



STORMSHIELD

AVIS D'EXPERT

INDUSTRIE 5.0 : ET LA CYBERSÉCURITÉ DANS TOUT ÇA ?

Khobeib Ben Boubaker

Head of Industrial Security
Business Line, Stormshield

Humaine, durable, résiliente : alors que l'industrie 4.0 axait son déploiement sur l'amélioration de la productivité grâce aux technologies Big Data, IoT et aux machines intelligentes, l'industrie 5.0 promet de se recentrer sur l'humain et la société. Quid de la cybersécurité dans ce contexte ?

Dix ans après l'introduction du terme officiel d'industrie 4.0, place à une nouvelle révolution industrielle avec l'industrie 5.0. Elle s'attache **à remettre l'humain au cœur de processus industriels aujourd'hui très largement numérisés**. Mais les interactions entre homme et machine impliquent toutefois de mettre en place des mesures de sécurité fortes au sein des environnements industriels. Quelle place alors pour la cybersécurité ? Et à quel horizon ? Explications.



LES PROMESSES DE L'INDUSTRIE 5.0

L'idée selon laquelle les machines et les technologies conduiront, à terme, à une élimination des hommes au sein des usines et au cœur des processus industriels est une vision aujourd'hui dépassée pour l'industrie. En se focalisant sur les gains de productivité, l'industrie 4.0 avait pour objectif de rendre les usines « *intelligentes* » en pilotant et en supervisant la production à distance.

Mais alors, **c'est quoi l'industrie 5.0 ?** Le nouveau paradigme de l'industrie 5.0 entend donc se recentrer sur l'humain. « *Le premier axe est d'améliorer les conditions de travail des ouvriers grâce à de nouvelles solutions techniques et à des machines robotisées performantes* », souligne **Vincent Nicaise**, Responsable des partenariats et de l'écosystème industriels chez Stormshield. Avant d'insister sur une autre dimension : « *redorer le blason de l'activité industrielle dans un contexte favorable à la thématique de la réindustrialisation en Europe. Il s'agit donc également d'apporter de l'attractivité à une filière qui souffre depuis plusieurs années en attirant les ouvriers de demain mais aussi des savoir-faire en ingénierie.* » **Profiter à la fois aux travailleurs, aux entreprises mais aussi à la planète, tel est le credo de l'industrie 5.0.** Il s'agit donc d'« *utiliser les nouvelles technologies pour assurer la prospérité des emplois et de la croissance, mais aussi et surtout en respectant les limites de production de la planète* », insiste **Stéphane Potier**, responsable de l'offre Cybersécurité OT & IoT chez Advens. En cela, ce nouveau paradigme industriel est l'antithèse du spectre d'une usine 100% automatisée qui détruit des emplois. La machine robotisée n'est pas envisagée comme une entité autonome et ne se substitue pas à l'expertise de l'homme. « *Le robot est collaboratif, il vient soulager l'opérateur dans les tâches pénibles* », poursuit-il. La machine sert avant tout à assister l'opérateur dans sa tâche en lui apportant de nouvelles capacités fonctionnelles grâce à l'intégration de l'intelligence artificielle, de la réalité augmentée, de la robotique et de l'IoT. Résolument tournée vers une démarche de production durable qui prend en compte l'impératif climatique, l'industrie 5.0 intègre de nouveaux critères comme l'efficacité énergétique des technologies, la priorisation des énergies renouvelables ainsi qu'une démarche d'autonomie. La question énergétique est primordiale pour l'industriel 5.0. Il lui faudra prendre en compte la consommation énergétique des machines, mais aussi celle de l'outil de production global. « *La question des terres rares qui sont présentes dans nombres de composants industriels et de machines devient ainsi cruciale*, indique Stéphane Potier. *Par exemple, les moteurs fabriqués de nos jours sont nettement moins gourmands en terres rares et sont fabriqués à partir de matériaux plus facilement disponibles.* »

Le facteur de résilience est également fondamental pour l'industrie 5.0 qui prend acte d'un contexte macro-économique et géopolitique démontrant chaque jour la nécessité de savoir s'adapter aux chocs. Pour **Marc Bagur**, Head of Human-Machine Performance chez Airudit, il s'agit d'une formidable opportunité stratégique pour les industriels. « *Ceux qui font le choix de donner la priorité aux valeurs humaines plutôt qu'à la technologie adoptent une approche globale et un modèle organisationnel plus performant sur le long*





