Rockwell Automation

Sécuriser la quatrième révolution industrielle

L'approche zéro confiance pour sécuriser la transformation numérique des technologies de la production

Introduction

La transformation numérique représente autant un formidable moteur de progrès et d'efficacité qu'une rupture économique susceptible de bouleverser les rythmes de l'innovation et du développement des entreprises.

L'adoption des technologies numériques pour transformer les produits, services et entreprises requiert une connaissance et un contrôle accrus, afin d'améliorer l'efficacité, notamment à travers les flux de données. Ces approches redéfinissent souvent l'expérience des différents intervenants, notamment des clients, et peuvent inclure des changements de modèles d'exploitation qui affectent la sécurité des actifs numériques.

Dans le domaine des technologies de la production (OT), la transformation numérique induit deux changements majeurs :

- Les systèmes OT se connectent à des réseaux auxquels ils ne l'étaient pas auparavant, pour extraire de nouvelles données sur les opérations. Par définition, ces systèmes sont situés à la « périphérie » de l'infrastructure et doivent donc être déployés, sécurisés et gérés comme des terminaux.
- Des applications logicielles orientées données sont en cours de déploiement dans des environnements OT, où ces nouvelles données peuvent être exploitées au mieux. Le traitement des données peut aboutir à des contraintes de latence, du fait de leur volume élevé et de la bande passante disponible. Pour résoudre ce problème, les applications sont aussi déployées, sécurisées et gérés sur le terminal.

Par ailleurs, les entreprises de production sont confrontées à de nombreux autres défis courants, qui impactent la sécurité et doivent être relevés pendant le parcours de modernisation.

1. Les capteurs de processus, y compris plus récents, n'intègrent pas la sécurité ni les mots de passe. Selon un exemple récent, un fournisseur de premier plan a expédié 3 000 capteurs neufs aux Émirats arabes unis sans mots de passe.
2. Les prestataires en sécurité des réseaux informatiques assurent généralement celle-ci aux niveaux 2-7, ce qui convient à la majorité des réseaux informatiques. Mais les menaces OT se matérialisent souvent au niveau 0-1, où la télémétrie n'est pas surveillée et où, par conséquent, les menaces ne sont pas détectées.
3. L'attribution de la responsabilité finale de la sécurité OT demeure floue. Sur le papier, elle peut relever des CISO et de nombreuses entreprises industrielles agissent pour qu'il en soit ainsi. Toutefois, les responsables des ateliers sont propriétaires de l'espace et rechignent à transférer le contrôle aux CISO, car ceux-ci ont souvent une compréhension limitée des opérations des ateliers.
4. Les directives de sécurité des pipelines de l'agence américaine TSA (Transportation Security Administration) n'abordent pas les systèmes de commande, notamment les capteurs. Pourtant, sous la Cybersecurity and Infrastructure Security Agency (CISA), la TSA est propriétaire du réseau d'énergie complet.

5. La norme 1164, « Pipeline Control Systems Cybersecurity » (août 2021) de l'American Petroleum Institute, a effectivement exclu les capteurs de processus (clause 6,6.5.4 (b)) en stipulant que l'inventaire ne doit pas inclure les instruments individuels non connectés au réseau.

Malgré l'utilité d'outils tels que l'outil MITRE ATT&CK et la méthodologie CVE, il faut aller plus loin. Par exemple, MITRE ATT&CK ne prend absolument pas en compte les capteurs de processus et les autres dispositifs de système de commande. De même, la méthodologie CVE pour les vulnérabilités logicielles n'a pas d'équivalent pour les composants matériels des systèmes de commande.

La tâche consistant à comprendre les normes actuelles et à combler leurs lacunes par rapport à des menaces OT qui évoluent plus rapidement ne s'adresse pas aux âmes sensibles.

D'autre part, la réussite d'une transformation numérique sécurisée passe obligatoirement par une collaboration entre les technologies de l'information et les technologies de la production sur les questions du déploiement, de la sécurité et de la gestion des changements de processus. Cette approche garantit, au final, la réalisation des améliorations de productivité souhaitées, leur sécurité, leur fiabilité et leur conformité.

