération des terminaux. Le télétravail s'inscrit désormais dans la durée, pandémie ou pas.

Malgré une sensibilisation accrue à la cybersécurité et des initiatives de formation, le phishing reste un problème majeur tandis que les entreprises sont confrontées au risque élevé de menaces internes. Les dommages imputables à ces menaces endogènes peuvent être difficiles à déterminer, compte tenu de la multiplicité des comportements et des objectifs de ces menaces. Les choses sont encore plus difficiles lorsque les collaborateurs ne sont pas sur site. Les industriels doivent être en mesure de sécuriser tous les utilisateurs, où qu'ils se trouvent et quel que soit le dispositif utilisé : les collaborateurs sur site, ceux œuvrant dans les usines et entrepôts, les cadres dirigeants, les contractuels et les intérimaires.

L'évolution des rôles, les équipes pluridisciplinaires et la collaboration accrue donnent lieu à des relations hiérarchiques complexes et une faible visibilité sur les responsabilités. Les départements, équipes et individus qui œuvraient de manière cloisonnée avant l'ère Industrie 4.0 doivent respecter les valeurs de chacun, en dépit d'objectifs parfois différents. Les RSSI, les architectes informatiques, les DSI, les directeurs d'usine et les analystes réseau doivent tenir compte des impératifs d'optimisation de l'opérationnel et parvenir à un consensus sur des questions telles que la confidentialité (priorité absolue pour les équipes IT) et la haute disponibilité (priorité absolue pour l'OT, au même titre que la sécurité physique du personnel des usines). Pour assurer une résilience durable de l'entreprise, il est essentiel de collaborer au renforcement de la posture de sécurité.

Pilier 3 : les processus de d'évaluation

À mesure que les entreprises opèrent leur transformation digitale, des changements sont apportés à la fois aux technologies et aux processus business. L'Industrie 4.0 illustre comment la technologie peut automatiser des processus qui pourraient être exécutés de manière plus simple à l'avenir. Cette approche tire pleinement parti des données pour améliorer l'efficacité tout au long d'un processus métier, qui peut s'étendre de la chaîne logistique à l'expérience client, et ainsi favoriser des décisions plus éclairées.

Les processus qui peuvent être améliorés vont du traitement des commandes à la fabrication des produits, en passant par la facturation des clients ou la détection et la réponse à un incident de sécurité. Dans chaque domaine, il convient de procéder à une évaluation pour arbitrer entre gains de productivité et risques pour l'entreprise.

Les entreprises devraient formaliser ce type d'évaluation des processus opérationnels face à une digitalisation croissante qui implique la collecte et le partage de volumes toujours plus importants de données, entre des systèmes et des processus qui n'étaient pas connectés auparavant. Lorsque les entreprises définissent les domaines à améliorer et à digitaliser, elles doivent identifier les lacunes ou les failles de sécurité qui en résultent.

54% des collaborateurs ayant des responsabilités et tâches pouvant être menées depuis leur domicile, déclarent vouloir travailler de chez eux, totalement ou partiellement, lorsque la crise du coronavirus touchera à sa fin.[10]

L'efficacité et l'optimisation des activités métiers étant une priorité, de plus en plus d'entreprises intègrent des services cloud pour améliorer leurs processus. Les industriels adoptent ainsi des services cloud de planification des ressources de production (MRP) et de planification des ressources d'entreprise (ERP). Ces services recueillent des données à partir de systèmes IT et OT pour assurer une prise de décision rapide et efficace. Il est essentiel de sécuriser ces ressources présentes au sein d'une architecture qui couvre le data center, les systèmes industriels et une multitude d'environnements cloud.

Pilier 4 : des technologies actualisées

Pour concrétiser les avantages de l'Industrie 4.0, les entreprises doivent disposer d'une sécurité OT et IT prête à faire face aux attaques les plus sophistiquées. Une solution de cybersécurité complète doit couvrir l'ensemble de la surface d'attaque, partager les renseignements de veille sur les menaces entre les différents produits de sécurité et automatiser la riposte aux menaces. La protection d'un environnement convergent de type Industrie 4.0 exige cinq bonnes pratiques.