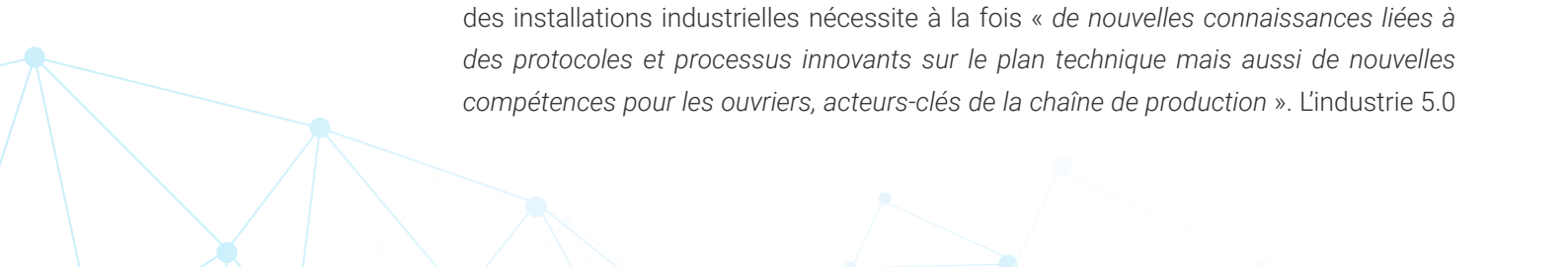
terme. » Il ne s'agit plus uniquement de numériser l'environnement industriel à tout prix, mais de viser « *une robustesse systémique, acceptable socialement, humainement et écologiquement* ». Avant de rappeler que cette exigence « *épouse parfaitement celles des nouvelles générations d'ingénieurs et d'ouvriers pour qui l'alignement avec les valeurs écologiques, la question des ressources énergétiques et la stabilité sociale sont des problématiques cruciales aujourd'hui* ».

Les niveaux de maturité des différents systèmes industriels étant toutefois hétérogènes, il reste difficile d'évaluer précisément quand ce nouveau paradigme sera réellement opérationnel. Et l'industrie 4.0 reste encore relativement récente ...

INDUSTRIE 4.0 VS INDUSTRIE 5.0 : SUBSTITUTION OU COMPLÉMENTARITÉ ?

L'industrie 5.0 n'est pas une itération supplémentaire dans la marche forcée vers le progrès. **Ce nouveau paradigme est à envisager en complément de celui de l'industrie 4.0 et vise à restituer la question de l'innovation technologique dans un cadre précis, centré sur le triptyque humain-durabilité-résilience.** Pour ce faire, l'industrie 5.0 s'appuie sur l'efficacité des technologies de l'industrie 4.0, par exemple pour résoudre des problématiques liées au critère de durabilité. « *Pour baisser la consommation énergétique d'une machine, qu'elle soit récente ou ancienne, il faut d'abord être en capacité de mesurer sa consommation. L'industrie 4.0 nous fournit les outils pour le faire, grâce aux capteurs, compteurs et aux systèmes IoT, souligne ainsi Stéphane Potier. En complément, on peut chercher à optimiser le fonctionnement d'une machine qui consommerait trop d'énergie. D'un côté avec la maintenance prédictive pour influencer la durée de vie de la machine, et de l'autre avec de l'intelligence artificielle pour optimiser les consommations.* » Dans son rapport « *Industry 5.0 – Towards a sustainable, human centric and resilient European industry* », la Commission européenne insiste sur cette complémentarité. **Il s'agit aussi de répondre aux fragilités de l'industrie 4.0 qui évoluait jusqu'alors de manière trop éloignée des enjeux sociétaux.** Le but est de produire des industriels capables non seulement d'être productifs et efficaces mais aussi capables d'inspirer confiance avec des valeurs qui sont celles de l'époque et des challenges qui sont posés par les nouvelles générations.

Avec ces orientations stratégiques, **comment préparer l'industrie de demain ?** Car l'usine 4.0 d'aujourd'hui est très largement numérisée, entre le pilotage des données grâce au Big Data, les mesures précises grâce à l'IoT, la mise en réseau des sites industriels grâce à la 5G ou encore le déploiement d'une capacité de calcul plus forte au pied des machines grâce au edge computing... Elle doit toutefois tenir compte d'un contexte macro-économique et géopolitique particulièrement complexe, marqué par les hausses du prix de l'énergie et l'urgence de la question environnementale. **Préparer une réponse industrielle à ces enjeux civilisationnels requiert donc de flécher les bons investissements aux bons endroits, mais aussi de revoir les processus à toutes les étapes de chaîne de production.** Pour Vincent Nicaise, cette modernisation des installations industrielles nécessite à la fois « *de nouvelles connaissances liées à des protocoles et processus innovants sur le plan technique mais aussi de nouvelles compétences pour les ouvriers, acteurs-clés de la chaîne de production* ». L'industrie 5.0





introduisant une nouvelle couche informationnelle, ce complément suscite des besoins nouveaux ce qui a un impact direct sur la question de la formation du personnel. « *On peut choisir de créer de nouveaux postes, par exemple des référents locaux chargés d'appliquer les nouveaux protocoles de sécurité sur les machines dans les usines disséminées dans le monde, ou faire le choix de faire monter les opérateurs en compétence* », indique-t-il.