Obstacles courants de la transformation numérique

Certaines raisons courantes expliquent l'échec des entreprises à atteindre leurs objectifs de transformation numérique. Ces problèmes peuvent être amplifiés par la transformation des technologies de la production.

L'intégration des systèmes OT isolés dans le paysage global.

Les 'îlots d'automatisation' dans l'infrastructure OT traditionnelle ne sont pas conçus pour permettre l'accès aux données. Par ailleurs, l'inventaire des environnements industriels étant insuffisant, les éléments connectés dans l'environnement sont mal répertoriés.

Les capteurs de processus ne disposent pas d'une sécurité intrinsèque, alors qu'ils sont omniprésents, fournissent des informations aux systèmes de commande et de sûreté, et facilitent les décisions des opérateurs. Des défaillances catastrophiques peuvent se produire. Cela a souvent eu comme conséquence que la question de la sûreté, qui est bien appréhendée par les services d'ingénierie, a pris le pas sur la sécurité, que les ingénieurs ont eu tendance à voir comme une attribution des services informatiques.

À leur tour, les services informatiques ont eu tendance à ignorer la sécurité des capteurs de processus et à la voir comme relevant de l'ingénierie et en dehors de leurs attributions.

Toutefois, au niveau des capteurs de processus, la sûreté et la sécurité ne sont qu'un seul et même problème.

Une stratégie inadaptée ou mal définie.

La stratégie de transformation numérique doit englober des efforts coordonnés, afin de définir des résultats mesurables et établis pour les résultats économiques clés, tout en préservant la sécurité des actifs numériques critiques et en assurant la conformité normative.

Une feuille de route, à terme porteuse de valeur.

La réussite du projet repose essentiellement sur une feuille de route à court et à long termes, laquelle concrétisera la valeur de la transformation numérique en se fondant sur les résultats économiques et non seulement sur la technologie.

Des acteurs clés aux objectifs différents.

La transformation numérique exige un changement de culture de l'entreprise. Il doit y avoir un alignement des mentalités des responsables IT et OT, afin que les deux groupes puissent réaliser les objectifs économiques du projet.

La première étape consiste à identifier et prioriser les éléments de l'entreprise à protéger, à savoir les données, les actifs, les applications et les services (DAAS).

Gros plan sur les capteurs de processus

Les systèmes existants en service depuis plus de 20 ans ne sont souvent pas conçus pour des environnements IoT forts de milliers de capteurs de processus et induisent des vulnérabilités en matière de sécurité. Sans une planification et des contrôles appropriés, les démarches de modernisation peuvent multiplier les cyberrisques.

Pourquoi est-il si important de sécuriser les capteurs de processus ?

Selon un récent rapport, « les cybermenaces augmentent et la transmission des données des capteurs pourrait être piratée. Il convient de comprendre en quoi des données de capteurs piratées affectent les performances de commande [des bâtiments]. Une situation type pourrait inclure la modification de données de capteurs par des pirates et leur envoi à des boucles de commande, d'où un déclenchement d'actions de commande extrêmes. »

Voici quelques cyber-incidents qui ont fait appel à des capteurs de processus :

- Un défaut de fonctionnement d'un barrage a entraîné un effondrement suite à des relevés de niveau bas erronés.
- Un capteur a provoqué le relâchement de près de 10 millions de litres d'eaux usées non traitées.
- Une soupape de sécurité dans une centrale nucléaire ne n'est pas relevée car le capteur de pression n'a jamais atteint son point de consigne.
- Une défaillance de capteur de tension dans une centrale à cycle combiné en Floride a provoqué une fluctuation de la charge de 200 MW à la centrale et, par conséquent, une fluctuation de 50 MW en Nouvelle Angleterre.
- Des relevés erronés de capteurs ont provoqué des explosions de cuves d'exploitations agricoles.
- Des relevés erronés de capteurs ont provoqué des catastrophes aériennes.
- Des relevés erronés de capteurs ont provoqué des explosions dans des raffineries.

Lorsque les capteurs de processus sont dépourvus de cyber-sécurité, d'authentification ou de cyber-journalisation, il est impossible de savoir si des incidents tels que ceux cités sont liés à des actes malveillants maquillés en accidents.

