

Sécurité matérielle : quel rôle dans l'essor de l'Industrie 4.0 ?

Erik Halthen, Cybersécurité et systèmes de contrôle industriel, Analog Devices Inc.

Enjeux de l'Industrie 4.0 et implications pour la cybersécurité

L'Industrie 4.0, qui implique la transformation numérique des usines et des installations de production, revêt différentes significations pour les dirigeants du secteur industriel. Par ailleurs, les enjeux de numérisation peuvent avoir un impact considérable sur la cybersécurité à mesure que les appareils utilisés dans les usines gagneront en intelligence et deviendront plus connectés. Par exemple, une entité de fabrication pourra être transformée pour accroître le niveau d'autonomie et de personnalisation, abaisser le coût total d'exploitation (TCO) et augmenter la valeur ajoutée apportée aux clients. Autre possibilité, les fournisseurs de systèmes et sous-systèmes proposeront des outils industriels plus intelligents afin de permettre la prise de décisions en temps réel et faciliter l'interaction autonome des unités de fabrication au sein de vastes environnements multicellulaires et entre différents systèmes d'entreprise. Selon la manière dont vous souhaitez tirer parti des solutions Industrie 4.0, la stratégie adoptée sera fonction de la place qu'elles occupent à l'intérieur de la chaîne de valeur et de leur niveau d'intégration au sein de l'usine.

La digitalisation d'une usine concerne tous les aspects de la chaîne de valeur et affecte directement le chiffre d'affaires d'une entreprise et ses résultats. Les innovations qui ouvrent la voie à nouvelles sources de recettes — nouveaux produits, nouveaux services ou la combinaison des deux — constituent l'un des sujets les plus couramment étudiés. La production numérique, le traitement et l'analyse des données en périphérie exigent de nouveaux produits innovants, tandis que la collecte des métadonnées s'accompagne de nouveaux services qui optimisent le contrôle, la maintenance et l'utilisation. Ces deux aspects de la production numérique existent à différentes étapes de la chaîne de valeur, ce qui a des répercussions directes sur les revenus de l'entreprise. Par ailleurs, les initiatives de réduction des coûts portent sur une meilleure efficacité de la chaîne d'approvisionnement et l'optimisation des performances opérationnelles. Ces améliorations exigent l'adoption de produits et de services plus efficaces dans une même usine. C'est la consommation de nouveaux produits innovants qui est nécessaire pour bénéficier des avantages de l'Industrie 4.0. Selon la façon dont l'entreprise entend tirer parti des solutions Industrie 4.0, la stratégie de cybersécurité évoluera pour adopter et déployer avec succès des solutions numériques dans l'usine.

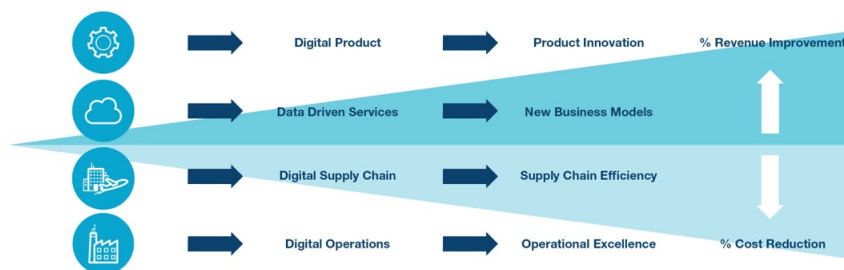


Figure 1. La numérisation des usines transforme tous les aspects de la chaîne de valeur et affecte directement son chiffre d'affaires et ses résultats.

La stratégie de cybersécurité retenue va également s'adapter à la manière dont les solutions numériques sont intégrées en périphérie de la boucle de contrôle industrielle. L'architecture d'automatisation industrielle traditionnelle est particulièrement hétérogène. Elle repose sur le cloisonnement des fonctions de contrôle entre, d'une part, les

appareils de terrain et, d'autre part, les services, applications et systèmes d'information déployés dans l'usine pour assurer sa protection contre les cybermenaces. En outre, les appareils effectivement utilisés sur le terrain sont généralement des solutions point à point qui disposent de capacités d'échange de données et de traitement en périphérie limitées, de sorte que les risques de cybersécurité posés par ce type d'appareil pour le système sont minimales. La transformation de cette architecture classique est particulièrement complexe et devra être abordée progressivement. Les grands utilisateurs de solutions Industrie 4.0 devront déterminer jusqu'à quel point ils souhaitent intégrer de nouvelles technologies dans l'usine et appliquer une stratégie de cybersécurité permettant d'atteindre leurs objectifs. La nouvelle architecture d'automatisation industrielle devrait prendre un aspect sensiblement différent. Les usines sont traditionnellement segmentées en cinq niveaux séparés selon le modèle Purdue ou similaire, un modèle dont l'architecture des usines de demain devrait s'éloigner. Les futurs appareils de terrain associeront des capacités de détection et d'actionnement à des fonctions d'exécution et de contrôle de la fabrication. Ces appareils seront non seulement reliés entre eux au sein d'une architecture connectée intégrée à l'usine, mais également — dans certains cas —, directement raccordés au système de l'entreprise, à Internet et à des services cloud, ce qui augmente considérablement les risques de sécurité pour l'ensemble du système. Quelle que soit la façon dont la future architecture Industrie 4.0 sera perçue, l'objectif final ne pourra être atteint sans une approche progressive et l'application d'une stratégie de cybersécurité adaptée au niveau souhaité d'intégration des solutions numériques dans l'usine.