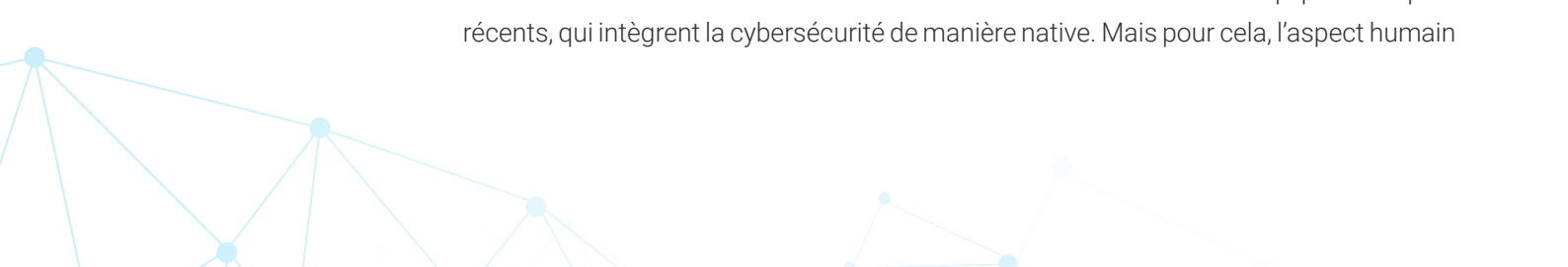
L'occasion d'enfin intégrer la cybersécurité au cœur de l'industrie ?

QUELLE PLACE POUR LA CYBERSÉCURITÉ DANS L'INDUSTRIE 5.0 ?

Au FIC 2022, la question de la cybersécurité en environnement industriel était sur toutes les lèvres. **Car l'usine connectée démultiplie sa surface d'attaque et donc ses problématiques de sécurité.** En effet, la combinaison entre la croissance du nombre de machines robotisées, une interconnexion croissante, une intégration de l'IoT, une dose de réalité augmentée et de nouvelles interfaces homme-machine implique une augmentation du nombre de failles potentielles dans la sécurité des systèmes.

Un rapport signé Claroty indique que 82 constructeurs industriels ont été attaqués lors de la seule année 2021. La même année, les vulnérabilités détectées étaient en croissance nette, passant de 637 à 787. Autant de points d'entrée critiques... Souvent cité en exemple, le système d'exploitation obsolète qui tourne sur des équipements en usine est un des facteurs de vulnérabilité les plus fréquents en matière de cybersécurité industrielle. Ce fameux Windows XP reste un système incontournable pour certains environnements industriels, et nécessite des outils de cybersécurité particuliers pour réduire le risque. Car les conséquences d'une cyberattaque sur un environnement opérationnel ont des impacts décuplés, de l'arrêt complet des chaînes de production à la mise en danger des travailleurs en passant par un impact réputationnel important pour l'entreprise concernée. Sans parler du risque environnemental, auquel est particulièrement sensible l'industrie 5.0.

La question à se poser alors est de savoir **quelles solutions de cybersécurité faut-il utiliser pour protéger les environnements industriels de demain ?** Pour faire face à cet enjeu de sécurité industrielle 5.0, deux scénarios sont étudiés. Le premier est un scénario de « revamping » dans lequel la chaîne de production est actualisée en intégrant la question de la cybersécurité dans les équipements. Dans ce premier scénario, l'installation de « *composants de type firewall est un bon moyen pour réaliser une segmentation des flux et des analyses protocolaires* », estime Vincent Nicaise, tout comme « *le durcissement de la protection des postes de travail, à grand renfort de gestion des ports USB, des réseaux Wifi ou encore des accès* ». Le choix de solutions de cybersécurité souveraines est ici une garantie de transparence et d'éviter tout risque d'exploitation des données à des fins malveillantes. Il s'agit ici de disposer d'un code souverain maîtrisé, qui atténue les risques de compromission et d'attaques par des organismes étrangers. C'est la seule façon de garantir une défense en profondeur sans maillon faible. Le second scénario de cette industrie 5.0 concerne des équipements plus récents, qui intègrent la cybersécurité de manière native. Mais pour cela, l'aspect humain





et le caractère collaboratif seront des clés ; plus encore qu'une sensibilisation, c'est une véritable collaboration à mettre en place entre les équipes dans tous les nouveaux projets. D'un côté, les besoins de sécurité des équipes cyber et de l'autre, les contraintes opérationnelles des équipes OT. Une collaboration nécessaire pour confronter les points de vue et aboutir à des compromis qui répondent aux contraintes cyber et OT.

