

Pourquoi l'infrastructure IT OT sécurisée est devenue un impératif industriel

Dans les ateliers de production, les salles de contrôle et les postes de supervision, la séparation nette entre l'informatique de gestion et les automates de terrain n'existe plus. Les industriels qui ont connecté leurs robots, leurs capteurs et leurs automates au réseau IP l'ont fait pour gagner en réactivité, pour collecter des données de production en temps réel et pour piloter à distance. Mais en ouvrant ces systèmes, ils ont aussi ouvert la porte à des risques que beaucoup sous-estiment encore. Une infrastructure IT OT sécurisée ne se limite pas à poser un pare-feu entre deux réseaux : elle oblige à repenser l'architecture dans son ensemble, en intégrant des protocoles historiques, des contraintes de disponibilité extrême et des menaces qui n'ont rien à voir avec celles d'un simple ransomware de bureau.

Le problème commence par un constat simple : les équipements OT – automates, contrôleurs, capteurs – ont été conçus pour durer quinze à vingt ans, pour fonctionner 24h/24 sans redémarrage et pour obéir à des cycles de communication déterministes. Les mécanismes de sécurité qu'on ajoute aujourd'hui ne doivent pas perturber ces cycles. Un correctif qui nécessite un redémarrage peut être inacceptable sur une ligne de production qui tourne en continu. C'est pourquoi les référentiels comme IEC 62443 ou le NIST CSF ne sont pas de simples check-lists : ils imposent une approche par zones et conduits, où chaque segment du réseau est isolé selon son niveau de criticité et où les flux sont strictement contrôlés.



Comprendre l'architecture Purdue pour bâtir une infrastructure IT OT sécurisée

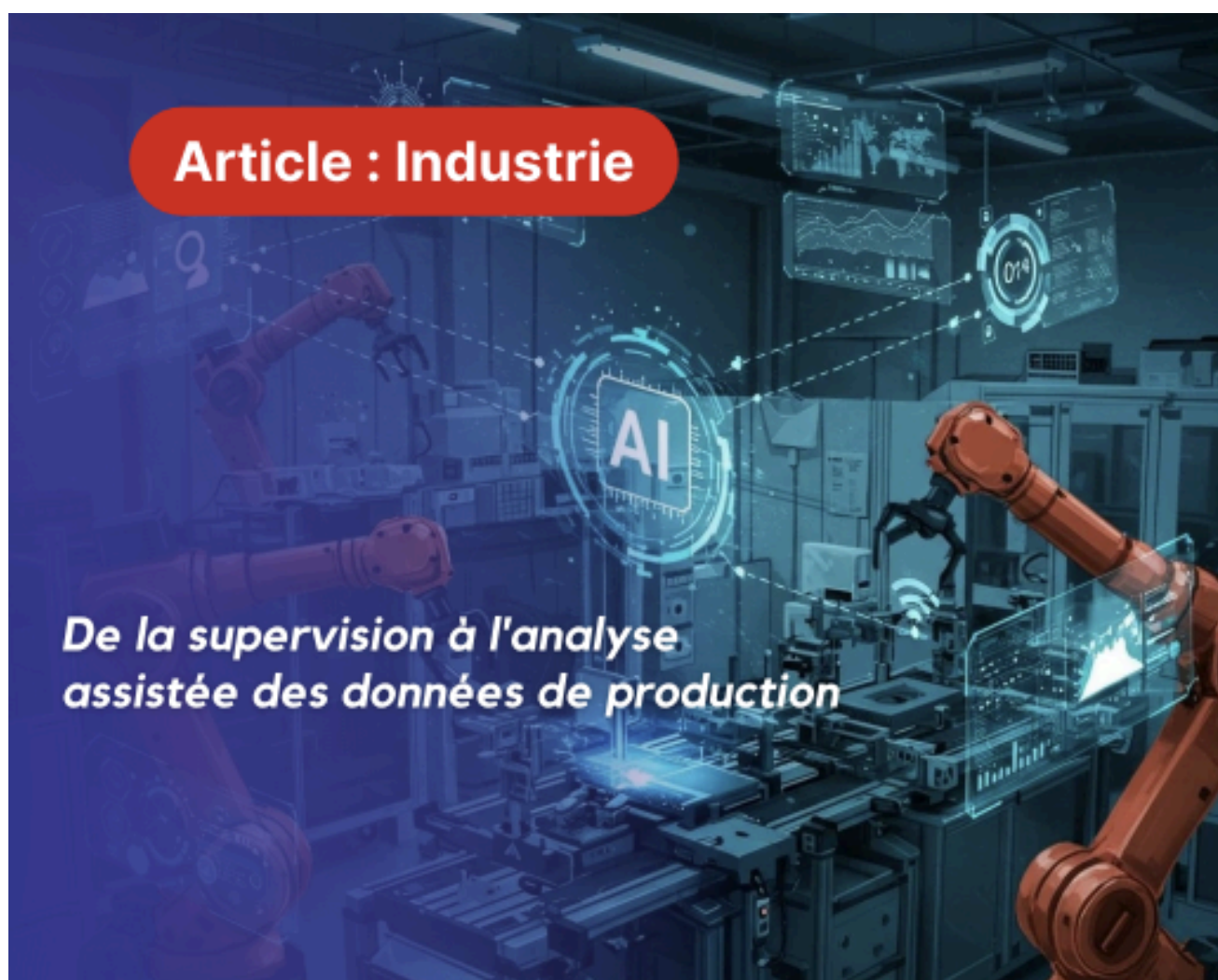
La Purdue Enterprise Reference Architecture reste le modèle le plus utilisé pour structurer les réseaux industriels. Elle définit plusieurs niveaux, du niveau 0 (capteurs et actionneurs) au niveau 5 (réseau d'entreprise). Chaque niveau communique avec les niveaux adjacents à travers des passerelles qui filtrent et traduisent les protocoles. Un automate de niveau 1 ne dialogue pas directement avec un ERP de niveau 5 : il passe par un superviseur SCADA en niveau 2, puis par un serveur d'historisation en niveau 3. Ce principe de segmentation semble simple sur le papier, mais dans la réalité, beaucoup d'usines l'ont contourné en connectant des automates directement au réseau WiFi ou en installant des accès distants sans cloisonnement.