Il convient de se poser trois questions importantes sur la sécurité, afin de comprendre les vulnérabilités inhérentes aux capteurs de processus :

1. Faut-il une présence physique pour compromettre le capteur ?
   Non, cela peut être effectué à distance.
2. Quel degré de dommages peuvent résulter d'une cyber-attaque menée sur un capteur ?
   L'étalonneur calibre un capteur à la fois, mais se connecte de manière non sécurisée à Internet. Les systèmes de gestion des actifs (AMS) ont accès à des milliers de capteurs. Entre temps, l'AMS peut avoir des connexions non sécurisées à Internet et est souvent connecté aux progiciels de gestion intégrés (ERP) d'entreprise. Colonial Pipeline constitue un exemple réel d'une défaillance catastrophique liée à des problèmes de capteurs.
3. Que se passe-t-il lorsque des données de capteurs compromises sont envoyées dans le cloud pour des applications d'analyse big data, d'IoT ou d'Industrie 4.0 ?
   Les données de capteurs sont censées ne pas être compromises.

Les entreprises de production doivent corriger les déficiences de capteurs de processus dans le cadre de leurs programmes de transformation numérique sécurisée et comprendre comment des acteurs malveillants peuvent interrompre, dégrader, voire endommager et détruire l'infrastructure. Elles doivent appréhender les risques et les coûts, ainsi que les mesures à adopter pour éliminer les vulnérabilités.

L'approche zéro confiance est une stratégie disponible pour éliminer l'excès de confiance et le risque autour des capteurs de processus. L'approche zéro confiance assure une visibilité intégrale et une validation continue de la fiabilité de chaque 'entité' dans une entreprise, qu'il s'agisse de données, d'applications, de services ou de dispositifs incluant des capteurs de processus, en commençant à supposer un niveau de confiance nul.

Planification de la transformation numérique sécurisée

Avec tous les défis de la transformation numérique sécurisée amplifiés dans les environnements OT, il n'y a rien d'étonnant à ce qu'en matière de modernisation, les entreprises industrielles soient à la traîne par rapport aux entreprises plus axées sur l'informatique.

La bonne nouvelle : il existe des voies éprouvées vers la réussite.

La transformation numérique sécurisée dans les technologies de la production nécessite quelques stratégies clés :

- Une approche zéro confiance
- Les solutions numériques modernes appropriées
- Un changement des détenteurs de propriété dans les entreprises
- Une amélioration des normes de conformité autour d'actifs aussi répandus et vulnérables que les capteurs de processus. Et, en remplacement de ces améliorations, une correction directe de ces lacunes

Même si chacun de ces points est important, la suite de ce document met l'accent sur l'approche zéro confiance.

L'approche zéro confiance

Cette stratégie est excellente pour déployer des technologies de transformation numérique sécurisée dans les environnements industriels. Elle favorise de nouveaux profils d'utilisateurs, des modèles d'implication des clients, des adoptions rapides et de nouveaux dispositifs et capteurs IoT et OT, au fur et à mesure que la transformation progresse, le tout sous le parapluie de la cybersécurité.

L'approche zéro confiance repose sur cinq principes de conception, lesquels peuvent être intégrés aux cinq étapes essentielles suivantes nécessaires pour promouvoir la transformation numérique sécurisée dans une entreprise :

1. Définition des actifs et des surfaces à protéger
2. Cartographie des flux de transactions
3. Conception de l'architecture
4. Application de la politique
5. Surveillance et maintenance continues

Définition des actifs et des surfaces à protéger. Selon son inventeur John Kindervag : « l'approche zéro confiance est une stratégie d'alignement de la stratégie de l'entreprise avec les pratiques de cybersécurité. » En mettant l'accent sur les résultats économiques, la sécurité peut être perçue comme un moteur et non comme un inhibiteur.

La première étape consiste à identifier et prioriser les éléments de l'entreprise à protéger, à savoir les données, les actifs, les applications et les services (DAAS). Les éléments DAAS sont hautement critiques pour l'entreprise et chacun doit constituer une priorité. Viennent ensuite les surfaces à protéger, par ex. les commandes de système de commande, les réseaux informatiques, les bases de données d'informations clients, les données de propriété intellectuelle, etc.