À condition que les industriels soient prêts pour cette industrie 5.0 cybersécurisée.

INDUSTRIE DE DEMAIN ET MATURITÉ CYBER : LES INDUSTRIELS SONT-ILS PRÊTS ?

Selon une étude d'avril 2023 du cabinet Wavestone, la maturité cyber des grandes organisations en France reste faible : seuls 49% des sondés se déclarent matures. Une moyenne similaire **au niveau du seul secteur industriel, puisque 49,4% des sondés se déclarent matures sur le sujet de la cybersécurité**. Et même si le secteur industriel est en hausse de 4,6 points par rapport à l'année passée, la sécurisation des systèmes industriels fait partie des thématiques en souffrance que les grandes entreprises peinent à traiter (au même titre que la gestion des tiers et la sécurité dans le cloud).

C'est dans le but de contraindre ces organisations à adopter les standards en matière de cybersécurité que des lois et réglementations à l'échelle européenne vont prochainement s'appliquer, comme la directive NIS2 pour la gestion des sous-traitants dans des environnements sensibles ou le Cyber Resilience Act pour le durcissement des produits numériques connectés. Pour Vincent Nicaise, ces textes de lois vont aider les professionnels à adopter un ensemble d'actions concrètes de sécurisation : « *dès la mise en place du Cyber Résilience Act à l'échelle européenne, les fabricants auront par exemple l'obligation d'intégrer des dispositifs de sécurité dans leurs équipements* ». En parallèle, des référentiels comme MITRE ATT&CK ou NIST peuvent également permettre de faire monter en maturité les industriels sur la question de la cybersécurité. Quel que soit le support utilisé, un diagnostic technique complet et sérieux doit permettre d'inviter les industriels à augmenter rapidement leur capacité de résilience face aux attaques dans l'optique de cette industrie 5.0.

« Une personne sensibilisée en vaut deux. Et c'est, je pense, un point qui rejoint les principes de l'industrie 5.0 qui marque la collaboration entre l'humain et la machine. »

Stéphane Potier, responsable de l'offre Cybersécurité OT & IoT chez Advens



De façon opérationnelle, cette capacité peut se traduire par une segmentation des réseaux et des environnements de production, l'utilisation du chiffrement pour les échanges de données sensibles, la mise en place de systèmes d'authentification forte ou encore une surveillance continue des infrastructures sensibles. Dès lors, **il devient absolument crucial de sensibiliser et former les personnels à la détection des cyberattaques**. « Les opérateurs connaissent leurs machines et sont parfaitement conscients des réactions normales de leurs outils, insiste Stéphane Potier. Les sensibiliser à la question de la cybersécurité en leur expliquant les différents types d'attaques et les conséquences potentielles sur leur environnement de travail permet de les rendre vigilant. L'opérateur sera alors en mesure de détecter très rapidement une situation anormale et le remonter à son RSSI ». Il relève toutefois que la sensibilisation en milieu OT n'est pas aussi systématique qu'en milieu IT. « Contrairement à l'adage populaire en cybersécurité qui dit que la principale vulnérabilité se situe entre la chaise et le clavier, je pense au contraire que la solution se situe entre la chaise et le clavier », remarque-t-il. Et de poursuivre : « Une personne sensibilisée en vaut deux. Et c'est, je pense, un point qui rejoint les principes de l'industrie 5.0 qui marque la collaboration entre l'humain et la machine ».

Pour être efficace, l'industrie 5.0 devra donc conjuguer ses principes cardinaux — humain, durabilité et résilience — à une sensibilisation accrue en matière de cybersécurité, doublée d'une intégration de dispositifs robustes au cœur de ses systèmes. En d'autres termes, la cybersécurité devra faire partie intégrante de ce nouveau paradigme industriel pour toutes les entreprises désireuses d'accélérer dans cette direction.



STORMSHIELD



Stormshield, filiale à 100% d'Airbus CyberSecurity, propose des solutions de sécurité de bout-en-bout innovantes pour protéger les réseaux (Stormshield Network Security), les postes de travail (Stormshield Endpoint Security) et les données (Stormshield Data Security).

www.stormshield.com