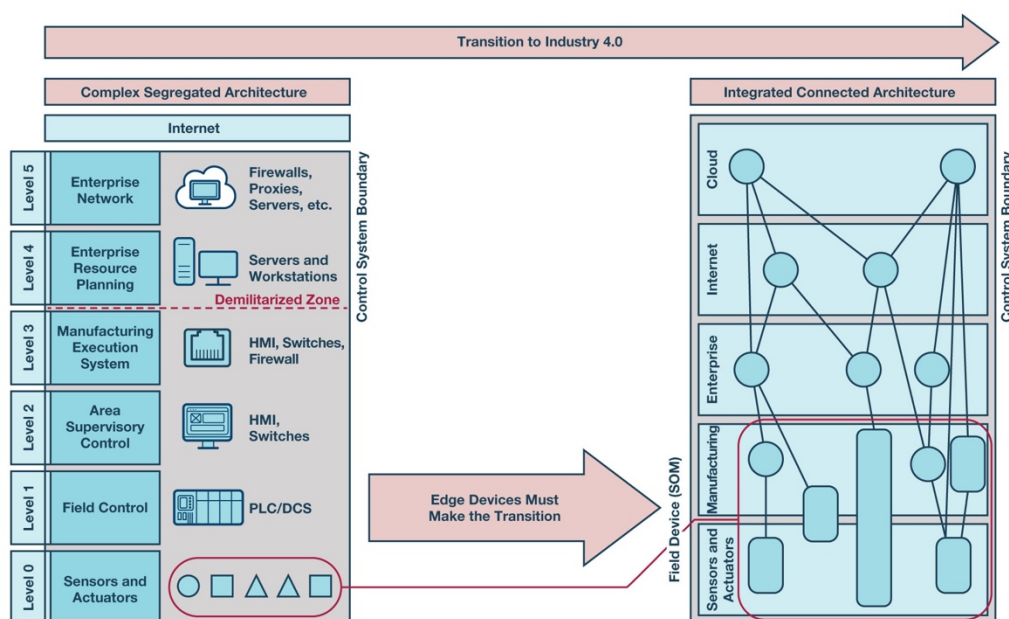


Figure 2. Transition vers une usine entièrement numérisée selon le concept Industrie 4.0.

Trois étapes pour protéger l'Industrie 4.0 contre les cybermenaces

Une fois ces solutions entièrement intégrées, l'environnement Industrie 4.0 pourra prendre différentes formes. D'aucuns pensent que la conception traditionnelle des usines restera en grande partie intacte, tandis que d'autres sont intimement convaincus que l'usine de demain sera méconnaissable selon les standards actuels. En revanche, et personne ne peut le nier, l'usine est en train de changer, et cette évolution ne se fera pas du jour au lendemain. Les raisons de cette transition sont évidentes, la principale étant liée à la durée de vie des appareils de terrain actuels. Ces outils conçus pour fonctionner pendant vingt ans au moins pourraient être exploités pendant longtemps encore. Il est en effet possible de les moderniser afin de les doter de caractéristiques et de

moyens de connectivité supplémentaires, mais ils seront limités par leur conception matérielle, et l'architecture des systèmes d'usine devra compenser leur inadaptation. S'agissant de la cybersécurité, ces appareils seront toujours limités et sources de risques. Un appareil sécurisé nécessite une architecture et une approche de la conception système hautement sécurisées. La modernisation d'un appareil ancien avec des fonctions de sécurité n'est pas une bonne solution, car elle est propice à l'apparition de vulnérabilités. Dans le cadre d'une transition complète vers l'usine numérique, les appareils devront afficher des niveaux de sécurité très élevés pour résister aux cyberattaques sans pénaliser leur aptitude à partager des informations en temps réel et prendre des décisions. La résilience — c'est-à-dire, la capacité à se rétablir rapidement en cas de difficulté — joue un rôle significatif dans la façon dont la cybersécurité est mise en œuvre et dans les étapes nécessaires à la migration vers une Industrie 4.0 protégée contre les risques de sécurité numérique.