- **Données** : Classez les données selon leur ordre d'importance dans votre entreprise, leur valeur potentielle pour des pirates et leur subordination à des réglementations. La documentation d'un plan sur la gouvernance des données, globalement et en particulier au sein d'une surface à protéger, signifie que l'entreprise peut identifier, classer, transmettre, archiver et supprimer des données avec des contrôles de sécurité efficaces.
- **Applications** : Appréhendez les applications qui utilisent des données sensibles ou du code propriétaire ayant une valeur potentielle pour un acteur malveillant. La conception doit être réalisée de l'intérieur vers l'extérieur. Cartographiez les modes de fonctionnement souhaités des systèmes et les modes d'interaction des différents composants de l'élément DAAS avec d'autres ressources sur le réseau. La compréhension des flux de trafic sur le réseau, en particulier pour les données dans la surface à protéger, aidera à élaborer une politique de sécurité des données à l'intérieur des applications et entre elles.
- **Actifs** : Dressez un inventaire détaillé de tous vos dispositifs, à savoir ordinateurs portables, téléphones mobiles, équipements de fabrication, API, dispositifs IoT tels que capteurs de processus, et autres actifs connectés au réseau. Ainsi, vous savez quoi inclure dans votre surface à protéger.
- **Services** : Identifiez tous les services réseau stratégiques à protéger, notamment Active Directory, DHCP et la messagerie. Les comptes de services en général doivent avoir des comportements connus et des privilèges de connexion limités. Ils ne doivent jamais essayer d'accéder directement à un contrôleur de domaine ou à un système d'authentification, et toute anomalie de comportement doit être identifiée rapidement et donner lieu à une escalade immédiate.

En focalisant les cyberdéfenses autour de chaque surface à protéger, laquelle est priorisée selon son importance dans l'entreprise, il est possible de créer des périmètres de défense significativement plus petits et gérables que la surface d'attaque d'entreprise habituelle, qui pourrait être considérée comme l'ensemble d'Internet.

Chaque entreprise sera confrontée à de multiples projets de transformation numérique, avec les surfaces à protéger correspondantes. En commençant par une initiative de transformation au départ réduite, mais stratégique, efficace et mesurable, l'entreprise peut se familiariser avec la cybersécurité zéro confiance et mettre en place un cadre pour la réussite de projets ultérieurs.

Cartographie des flux de transactions. Dans les environnements industriels, les actifs réseau sont souvent mal inventoriés, d'où des vulnérabilités concernant les éléments censés être, et actuellement, connectés dans l'environnement. Ces systèmes ont souvent connu une croissance organique, ce qui produit des lacunes fréquentes dans la connaissance de la conception. Ainsi, des dispositifs soi-disant sécurisés peuvent constituer des points d'entrée non protégés sur les réseaux à partir d'Internet.

La conception appropriée d'un réseau se déroule du centre vers l'extérieur. Il est critique de comprendre le fonctionnement requis des systèmes et les interactions de différents composants DAAS avec d'autres ressources sur le réseau. En cartographiant les flux de trafic et les interdépendances, en documentant les interactions mutuelles de ressources spécifiques et en intégrant ces interdépendances dans des politiques et contrôles de sécurité, vous êtes à même de déterminer les types et niveaux de protection requis.

La cartographie des flux de transactions et des interdépendances DAAS, en particulier concernant les éléments recoupant vos surfaces à protéger, assure de meilleures protections sans interrompre accidentellement des applications, services ou opérations liés. Elle offre aussi une meilleure compréhension et les informations nécessaires pour des décisions plus avisées à l'étape suivante.

Conception de l'architecture. Une fois la surface à protéger définie et les flux cartographiés, l'architecture zéro confiance nécessaire apparaîtra généralement clairement.

Les meilleures pratiques en matière d'approche zéro confiance dictent de placer les contrôles de sécurité au plus près des éléments DAAS à protéger. Pour le reste, l'architecture zéro confiance ne repose pas sur un modèle universel. Elle fait plutôt appel à de multiples types d'outils et de politiques de cybersécurité, spécifiques à chaque surface à protéger, pour atteindre ses buts. Les entreprises doivent déployer et intégrer un mix de possibilités qui améliorent la gestion des identités et des accès, les contrôles d'accès, la segmentation du réseau, la création de micro-périmètres, et plus encore, selon les besoins de l'élément DAAS dans chaque surface à protéger.

