

Accélérer l'avènement de l'Industrie 4.0 en élargissant le périmètre de sécurité des systèmes de contrôle industriel

Erik Halthen, directeur du développement des solutions de cybersécurité chez Analog Devices

La cybersécurité des systèmes de contrôle industriel (*Industrial Control Systems* — ICS) pourrait retarder l'adoption du concept Industrie 4.0. De nombreux chefs d'entreprise éprouvent en effet certaines difficultés pour prendre la mesure des défis de cybersécurité associés aux SCI en raison des nombreux facteurs qui contribuent à leur complexité. De plus, les ingénieurs chargés de mettre au point des solutions pour systèmes de contrôle industriel n'ont probablement pas été confrontés à des exigences particulières en matière de cybersécurité au niveau des appareils. Les méthodes traditionnelles utilisées pour sécuriser les SCI reposent sur la limitation de l'accès aux réseaux et aux dispositifs, ainsi que sur la surveillance du trafic réseau au moyen de solutions informatiques. Un chef de produit qui travaille en environnement d'usine considérera sans difficulté que la cybersécurité est un problème d'ordre informatique. Mais à l'heure de l'Industrie 4.0, les méthodes habituelles utilisées pour sécuriser les systèmes de contrôle industriel ne suffisent plus. Si les entreprises ne définissent pas une stratégie leur permettant d'aborder la sécurité des appareils en périphérie de réseau, les enjeux inhérents à la cybersécurité des SCI retarderont l'arrivée de la 4^e révolution industrielle. Pour tirer pleinement parti des avantages de l'Industrie 4.0, la cybersécurité doit être un élément essentiel du modèle industriel. Analog Devices est conscient des défis que ce concept soulève sur ce marché. Alors que le secteur industriel a longtemps affiché une certaine lenteur face aux évolutions, l'adoption de l'Industrie 4.0 a lieu à un rythme record qui dépasse toutes les attentes. Dans ce contexte, la cybersécurité se positionne comme l'un des obstacles majeurs à l'adoption de la 4^e révolution industrielle. Des instructions et des standards de cybersécurité sont en place ou en cours d'établissement pour sécuriser les usines, mais ils ne fournissent aucune orientation quant à la façon d'accélérer le déploiement de ce concept. Notre mission est de permettre à nos clients d'adopter plus rapidement les solutions Industrie 4.0 en élargissant le périmètre sécurisé, ainsi que de faciliter la mise en œuvre de cette sécurité.

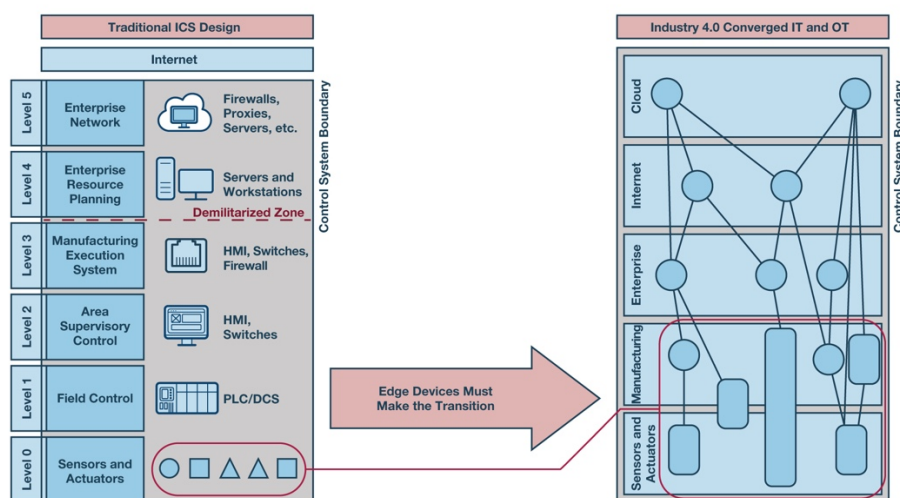


Figure 1. Les appareils connectés en périphérie de réseau requièrent une phase de transition pour évoluer vers l'Industrie 4.0.