1. **Gagner en visibilité sur le réseau en identifiant, catégorisant et hiérarchisant les ressources**

   Un inventaire à jour des environnements et ressources IT et OT facilite la planification de la sécurité et la sensibilisation à celle-ci. Les entreprises ne peuvent protéger les segments d'infrastructure qu'elles ne peuvent voir, d'où l'intérêt d'un inventaire à jour des dispositifs et applications fonctionnant sur leurs réseaux. Ces derniers doivent être identifiés et catégorisés en fonction de leurs caractéristiques et de leur comportement.

2. **Segmenter le réseau**

   La segmentation est un levier efficace pour protéger les environnements réseau. L'absence de segmentation IT/OT ou une segmentation mal réalisée peut favoriser l'exploitation d'une vulnérabilité OT qui est divulguée. Une segmentation réseau pertinente compartimente un réseau en des segments ou zones fonctionnels, avec la possibilité de définir des sous-zones ou des micro-segments. Chaque zone n'est accessible qu'aux dispositifs, applications et utilisateurs pré-autorisés. Un pare-feu de nouvelle génération (NGFW) définit et applique les zones de contrôle. Ce NGFW définit également des canaux permettant aux données et aux applications essentielles de passer d'une zone à l'autre en toute sécurité.

   Cette architecture en zones et canaux réduit considérablement le risque d'infection et de piratage de l'infrastructure au sens large. Elle limite l'impact potentiel d'une intrusion en restreignant la capacité d'un assaillant à se déplacer au sein ou via un réseau OT. Les utilisateurs ou les dispositifs autorisés pour une activité spécifique sur une zone sont restreints à cette zone. Le modèle de zones et de canaux doit être dynamique plutôt que statique, avec un contrôle d'accès granulaire qui surveille en permanence les niveaux de confiance et adapte les politiques de sécurité en conséquence.

3. Analyser le trafic

Les pare-feu sont utilisés pour dissocier un réseau en zones, segments et canaux, mais il est tout aussi important d'analyser le trafic réseau pour identifier les menaces connues et inconnues. Les acteurs de l'OT peuvent se protéger davantage des vulnérabilités affectant les applications et dispositifs des constructeurs de systèmes de contrôle industriel. Face à de nombreux dispositifs OT qui sont dépourvus de correctifs, l'utilisation de correctifs virtuels (virtual patching) permet d'identifier et neutraliser les exploits. Le trafic réseau doit être analysé sur la base des évènements réseau. Au lieu de recouper manuellement les données, un moteur intelligent de découverte des infrastructures et des applications peut être utilisé pour identifier et cartographier la topologie des infrastructures physiques et virtuelles, sur site et dans les clouds publics et privés, à l'aide d'identifiants et sans connaissance préalable des dispositifs ou des applications.

78 % des entreprises n'ont qu'une visibilité centralisée partielle sur leurs environnements OT.[11]

4. Contrôler l'accès

Les dispositifs, utilisateurs et applications doivent être authentifiés avant d'accéder à l'environnement OT ou à l'une de ses ressources segmentées. Une authentification sécurisée est essentielle. La plupart des incidents de sécurité OT, dûs au piratage de comptes utilisateurs et de mots de passe, sont également exacerbés par l'attribution de niveaux d'accès inappropriés aux utilisateurs.

Les industriels ont besoin de solutions qui valident contextuellement les utilisateurs et dispositifs qui se connectent au réseau, et restreignent leur accès aux seules ressources dont ils on besoin. Grâce à des solutions de contrôle, les politiques peuvent être appliquées et des mesures appropriées peuvent être prises si nécessaire, sans perturber les systèmes critiques. L'authentification multifactorielle (MFA) et la possibilité de restreindre le réseau aux utilisateurs et aux appareils authentifiés sont des fonctionnalités importantes. Les solutions de contrôle d'accès au réseau doivent couvrir chaque partie de l'infrastructure, y compris l'edge, la 5G, l'IIoT et le cloud hybride et public.