La conception de réseaux zéro confiance doit, par conséquent, reposer sur le flux des transactions à travers un réseau, vers et à partir des éléments DAAS de la surface à protéger. Elle doit aussi prendre en compte les modes d'accès des utilisateurs et applications aux données de la surface concernée. En ayant un flux optimisé à l'esprit, il est possible de prendre des décisions concernant l'emplacement de la segmentation et des micro-périmètres, en utilisant des appareils physiques et/ou virtuels.

Application de la politique. Au cours de cette quatrième étape, les règles de la politique sont rédigées pour la passerelle de segmentation, sur la base du comportement escompté des données et de l'utilisateur ou des applications interagissant avec celles-ci.

Une fois que l'équipe de conception a déterminé le flux de trafic optimal, l'étape suivante consiste à déterminer le mode d'application des politiques de contrôle des accès et d'inspection au niveau passerelle de segmentation. La politique doit débuter par une approche sommaire et gagner en granularité, à mesure que les besoins des utilisateurs et les exigences de l'entreprise sont mieux appréhendés au cours de la transformation numérique et du développement de la vision de l'entreprise.

Un principe clé de l'approche zéro confiance consiste à limiter les accès sur la base du besoin strictement nécessaire (principe du privilège le plus bas) et en appliquant à la lettre ce contrôle des accès. Pour définir ces règles, l'équipe de conception doit avoir une connaissance détaillée des utilisateurs et des données auxquelles ils accèdent, avec des informations contextuelles.

Il ne suffit plus de connaître l'adresse source, l'adresse de destination, le port et le protocole. Les équipes de sécurité doivent comprendre l'identité supposée des utilisateurs, ainsi que l'application, laquelle sert souvent de proxy pour le type de données dans la passerelle de segmentation moderne.

Pour qu'une ressource puisse dialoguer avec une autre, une règle spécifique doit autoriser ce trafic. L'établissement de cette règle exige de répondre aux questions suivantes :

- Qui doit disposer d'accès ? Cela définit l'identité supposée.
- Quelle application pour quelle ressource ? Quelle application l'identité supposée utilise-t-elle pour accéder à une ressource à l'intérieur de la surface à protéger ?
- À quel moment l'utilisateur doit-il disposer d'un accès ? À quel moment intervient la tentative d'accès à la ressource ?
- À partir de quel emplacement doivent-ils bénéficier de l'accès ? Quelle est la destination de ce paquet de données ?
- Quelle est la raison de cette action ? Pourquoi ce paquet essaie-t-il d'accéder à cette ressource au sein de la surface à protéger ? Il y a un lien avec la classification des données, à savoir les métadonnées consommées automatiquement à partir des outils de classification des données augmentent la granularité de votre politique.
- Comment protéger cet aspect ? La protection passe par la compréhension du mode d'accès de l'identité supposée d'un paquet à la surface à protéger via une application spécifique.

Surveillance et maintenance continues. Il s'agit de la cinquième étape de mise en œuvre de l'approche zéro confiance.

Ce processus itératif consiste à examiner en continu tous les journaux internes et externes à travers la couche 7, en ciblant les aspects opérationnels de l'approche zéro confiance. L'envoi d'autant de données télémétriques que possible concernant l'environnement fournit de nouvelles informations sur les modalités d'amélioration de la sécurité et de l'efficacité au fil du temps, et concernant l'acquisition de nouvelles connaissances utiles pour transformer de nouveaux domaines.

Les environnements technologiques sont exposés à une myriade de menaces. Les entreprises doivent maintenir des capacités de surveillance continue pour être assurées de savoir ce qu'il se passe dans leurs environnements. Ensuite, plus un réseau est attaqué, plus il deviendra fort, du fait du renforcement des politiques de sécurité et de l'information des conceptions itératives avec des optimisations architecturales qui rehaussent davantage la sécurité.

Normes de sécurité industrielle

Les entreprises de production (OT) s'appuient sur quatre normes de sécurité principales.