L'Industrie 4.0 transforme la cybersécurité des systèmes de contrôle industriel

Le concept Industrie 4.0 est en train de modifier le problème de la cybersécurité des SCI pour une bonne et simple raison. Par sa nature même, l'Industrie 4.0 a pour vocation d'accroître l'accès aux appareils en usine, ainsi que l'accessibilité des processus de contrôle. En d'autres termes, ce concept vise à faciliter l'accès aux données pour augmenter la transparence, réduire la planification du réseau, minimiser les investissements en capital (CapEx) et les dépenses d'exploitation (OpEx), améliorer la bande passante et optimiser l'interconnexion des machines. Or, cette amélioration de l'accès et de l'accessibilité des processus de contrôle nécessite une modification de l'évaluation des risques de cybersécurité pour les systèmes industriels. Les solutions de cybersécurité associées aux SCI doivent s'adapter à l'évolution des risques, et les contre-mesures traditionnelles appliquées au système (pare-feu et positionnement d'un appareil derrière une « porte verrouillée », par exemple) vont à l'encontre des objectifs de l'Industrie 4.0. En d'autres termes, la sécurité des appareils devra être renforcée pour fonctionner en toute sécurité. Et pour contribuer à la fiabilité des données (« confiance ») et à la sécurité des opérations, des fonctions de gestion d'identité et d'intégrité devront être intégrées au cœur de tout dispositif déployé sur le terrain.

De nombreuses normes industrielles facilitent l'application de la sécurité dans les systèmes de contrôle industriel. Par exemple, le National Institute of Standards and Technology (NIST) propose des recommandations en matière de sécurité dans le cadre de la gouvernance américaine, tandis que le projet de norme CEI 62443 couvre la sécurité pour le marché international avec une gouvernance en Europe. Ces deux normes majeures définissent des lignes directrices utiles pour mettre en œuvre des procédures de sécurité et évaluer le niveau de sécurité des systèmes de contrôle industriel ; cependant, elles ne fournissent aucune indication quant à la façon d'accélérer l'adoption de l'Industrie 4.0. La norme CEI 62443 ne contient actuellement aucune ligne directrice portant sur la mise en œuvre de la sécurité sur les couches basses des automates programmables et par ailleurs, un groupe de travail ISA99 a récemment été mis en place pour aborder la question de la cybersécurité dans les couches inférieures de l'usine dans le cadre de la norme CEI 62443. Aujourd'hui, pour atteindre un niveau de sécurité acceptable, des contre-mesures doivent être appliquées aux appareils qui n'atteignent pas un niveau de sécurité suffisant. Ces contre-mesures reposent généralement sur des méthodes telles que les pare-feux pour limiter l'accès et isoler les dispositifs vulnérables. À l'avenir, les dispositifs devront atteindre des niveaux de sécurité plus élevés pour permettre la transition vers l'Industrie 4.0.

Analog Devices étend le périmètre de cybersécurité des systèmes de contrôle industriel

Analog Devices occupe une position idéale pour étendre ce périmètre de sécurité. Notre cœur de métier se situe à la périphérie physique, à l'endroit où le monde réel est traduit en signaux numériques et où les données voient le jour. Ce positionnement nous permet d'injecter de la « confiance » dans les données en leur fournissant une identité et de l'intégrité beaucoup plus tôt dans la chaîne du signal, mais également de modifier la définition de la périphérie sécurisée. Traditionnellement, la sécurité en périphérie se situe au niveau des passerelles, des automates logiques programmables (PLC), voire des serveurs, dans le cadre de la sécurité des systèmes de contrôle industriel. Ce point de vue qui rappelle l'approche historique de la cybersécurité « informatique » des usines est encore bien vivant dans l'industrie. La perspective de déplacer la périphérie de sécurité « plus bas » dans la chaîne du signal est séduisante, en ce sens où elle permet de prendre des décisions prises à partir de ces données avec une confiance accrue. Plus l'identité et l'intégrité seront établies tôt dans la chaîne du signal, plus le niveau de confiance accordé aux données qui étayent les décisions sera élevé.