Premier obstacle majeur, assurer la conformité aux nouvelles normes et aux bonnes pratiques définies par les industriels de la cybersécurité. La mise en conformité au sein d'une usine en mutation implique une approche originale. En effet, les solutions traditionnelles qui consistent à appliquer les méthodes de sécurité informatique qui isolent, surveillent et configurent le trafic réseau n'apportent pas la résilience requise par le concept Industrie 4.0. À mesure que des appareils vont se connecter et partager des informations en temps réel, de nouvelles solutions de sécurité matérielle s'avèreront nécessaires pour que des décisions puissent être prises en temps réel de façon autonome, tout en maintenant la résilience de l'environnement de production. Et compte tenu de l'évolution de l'approche de la cybersécurité, les entreprises vont devoir s'adapter pour relever de nouveaux défis. De nombreuses entreprises se restructurent pour se doter de compétences en cybersécurité qui seront administrées séparément de la structure technologique traditionnelle tout en étant intégrées aux différentes équipes de projet. Mettre en place une organisation chargée de déployer des solutions de cybersécurité conformes aux normes existantes et aux bonnes pratiques industrielles constitue la première grande étape vers l'Industrie 4.0.

Une fois qu'elles maîtriseront les normes de sécurité émergentes et seront équipées pour faire face aux exigences de sécurité tout au long du cycle de vie de leurs produits et au-delà des entités organisationnelles, les entreprises pourront se concentrer sur l'augmentation de l'autonomie des différentes cellules de production. Mais cette autonomie ne pourra être atteinte que si les appareils disponibles deviennent assez intelligents pour prendre des décisions en fonction des données qu'ils reçoivent. L'approche de la cybersécurité repose sur la conception d'un système basé sur l'utilisation d'appareils en périphérie de réseau qui sont capables de faire confiance aux données à l'endroit même où celles-ci sont produites. C'est ainsi que des décisions peuvent être prises en temps réel et en toute confiance à l'aide d'un système capable de déjouer les cybermenaces, ainsi que d'accepter des informations venant de l'extérieur, d'en évaluer la fiabilité et d'agir de façon autonome.

Le dernier problème porte sur la création d'une usine qui sera connectée au cloud et fonctionnera également en parfaite synchronisation avec d'autres systèmes industriels par l'intermédiaire de services accessibles sur le 'cloud'. À cet effet, il importe de généraliser l'adoption de solutions numériques, ce qui constituera à terme le dernier obstacle à franchir, compte tenu du délai nécessaire pour parachever la transition vers l'usine numérique. Aujourd'hui, les appareils sont déjà connectés au cloud, mais dans la plupart des cas, cette connexion est uniquement utilisée pour recevoir des données, ces dernières étant analysées et les décisions prises à distance, loin de l'usine. Ces décisions peuvent permettre d'accélérer ou de retarder des interventions de maintenance, voire d'affiner un processus automatisé. Aujourd'hui, il est rare que ces décisions soient exécutées à partir du

cloud, dans la mesure où le contrôle a lieu sur site, indépendamment du système de l'entreprise. À mesure que l'usine gagnera en autonomie, il sera plus pertinent de surveiller et contrôler une usine par le biais de services cloud, ainsi que de partager des informations en temps réel entre les différents systèmes de l'entreprise.



Figure 3. Processus d'adoption de l'autonomie en usine.

