# USINES INTELLIGENTES : RENFORCER LA CYBERSÉCURITÉ PAR LA CONVERGENCE IT, OT ET IoT

# USINES INTELLIGENTES, LA NOUVELLE FRONTIÈRE DE LA CYBERGUERRE

L'industrie 4.0 et la transition vers les usines intelligentes entraînent des questions complexes en matière de cybersécurité, que les entreprises doivent aborder sans tarder.

Jusqu'à récemment, les fabricants sécurisaient leurs usines à l'aide de la vidéosurveillance, d'alarmes et de volets roulants. Aujourd'hui, la modernisation des usines passe par la connectivité et l'accès aux technologies digitales.

Le nombre de connexions à l'internet industriel des objets (IIOT) devrait par ainsi atteindre 37 milliards d'ici à 2025, sans compter le nombre croissant de pièces connectées qui circulent sur les chaînes de production.

L'IT, l'OT et l'IOT ont une stratégie historiquement distincte, de par la différence d'objectifs métiers, de technologies, de gouvernance et de culture. L'IT se concentre généralement sur l'efficacité, la flexibilité, la gestion de données et la connectivité alors que l'OT met l'accent sur la disponibilité et la stabilité des systèmes et des machines physiques, car des interruptions ou des défaillances peuvent entraîner des conséquences graves sur la production et la sécurité des installations industrielles. Le domaine de l'IOT se concentrera sur l'acquisition, la transmission et l'exploitation de données pour prendre des décisions éclairées.

Pourtant, la protection des données, des systèmes de contrôle industriel et la résilience opérationnelle sont essentielles pour maintenir la sécurité et la stabilité des opérations industrielles. Pour éviter le manque de visibilité et de coordination, les difficultés de partage de données et l'inefficacité opérationnelle, l'enjeu actuel est donc de supprimer les silos de l'organisation classique.

La convergence des technologies de l'information (IT), des technologies opérationnelles (OT) et de l'internet des objets (IoT) permet de plus d'optimiser les opérations et les processus. L'objectif : minimiser les dépenses tout en favorisant l'engagement des employés dans des activités cruciales et créatives plutôt que des tâches répétitives.

# FAIRE CONVERGER L'IT, L'OT ET L'IoT, UNE DÉMARCHE QUI OFFRE DE NOMBREUX BÉNÉFICES

L'IT est responsable de la gestion des données et des systèmes d'information, tandis que l'OT est responsable de la gestion des systèmes physiques tels que les équipements de fabrication dans les usines et les systèmes de contrôle. L'IoT, quant à lui, est un réseau d'appareils interconnectés qui communiquent entre eux afin de récolter, produire et échanger des données permettant d'optimiser les secteurs dans lesquels ces appareils sont déployés.

Faire converger ces trois domaines, permet d'obtenir des avantages considérables. En connectant des capteurs aux machines, par exemple, les données sont automatiquement récoltées et transmettent de l'information immédiatement. Cette transmission d'information en temps réel permet aux organisations d'optimiser les processus de production, adapter la cadence de fabrication, réduire les temps d'arrêt, etc… D'autres avantages notables impactent également le facteur humain grâce à l'automatisation de certaines tâches récurrentes ou fatigantes, permettant ainsi aux collaborateurs de se concentrer sur des tâches intéressantes et à valeur ajoutée.

Mais ce contexte de convergence implique pour les entreprises d'améliorer leurs postures en cybersécurité en reliant l'IT, l'OT et l'IoT, ainsi que leur capacité à répondre aux cybermenaces et à les atténuer. Une attaque sur l'un des domaines peut avoir un effet cascade sur les autres, par conséquent un cadre de sécurité de bout en bout et couvrant les trois domaines est nécessaire.

# CONSTRUCTION D'UNE STRATÉGIE GLOBALE ET IMPLICATION DE L'ENTREPRISE À TOUS LES NIVEAUX

Cette convergence des activités IT, OT et IoT permet de faire des économies pour l'entreprise, en réutilisant les ressources déjà développés, et de donner une vue d'ensemble pour maximiser et renforcer la gestion de la cybersécurité. Cela donne naissance à de **nouveaux défis impactant des périmètres et des niveaux différents qui doivent impérativement être couverts :**

- **Sensibiliser à tous les niveaux de l'entreprise.** Le facteur humain est l'un des plus gros enjeux de cybersécurité, qui offre des portes d'entrée privilégiées par les cyber-attaquants. Tous les collaborateurs de l'organisation, et en particulier ceux qui opèrent l'IT, l'OT et l'IoT doivent donc maîtriser les enjeux de cybersécurité et prendre conscience de l'importance de leur rôle de rempart face aux menaces.

- **Gérer les risques de façon transverse.** Afin d'anticiper au mieux les menaces, l'entreprise doit être en capacité d'avoir de la visibilité sur toutes les portes d'entrée potentielles d'une cyberattaque, que ce soit au sein du domaine IT, OT ou IoT.