Construire une [infrastructure IT OT sécurisée](#), c'est d'abord revenir à cette logique de zones et conduits. Chaque zone regroupe des équipements ayant un même niveau de criticité et des besoins de sécurité comparables. Les conduits sont les chemins de communication autorisés entre ces zones. Un conduit peut être un simple câble Ethernet, mais il doit être protégé par des règles de filtrage, du chiffrement si le protocole le permet (OPC UA le fait nativement,

Modbus pas du tout) et une authentification forte des équipements. L'enjeu est de ne pas bloquer le trafic légitime tout en empêchant un mouvement latéral en cas d'intrusion.

Protocoles anciens, nouvelles menaces

Modbus est encore le protocole roi sur des milliers de sites industriels. Il a été conçu dans les années 1970, sans aucune notion d'authentification ni de chiffrement. Un attaquant qui accède au réseau Modbus peut lire ou écrire n'importe quelle variable sur un automate. Siemens, Rockwell Automation et Schneider Electric ont tous modernisé leurs gammes pour intégrer des protocoles plus sûrs comme OPC UA avec sécurité intégrée, mais le parc installé reste massivement basé sur des protocoles non sécurisés. Un plan de migration progressif est nécessaire, avec des passerelles de traduction et des proxies capables de filtrer les commandes malveillantes sans impacter la production.



Les outils de détection spécialisés se sont beaucoup améliorés. Des plateformes comme Dragos, Nozomi Networks ou Claroty sont capables d'apprendre le comportement normal d'un réseau OT et d'alerter dès qu'un automate commence à envoyer des trames inhabituelles. Elles

s'appuient sur des bases de connaissances comme MITRE ATT&CK for ICS, qui recense les tactiques et techniques spécifiques aux systèmes industriels. Un opérateur peut ainsi détecter une tentative de modification de logique sur un automate ou une communication vers un serveur de commande inconnu. Ces outils ne remplacent pas une architecture bien conçue, mais ils ajoutent une couche de visibilité indispensable.

Les référentiels comme boussole, pas comme carcan

IEC 62443 est devenu la référence pour la cybersécurité des systèmes d'automatisation. Il définit quatre niveaux de sécurité (SL 1 à SL 4) qui correspondent à des exigences croissantes en termes d'authentification, d'intégrité et de disponibilité. Le NIST CSF, plus général, peut servir de cadre d'analyse des risques complémentaire. L'important est de ne pas les appliquer mécaniquement. Un site de traitement chimique n'a pas les mêmes contraintes qu'un entrepôt logistique : le niveau de sécurité acceptable pour un capteur de température n'est pas le même que pour un automate de sécurité qui commande l'arrêt d'urgence.