La cybersécurité des systèmes de contrôle industriel ne peut être prise en charge par une solution unique, de sorte qu'une approche de la défense en profondeur doit être adoptée et appliquée en fonction des risques évalués. La stratégie d'Analog Devices vise à étendre la profondeur de la cybersécurité des SCI à mesure qu'Ethernet est adopté en périphérie. La mise en œuvre de l'Industrie 4.0 exige des usines qu'elles adoptent de nouvelles méthodologies de connectivité, ce qui signifie qu'Ethernet continuera de jouer un rôle croissant dans les systèmes de contrôle industriel. La stratégie de sécurité d'Analog Devices consiste à se concentrer sur l'endroit où opère la connectivité Ethernet, car cette situation modifie considérablement l'impact potentiel des dispositifs connectés au réseau sur le système. Notre actuelle famille de solutions Ethernet industrielles et de solutions de synchronisation temporelle TSN (*Time-Sensitive Networking*) a été au centre de nos initiatives de développement sur le plan de la sécurité. À court terme, le circuit de commutation fido5000 et la

plateforme RapID®, qui offre une connectivité multiprotocoles à 2 ports, seront dotés de fonctions de sécurité qui engloberont les fonctions de génération et de gestion des clés, de démarrage sécurisé, de mise à jour sécurisée et d'accès mémoire sécurisé pour une protection complète contre les attaques visant le réseau. La feuille de route de cette famille de produits comprend des solutions monocircuit qui embarquent une racine de confiance matérielle, une fonction de gestion sécurisée du cycle de vie des périphériques, une fonction de communications sécurisées/authentification mutuelle et une protection contre les tentatives de falsifications. À mesure que l'industrie adopte des capteurs de plus en plus intelligents, la connectivité s'étendra à un niveau inférieur dans les usines, avec à la clé des exigences de sécurité supplémentaires au niveau des appareils. Analog Devices s'engage à développer un portefeuille de produits sécurisés qui facilitent l'adoption de solutions de sécurité pour SCI et intègre la confiance en périphérie en vue d'accélérer l'adoption de l'Industrie 4.0.

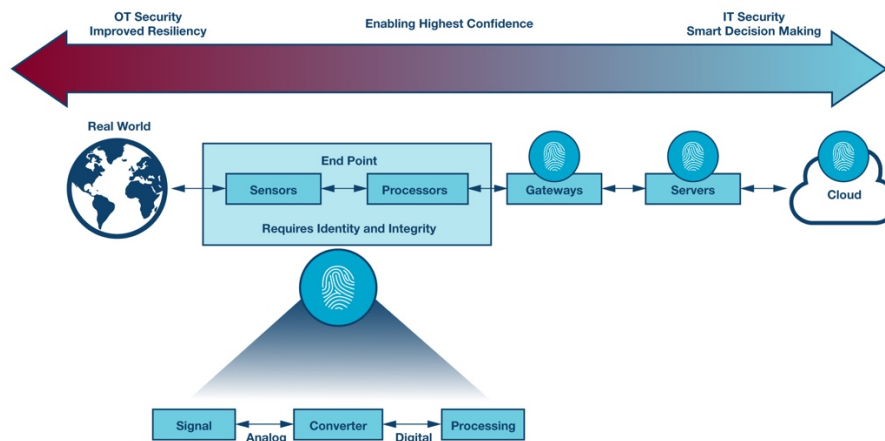


Figure 2. Accroître le niveau de confiance décisionnel à l'endroit où a lieu la conversion entre signaux physiques et numériques.

À propos de l'auteur

Dans le cadre de l'acquisition de Sypris Electronics par Analog Devices en 2016, Erik Halthen apporte à la société son expertise des solutions de cybersécurité. Au sein du centre d'excellence en cybersécurité d'ADI, Erik assume le rôle de directeur du développement du marché et met à profit l'expérience acquise en tant que gestionnaire de programmes pour développer des solutions de sécurité de pointe qui répondent aux principales attentes des secteurs de l'automobile, de l'industrie et de l'Internet des objets. L'expérience accumulée à la tête d'équipes chargées de développer et d'intégrer de nouvelles technologies de sécurité s'ajoute à une solide expérience commerciale pour, en partenariat avec ses clients, révolutionner la façon dont la sécurité de l'Internet des objets est assurée de la périphérie jusqu'au cloud.