- **Maîtriser les standards et normes applicables.** Ces standards et normes doivent être appliqués sur chacun des domaines afin d'assurer une maturité cybersécurité homogène

- **Définir une gouvernance transverse.** La gouvernance doit s'étendre à chacun des 3 domaines pour s'assurer du suivi et de l'application de la stratégie définie par l'entreprise, et doit être accompagnée d'un operating model clair et défini.

- **Savoir gérer les crises et répondre aux incidents.** La gestion de crise et la réponse à incident doivent être optimisées avec un pilotage centralisé pour les 3 domaines afin d'accélérer la mise en place de mesures efficaces dans le temps imparti. Cela garantit une continuité d'activité plus fluide des opérations, ce qui est essentiel pour l'organisation.

- **Faciliter la convergence des domaines.** Une feuille de route claire et définie doit permettre d'avoir une vision long terme des activités existantes et de celles à mettre en place pour faciliter la convergence des différents domaines.

- **Appuyer la stratégie par un par un soutien fort de la direction.** Une équipe de direction présente et communicante sur la volonté de l'entreprise à mettre en place cette gestion homogène de la cybersécurité au sein de l'organisation facilitera l'implication de chaque domaine dans cette transformation.

# ACCÉLÉRATION DE LA MONTÉE EN MATURITÉ CYBERSÉCURITÉ DE L'INDUSTRIE

L'OT en particulier doit accélérer sa montée en maturité en matière de cybersécurité et doit relever des défis qui lui sont propres :

**Construire des équipes incluant la double compétence métier : production industrielle, énergie, transports, …et sécurité** afin de proposer des solutions respectant le cadre réglementaire et normatif de la sécurité des SI Industriels (ANSSI/NIS, IEC 62443, IEC 62351, ISO270xx, NIST-800 …) et adaptées aux contextes métier :

- Respect de la cohérence avec la sûreté de fonctionnement,
- Respect des contraintes opérationnelles,
- Respect des contraintes technologiques (hétérogénéité, obsolescence, performance temps réel, ressources limitées, bande passante réseau …)

De même, pour détecter et réagir en cas d'attaque sans « tout casser », il est essentiel d'impliquer des personnes comprenant le fonctionnement de la chaine de production et des équipements ou réseaux industriels ainsi que les enjeux de cybersécurité. L'objectif : être capable d'analyser finement les évènements et surtout construire un plan de remédiation minimisant l'impact sur la production ou évitant la détérioration d'équipement industriels critiques.

Pour mettre en place ces protections, **quelques étapes sont clés :**

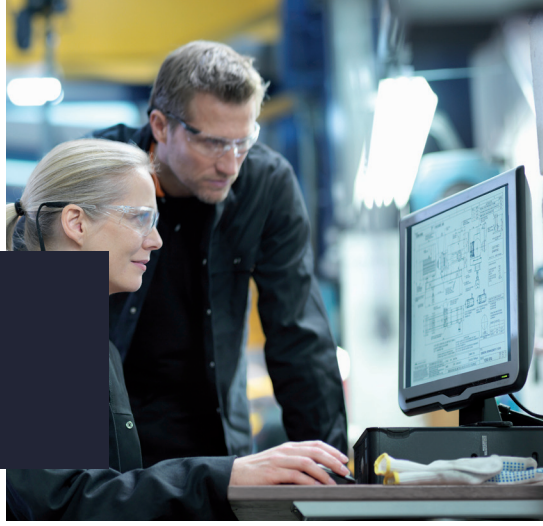
- **Avoir une vision claire de ce que l'on veut protéger** en faisant régulièrement un état des lieux des équipements présents sur le réseau industriel. Comprendre leur diversité permet de mettre en place des protections couvrant le maximum d'entre eux.

- **Mettre en place une cartographie fonctionnelle des équipements,** permettant de comprendre lesquels contribuent à quelle fonction (en s'inspirant pour cela du concept zones et conduits de l'IEC62443). Cela permettra une meilleure réaction en cas d'attaque car l'organisation saura immédiatement quelle fonction est impactée pour ensuite adapter l'action de remédiation.

- **Ne protéger que ce qui est nécessaire,** ou en d'autres termes optimiser les coûts de sécurisation avec une analyse de risque basée sur des scénario d'attaques spécifiques aux usines. Ainsi les risques que l'on accepte et ceux que l'on veut réduire seront identifiés plus rapidement. Ces scénarios doivent être étudié avec des opérationnels de l'usine pour toujours impliquer l'aspect métier à l'aspect cybersécurité tout en sensibilisant les opérationnels et en les embarquant dans le programme.

- **Construire une roadmap réaliste, efficace, progressive et modulable** pour tenir compte au mieux des enjeux business de l'usine. On peut commencer par exemple par déployer des protections n'impactant pas l'architecture de la ligne de production (EPP/EDR sur des end points, dispositif de contrôle des clés USB, outils de détection et asset management en port mirroring), sans oublier de sensibiliser et accompagner les opérateurs. Dans un second temps l'organisation peut modifier peu à peu l'architecture avec l'isolation et la segmentation des réseaux et une gestion plus fine des droits d'accès et privilèges. Pour ce faire, il est judicieux de catégoriser les usines en fonction de leur criticité et de choisir de ne déployer que certaines protections en fonction de la catégorie.