La norme pousse aussi à adopter le principe de zéro confiance (zero trust) dans les environnements OT. Concrètement, cela signifie qu'aucun équipement, même s'il est physiquement connecté au réseau local, n'est considéré comme fiable par défaut. Chaque requête est authentifiée, chaque flux est autorisé explicitement. C'est un changement culturel profond pour des équipes qui ont l'habitude de considérer le réseau de terrain comme un environnement de confiance. Mais avec l'IT-OT convergence, la surface d'attaque s'est élargie : un terminal de supervision qui exécute un navigateur web peut être le point d'entrée d'une attaque qui finit par modifier un registre de variateur.

Des outils pour opérationnaliser la sécurité

Au-delà des architectures et des référentiels, le marché propose des solutions qui aident à mettre en œuvre ces principes dans des environnements contraints. La plateforme Singularity, par exemple, intègre des capacités de détection et de réponse adaptées aux réseaux OT, avec une console unique qui couvre à la fois les postes de travail IT et les automates. SiteManager, de son côté, permet de gérer les accès distants aux équipements industriels de manière sécurisée, en enregistrant toutes les sessions et en les isolant du réseau principal.

Article : l'IA, remède à tout?

Fabien Villareal
Chief Strategy and Innovation Officer

Ces outils ne sont pas des baguettes magiques. Leur efficacité dépend de la qualité de l'architecture sous-jacente. Une infrastructure IT OT sécurisée ne peut pas se contenter de superposer des solutions de détection sur un réseau plat. Il faut d'abord segmenter, puis instrumenter. Et il faut former les équipes : un automaticien qui ne comprend pas pourquoi on lui demande un mot de passe pour modifier un programme va le contourner. La sécurité technique ne tient que si elle est acceptée et comprise par ceux qui opèrent les systèmes.

Industrie 4.0 et sécurité : un équilibre à trouver

L'Industrie 4.0 promet des usines connectées, flexibles et capables de s'auto-organiser. Les données de production remontent vers des jumeaux numériques, les ordres de fabrication descendent directement du MES vers les automates, et la maintenance prédictive s'appuie sur des flux continus de capteurs. Dans ce schéma, la sécurité ne peut pas être une couche ajoutée après coup. Elle doit être pensée dès la conception des flux, en intégrant les contraintes de latence et de disponibilité.

Les protocoles modernes comme OPC UA avec ses profils de sécurité permettent de chiffrer et d'authentifier les communications sans ajouter de latence rédhibitoire. Mais le passage à l'échelle reste un défi : un site industriel compte des milliers de points de données, et chaque flux doit être configuré individuellement. Des approches comme la gestion centralisée des certificats et l'utilisation de solutions comme SiteManager simplifient cette tâche, mais elles exigent une discipline d'exploitation que beaucoup d'entreprises n'ont pas encore.

Le facteur humain et organisationnel

La cybersécurité OT n'est pas seulement un problème technique. C'est aussi un problème de gouvernance. Trop souvent, la DSI et la production ne parlent pas le même langage. La première veut appliquer des correctifs tous les mois, la seconde refuse toute interruption. Le résultat, c'est un entre-deux où personne n'est vraiment responsable de la sécurité des automates. Les entreprises qui progressent sont celles qui mettent en place des comités de pilotage conjoints, qui définissent des fenêtres de maintenance acceptables et qui acceptent de ralentir certains projets de digitalisation pour les sécuriser correctement.



Les fournisseurs d'équipements — Siemens, Rockwell Automation, Schneider Electric — proposent désormais des services de diagnostic et des mises à jour de sécurité pour leurs gammes les plus récentes. Mais le parc installé ancien reste vulnérable. Remplacer un automate de quinze ans n'est pas toujours possible financièrement, mais des mesures

compensatoires existent : mise en place de DMZ, filtrage strict des flux, surveillance comportementale via des solutions comme celles de Dragos ou de Nozomi Networks. L'important est de prioriser les actions en fonction des risques réels, pas de chercher la perfection théorique.

Au final, une infrastructure IT OT sécurisée ne se mesure pas au nombre de pare-feux installés ou de certificats déployés, mais à la capacité de l'organisation à détecter une anomalie, à la comprendre et à y répondre sans arrêter la production. C'est un processus continu, qui évolue avec les menaces, les technologies et les usages. Les référentiels comme IEC 62443 et NIST CSF donnent un cadre, les outils comme Claroty ou Singularity apportent de la visibilité, et les architectures comme le modèle de Purdue offrent une structure. Mais c'est l'engagement des équipes et la qualité des processus qui font la différence.