Pilz GmbH & Co. KG
Felix-Wankel-Straße 2
73760 Ostfildern
Allemagne / Germany
www.pilz.com

« Zones and Conduits » dans les réseaux d’automatisation : la cybersécurité protège la sécurité

La sécurité est notre priorité absolue

Ostfildern, juillet 2026 – **Le règlement machines l’impose : la cybersécurité industrielle doit protéger les fonctions de sécurité critiques contre toute manipulation – la cybersécurité étant donc une condition préalable à une sécurité fonctionnelle. Mais comment assurer la sécurité d'un réseau d'automatisation de manière globale ? Des normes telles que la CEI 62443-3-2 et la future norme EN 50742 indiquent une voie à suivre : séparer les systèmes en zones, contrôler les liaisons – un principe que l'on retrouve dans toutes les recommandations actuelles des associations et des experts. Pilz en est convaincu : la séparation stricte entre la sécurité et ce qu’on appelle l'automatisation standard constitue la clé d’une sécurité efficace des machines – fondée sur le principe de la Defence-in-Depth et mise en œuvre grâce à l'approche « Zones and Conduits ».**

Une maison peut être construite de manière solide et sécurisée : avec des murs stables, des matériaux ignifuges, un système électrique fiable et des détecteurs d'alarme fonctionnels. Cette sécurité structurelle illustre parfaitement la sécurité des machines, pour lesquelles des mesures de conception, des capteurs et des mécanismes de protection sont censés prévenir des risques involontaires. Une telle maison ne reste toutefois en sécurité que si elle n’est la cible d’aucune intervention ciblée. Des commandes de chauffage manipulées, des circuits électriques sabotés ou des systèmes d'alarme désactivés peuvent transformer un bâtiment

objectivement sûr en un lieu à risque. Même dans l'univers des machines, la meilleure conception technique de sécurité perd toute efficacité si des composants essentiels en termes de sécurité sont altérés ou mis hors service sans autorisation.

Dans ce contexte, la cybersécurité joue le rôle de la protection extérieure : des portes robustes, des accès sécurisés, des liaisons surveillées et des barrières contre les interventions indésirables. La cybersécurité ne constitue donc pas une protection contre les accidents en soi, mais contre la mise hors service des mécanismes de protection – par exemple par des personnes qui y accèdent en sélectionnant un mode de fonctionnement non autorisé ou en effectuant des actions non autorisées. C'est la seule façon que la sécurité reste efficace et fiable – la cybersécurité au service de la sécurité.

De la spécification normative à la suggestion de solution

Le Règlement machines (UE) 2023/1230 fait pour la première fois de la cybersécurité une condition préalable obligatoire pour le bon fonctionnement de la sécurité sur les machines et les installations : les fonctions de sécurité ne doivent être compromises ni par une manipulation intentionnelle ni par une manipulation involontaire. C'est précisément dans cette optique que s'inscrit la future norme EN 50742, qui contribuera à préciser les exigences fondamentales en matière de cybersécurité prévues par le règlement machines. La norme définit les détails techniques relatifs à la protection contre la corruption et énonce des exigences claires concernant le matériel, le logiciel et les données susceptibles d'influencer les fonctions de sécurité. La norme couvre l'ensemble du cycle de vie – du développement à la mise hors service, en passant par l'utilisation. La série de normes CEI 62443, qui décrit la cybersécurité systématique

pour les systèmes d'automatisation et de commande industriels, joue également un rôle central. Elle offre un cadre structuré pour l'analyse des risques, la « Defence-in-Depth » ainsi que le principe de segmentation (« Zones and Conduits ») et est expressément reconnue dans la norme EN 50742 comme une approche alternative ou complémentaire en matière de sécurité. Ensemble, ces normes constituent le cœur normatif du concept de la cybersécurité au service de la sécurité : elles exigent que l'intégrité numérique d'une machine soit considérée comme une condition préalable à sa sécurité fonctionnelle et qu'elle soit protégée en conséquence.