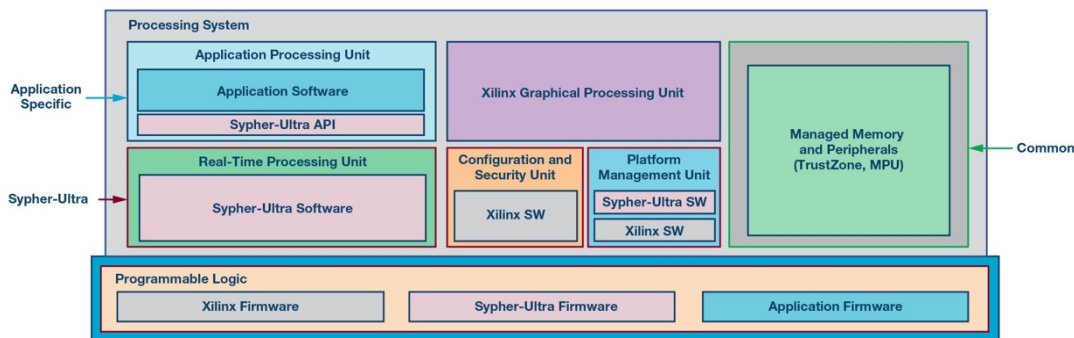


Figure 4. Mise en œuvre de la plateforme Sypher™-Ultra d'Analog Devices

Favoriser l'avènement de l'usine connectée grâce à la sécurité matérielle

La sécurité matérielle est rendue indispensable par la prolifération de normes industrielles qui imposent des niveaux de sécurité accrus aux solutions déployées dans les environnements industriels. L'augmentation des possibilités d'accès et de l'accessibilité aux points de contrôle induit de nouveaux risques contre lesquels les solutions de sécurité informatique traditionnelles sont généralement impuissantes dès lors que la sécurité des périphériques n'est pas associée à un élément matériel sécurisé. Une fois connectés en réseau, les appareils se transforment en autant de points d'accès à l'ensemble du système. Les dommages pouvant être provoqués par l'un ou l'autre de ces points d'accès s'étendent à l'ensemble du réseau et peuvent rendre les infrastructures critiques vulnérables. Les méthodes de sécurité traditionnelles basées sur des pare-feux, sur la détection de logiciels malveillants ou sur l'identification d'anomalies nécessitent une configuration et une actualisation constantes, et sont sujettes à des erreurs humaines. Dans l'environnement que nous connaissons actuellement, il convient de partir du principe qu'un adversaire est *déjà* présent dans le réseau ; pour se défendre contre une telle menace, il convient de suivre une approche de défense en profondeur de type « zero-trust », et pour avoir la certitude que les périphériques connectés fonctionnent comme prévu, un élément matériel sécurisé doit être intégrée au périphérique. Il est essentiel d'installer dès aujourd'hui les modules matériels appropriés dans les appareils pour que la transition vers l'usine numérique puisse avoir lieu demain dans des conditions optimales.

Analog Devices a utilisé la famille de systèmes sur puce multiprocesseurs (MPSoC) programmables sur site (FPGA) Zynq® UltraScale+™ (ZUS+) de Xilinx® pour développer Sypher™-Ultra, une plateforme qui apporte un niveau de confiance accru à l'intégrité des données générées et traitées par son système de chiffrement haute sécurité à plusieurs niveaux de contrôle. Cette plateforme s'appuie sur le socle de sécurité du SoC ZUS+, ainsi que d'autres fonctions de sécurité développées par Analog Devices pour permettre à ses produits de répondre à des exigences de sécurité telles que la norme FIPS 140-2 publiée par l'Institut national américain des normes et des

technologies (NIST —*National Institute of Standards and Technology*), la norme européenne CEI 62443 relative à la cybersécurité des installations industrielles ou, dans le secteur automobile, les modules de sécurité matérielle (HSM) EVITA (*E-Vehicle Safety Intrusion Protected Applications*). La plateforme Sypher-Ultra réside entre la fonction ZUS+ embarquée et l'application finale, fournissant aux équipes de conception une solution monocircuit capable d'exécuter des opérations sécurisées. Afin d'assurer un haut niveau de sécurité, la plateforme Sypher-Ultra utilise un environnement d'exécution de confiance (*Trusted Execution Environment* — TEE) qui fournit une fondation aux données sécurisées au repos et en mouvement. Les fonctions de sécurité sont essentiellement exécutées dans l'unité de traitement en temps réel et l'unité logique programmable, de sorte que les équipes de conception peuvent facilement ajouter leur application à l'unité de traitement applicative. Cette conception évite aux équipes Produits de devoir maîtriser les aspects hautement complexes liés à la conception et à la certification de la sécurité, tout en offrant un haut niveau de confiance lors de l'exécution des tâches requises.

Il est difficile de définir une stratégie visant un niveau de sécurité accru, notamment en raison des contraintes liées aux délais de mise sur le marché qu'impose le rythme exigeant de la transformation numérique des usines. La complexité inhérente à la mise en œuvre de la sécurité exige des compétences et des processus uniques. Avec la plateforme sécurisée d'Analog Devices, les équipes de concepteurs disposent d'une solution fiable pour intégrer la sécurité en périphérie, au plus près de la boucle de contrôle industrielle. En soulageant les concepteurs de produits des complexités de mise en œuvre — conception de la sécurité, certification aux normes de sécurité et analyse des vulnérabilités, par exemple —, les risques encourus et les délais de conception diminuent de façon significative. La solution imaginée par Analog Devices intègre des interfaces API sécurisées d'utilisation aisée sur une plateforme commune où des applications évoluées et à haut niveau de sécurité peuvent cohabiter sur un seul FPGA. La plateforme Sypher-Ultra d'Analog Devices permet d'utiliser en toute sécurité la famille de systèmes sur puce multiprocesseurs Xilinx ZUS+ pour isoler les opérations de chiffrement sensibles et empêcher tout accès non autorisé aux blocs IP confidentiels, ouvrant la voie vers l'usine connectée *via* une sécurité matérielle déployée en périphérie.