5. Sécuriser les accès filaires et sans fil

Historiquement, les infrastructures OT étaient moins dépendantes de la connectivité sans fil pour assurer le bon fonctionnement des usines. Cependant, les acteurs de l'OT sont aujourd'hui plus nombreux à déployer des capteurs et autres dispositifs IIoT et à les interconnecter via des liens sans fil. La portée et la fréquence de ces connexions étendent proportionnellement la surface d'attaque digitale. Les points d'accès (AP) sans fil et les commutateurs réseau sont des cibles attrayantes pour les cyberattaques. Ils doivent être sécurisés en natif et administrés à partir d'une interface centralisée, au lieu d'être protégés par des outils de sécurité distincts et donnant lieu à plusieurs interfaces de gestion. La gestion centralisée de la sécurité permet de réduire les risques, facilite l'application des politiques, améliore la visibilité et réduit la charge d'administration pour les équipes de sécurité et opérationnelle.

Pilier 5 : une veille et un reporting décisionnels

Au-delà de se baser sur les meilleures pratiques de cybersécurité, une stratégie de sécurité intégrale pour l'Industrie 4.0 doit permettre un partage intégré et automatisé d'informations de veille sur les menaces et offrir un reporting de conformité. Les RSSI ont besoin d'une solution de sécurité OT évolutive et capable de notifier automatiquement la présence de toute menace sur l'ensemble de l'écosystème OT. Une veille décisionnelle doit être déployée pour défendre de manière proactive les environnements OT en mobilisant chaque composante de sécurité. Elle doit s'étendre du data center au campus corporate et jusqu'à l'edge du réseau.

En marche vers l'Industrie 4.0

Pour tirer le meilleur parti de la digitalisation des processus métiers et optimiser la création de valeur qu'offre l'Industrie 4.0, les industriels doivent traiter la question cruciale de la sécurité OT. Lorsqu'ils concrétisent les principes de l'Industrie 4.0 et modernisent leur environnement OT, il est essentiel qu'ils élaborent une stratégie de transformation basée sur une approche qui privilégie sécurité. En analysant, dans un premier temps, leur état actuel, leurs ressources et leurs initiatives d'amélioration des processus métiers, ils peuvent opter pour les améliorations technologiques et la sécurité qui les aideront à atteindre leurs objectifs.

La visibilité et une surveillance permanente de l'environnement des industriels permettront à ces derniers à sécuriser ces nouveaux réseaux IT et OT convergents qui accompagnent les initiatives Industrie 4.0. En prenant des mesures pour s'assurer d'une stratégie agile, ils auront la capacité de s'adapter aux changements business, industriels et technologiques à venir.

[1] "2020 State of Operational Technology and Cybersecurity Report," Fortinet, 30 juin 2020.

[2] David Beckoff, et al., "Securing Critical Operational Technology in Manufacturing: Managing Cyber Risk, Readiness, and Resilience," Manufacturers Alliance for Productivity and Innovation, 2020.

[3] Aamer Baig, et al., "The COVID-19 recovery will be digital: A plan for the first 90 days," McKinsey Digital, 14 mai 2020.

[4] David Beckoff, et al., "Securing Critical Operational Technology in Manufacturing: Managing Cyber Risk, Readiness, and Resilience," Manufacturers Alliance for Productivity and Innovation, 2020.

[5] « Independent Study Pinpoints Significant SCADA/ICS Cybersecurity Risks », Fortinet, 28 juin 2019.

[6] "Microsoft Digital Defense Report," Microsoft, Septembre 2020.

[7] David Beckoff, et al., "Securing Critical Operational Technology in Manufacturing: Managing Cyber Risk, Readiness, and Resilience," Manufacturers Alliance for Productivity and Innovation, 2020.

[8] Idem.

[9] "2020 State of Operational Technology and Cybersecurity Report," Fortinet, 30 juin 2020.

[10] Kim Parker, et al., "How the Coronavirus Outbreak Has—and Hasn't—Changed the Way Americans Work," Pew Research Center, 9 décembre 2020.

[11] "2020 State of Operational Technology and Cybersecurity Report," Fortinet, 30 juin 2020.

septembre 5, 2022 1:50 PM

989802-0-0-FR