- **Tester une solution avant de la déployer dans les usines** en réalisant un prototypage de la solution dans une usine pilote. Cela permet de comprendre finement la solution et de mieux préparer son déploiement. Il est par ailleurs nécessaire de s'assurer qu'elle est facilement installable et "patchable", avec un maximum d'automatisation permettant d'écrire des procédures de déploiement minimisant l'impact sur la production.



# DIGITALISATION ET SÉCURISATION DES PRODUITS EMBARQUÉS

L'idée reçue résume les objets et produits connectés aux interfaces et communications sans-fil, basées sur des technologies telles que Wi-Fi, Bluetooth/BLE, radio (4G/5G), etc. Pourtant leur sécurisation va bien au-delà et doit également s'appliquer à l'ensemble des interfaces et composants physiques, matériels et logiciels. Les services IT/Cloud/Edge permettant le stockage et le traitement des données doivent aussi être sécurisés.

Les problématiques propres à la digitalisation des produits embarqués doivent également être prise en considération : limitation des ressources disponibles (calcul et stockage), priorisation des contraintes extrêmes de sûreté (safety critical), fonctionnalités de mise à jour, collecte et communication de données, exposition des services user-centric, etc.

Ainsi, concevoir et mettre en œuvre des architectures adaptées prenant en compte des processus de cybersécurité des produits est une tâche complexe, nécessitant une palette variée de compétences cyber, (micro) électronique, ingénierie système et logiciel embarqués.

S'assurer que le système complet intégrant toutes ces dimensions soit protégé de bout en bout avec le niveau de sécurité adapté au contexte doit passer par **plusieurs étapes indispensables :**

- **Maîtriser et appliquer à la lettre le contexte règlementaire.** De nombreuses réglementations sont apparues au fil des années dans les plus grandes majorités des industries : ISO 21434, UL 2900… Ces réglementations s'appuient sur des standards offrant des lignes directrices et impactent concrètement les activités des organisations : interdiction de commercialiser des véhicules connectés et/ou autonomes par exemple.

- **Mettre en place un système de gestion de la cybersécurité (CSMS) et une cartographie des risques** pour : obtenir un niveau de confiance satisfaisant concernant la sécurité du produit développé. Cette gestion des risques, de leur identification à leur traitement, passe par des processus et procédures bien définis et par une prise de conscience collective de l'importance des enjeux de cybersécurité.

- **Couvrir l'ensemble du cycle de vie du produit.** Dès les phases d'architectures, d'implémentation et de test, le produit connecté en cours de conception peut faire l'objet de vulnérabilités. Celles-ci doivent donc être considérées avec la plus grande attention. Les objets et produits connectés peuvent avoir une durée de vie très importante (par exemple plus de 20 ans pour une automobile). Il est donc aussi primordial de mettre en place des processus de gestion des vulnérabilités et de mise à jour pour contrer l'apparition de tout nouveau risque. Le coût induit par la correction d'une vulnérabilité explose par ailleurs de manière exponentielle plus on avance dans le développement du produit, d'où l'intérêt de s'en préoccuper dès le départ…

- **Ne pas sous-estimer la phase de supervision.** Une activité de supervision cybersécurité est nécessaire afin de pouvoir détecter dans un délai acceptable les événements de sécurité affectant un produit (par exemple une flotte de véhicules), et prendre les mesures nécessaires et adaptées. Des services dédiés peuvent être mis en place afin d'analyser les journaux d'événements de sécurité, les investiguer et identifier les sources de ces potentielles failles.

## Auteurs

**Didier Appell**
Directeur de la Cybersécurité OT et IOT
Capgemini

**Ali Bekkali**
Directeur & CTO cybersécurité
Capgemini Engineering

**Marine Boizard**
Consultante Senior Cybersécurité
Capgemini Invent

# A propos de Capgemini

Capgemini est un leader mondial, responsable et multiculturel, regroupant près de 360 000 personnes dans plus de 50 pays. Partenaire stratégique des entreprises pour la transformation de leurs activités en tirant profit de toute la puissance de la technologie, le Groupe est guidé au quotidien par sa raison d'être : libérer les énergies humaines par la technologie pour un avenir inclusif et durable. Fort de 55 ans d'expérience et d'une grande expertise des différents secteurs d'activité, Capgemini est reconnu par ses clients pour répondre à l'ensemble de leurs besoins, de la stratégie et du design jusqu'au management des opérations, en tirant parti des innovations dans les domaines en perpétuelle évolution du cloud, de la data, de l'Intelligence Artificielle, de la connectivité, des logiciels, de l'ingénierie digitale et des plateformes. Le Groupe a réalisé un chiffre d'affaires de 22 milliards d'euros en 2022.

**Get the Future You Want I [www.capgemini.com](http://www.capgemini.com)**