- CEI 62443 Sécurité des systèmes d'automatisation et de commande industrielles (IACS)
- Department of Homeland Security/The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)
- NIST 800-82 Industrial – National Institute of Standards and Technology
- Department of Homeland Security/Idaho National Lab

Chaque norme repose sur une architecture de sécurité de défense en profondeur qui présente intrinsèquement des vulnérabilités. Qui plus est, ces normes ne sont pas réellement une stratégie, mais plutôt un déploiement de tactiques pour résoudre des vulnérabilités ponctuelles spécifiques à travers une solution de contrôle ou de produit, basée sur le concept de zone démilitarisée industrielle (IDMZ). Celle-ci est une zone tampon au sein d'un établissement de production ou de transformation, entre les systèmes d'entreprise et les systèmes de commande ayant différentes exigences de sécurité et n'ayant aucune confiance intrinsèque entre eux.

La transformation numérique modifie le facteur de confiance pour les deux systèmes. Aujourd'hui, la confiance doit être attentive, contextuelle et adaptative si l'interaction des nouveaux modèles d'entreprise développés via la transformation numérique souhaite réussir et fournir les résultats positifs escomptés.

Rockwell Automation est en phase avec la norme CEI 62443 Sécurité des systèmes d'automatisation et de commande industrielles (IACS), et avec l'approche zéro confiance. Les principes de conception de l'approche zéro confiance s'accordent bien avec les exigences de la norme CEI 62443, en simplifiant la conformité tout en renforçant les défenses face un paysage des menaces en constante évolution.

Résumé

La transformation numérique sécurisée dans les technologies de la production peut exploiter l'approche zéro confiance en tant que cadre clé pour garantir le lancement des projets de transformation avec la cyberprotection appropriée en place.

L'approche zéro confiance et la transformation numérique sécurisée sont deux voies nécessitant une mise en œuvre incrémentielle. Comme la transformation numérique modifie le facteur de confiance entre les systèmes de commande et les systèmes d'entreprise, il convient d'exécuter un plan de transformation numérique sécurisée, lequel utilise des stratégies complémentaires pour atteindre une meilleure efficacité et une plus grande productivité, avec une visibilité complète de la cybersécurité et une mise en application qui englobe chaque point de connexion du réseau.

La planification d'un projet initial de transformation numérique sécurisée et l'identification, la priorisation et la protection des éléments DAAS au sein de chaque surface à protéger du projet aideront l'entreprise à générer rapidement une valeur à partir de ses efforts et établiront un modèle de cyberprotections pour l'entreprise pendant la transformation.

Une approche globale

Rockwell Automation est hautement spécialisé dans la transformation numérique sécurisée au sein des environnements de production (OT) complexes. Faites appel à notre expertise pour vous aider à concevoir, mettre en œuvre et surveiller les projets de votre entreprise, afin de mieux tirer parti de vos opérations, et d'avoir l'assurance de disposer des cyberprotections appropriées, de la planification jusqu'à la production.

Passez à l'action

Apprenez en plus sur la transformation numérique sécurisée.

Découvrez l'approche zéro confiance dans la cybersécurité des technologies de la production.

Consultez un expert pour savoir par où commencer.

Suivez-nous.

rockwellautomation.com — expanding **human possibility**®

AMÉRIQUES : Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496 États-Unis, Tél. : +(1) 414.382.2000, Fax :+ (1) 414.382.4444
EUROPE / MOYEN-ORIENT / AFRIQUE : Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Belgique, Tél. : +(32) 2 663 0600, Fax : +(32) 2 663 0640
ASIE PACIFIQUE : Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, Tél. : +(852) 2887 4788, Fax : +(852) 2508 1846
CANADA : Rockwell Automation, 3043 rue Joseph A. Bombardier, Laval, Québec, H7P 6C5, Tél: +1 (450) 781-5100, Fax: +1 (450) 781-5101, www.rockwellautomation.ca
FRANCE : Rockwell Automation SAS – 2, rue René Caudron, Bât. A, F-78960 Voisins-le-Bretonneux, Tél: +33 1 61 08 77 00, Fax : +33 1 30 44 03 09
SUISSE : Rockwell Automation AG, Av. des Baumettes 3, 1020 Renens, Tél: 021 631 32 32, Fax: 021 631 32 31, Customer Service Tél: 0848 000 278

Publication GMSN-WP003A-FR-P – Mai 2022