Pourquoi « Zones and Conduits » rend les machines plus sûres

Revenons à l'image de la maison : la chaufferie représente une zone, tandis que la liaison avec la passerelle domotique correspond au chemin de liaison associé. Si cette liaison est manipulée, l'ensemble du système risque d’être compromis – même si la pièce est parfaitement protégée. Ce qui donc déterminant, ce n'est pas seulement la sécurité des différentes zones, mais aussi celle des liaisons qui les relient. C'est précisément là qu'intervient le principe des « Zones and Conduits ». Les zones sont clairement séparées les unes par rapport aux autres, et les transitions entre elles sont aménagées de manière contrôlée. Tout comme dans une maison où les portes et les clés attribuées déterminent qui peut accéder à quel endroit, dans une installation industrielle, la protection interne (sécurité) et la protection externe contre les manipulations (cybersécurité) s'imbriquent de manière structurée.

On obtient ainsi un concept de protection qui repose sur le principe de Defence-in-Depth : la sécurité n'est pas assurée par une seule barrière, mais par plusieurs couches de protection disposées successivement. Quand une couche est franchie, la suivante résiste.

Ces zones en gradins constituent des espaces, tandis que les conduits constituent les passages contrôlés qui les relient. Cela permet d'éviter qu'une seule vulnérabilité ne mette en danger l'ensemble du système, en particulier lorsqu'il s'agit de sécurité et, par conséquent, de la protection des personnes.

Pilz applique systématiquement cette approche sous le nom de « Cybersécurité au service de la sécurité » : la sécurité (Safety) est l'objectif premier de la cybersécurité (Security). La priorité est donnée à la protection de la sécurité, qui, à son tour, protège les personnes. C'est pourquoi Pilz Safety sépare la commande générale des machines, ce qu'on appelle l'automatisation standard, réduisant ainsi l'exposition des fonctions de sécurité. Plus ces « trésors » sont clairement séparés sur le plan fonctionnel, moins il est nécessaire de mettre en place des mesures de sécurité supplémentaires pour les protéger de manière fiable.

Les avantages de cette approche se manifestent tout au long du cycle de vie d'une machine. Si la sécurité et les fonctions standard sont séparées, il n'est pas nécessaire de recertifier ou d'adapter les fonctions de sécurité en parallèle lors d'une mise à jour des fonctions standard, ce qui réduit considérablement les opérations de maintenance et d'entretien. De plus, les contrôleurs de sécurité classiques nécessitent des mises à jour critiques pour la sécurité considérablement moins souvent que les contrôleurs standard, de

sorte que cette séparation permet d'éviter de nombreuses interventions inutiles. Sur le plan technologique également, la séparation offre des avantages : un système de sécurité autonome, tel que le micro automate configurable de sécurité PNOZmulti 2, peut être combiné librement avec des produits de différents fabricants, tandis que les systèmes intégrés sont souvent liés à des technologies spécifiques. En même temps, les solutions de sécurité distinctes compliquent la tâche des personnes malveillantes, car les systèmes distincts doivent être compromis un par un, ce qui rend la fraude considérablement plus difficile. De plus, un système standard peut être connecté à Internet si nécessaire, tandis que les fonctions de sécurité proprement dites restent isolées, ce qui réduit considérablement sa surface d'attaque.

Par ailleurs, cette séparation entre l'automatisation de la sécurité et celle de la cybersécurité, chacune avec des security levels parfaitement adaptés, améliore l'efficacité grâce à une meilleure prévisibilité des mesures de sécurité, de maintenance et d'extension. Les modifications apportées au programme standard ne nécessitent alors aucune intervention sur la partie relative à la sécurité, ce qui réduit considérablement le travail de programmation et d'adaptation. En même temps, cette séparation a une conséquence positive sur les coûts liés aux logiciels et au support, étant donné que les systèmes distincts entraînent souvent moins de frais de licence et de service.

La sécurité par la séparation – la compétence par la formation

La séparation claire entre la sécurité et l'automatisation standard garantit non seulement une grande résistance technique, mais permet également de réduire les utilisations inappropriées et les besoins en formation. Étant donné que les fonctions de sécurité s'exécutent sur un matériel dédié et sont clairement délimitées sur le

plan organisationnel, elles restent protégées même en cas de modifications apportées au programme standard. Les erreurs commises dans le cadre de l'exploitation quotidienne ne compromettent donc pas la sécurité et permettent une attribution plus claire des responsabilités.

Afin d'aider les entreprises à mettre en œuvre cette architecture, Pilz propose un programme complet de formation et de services. Il s'agit notamment des formations « Principes fondamentaux de la cybersécurité industrielle » et « CESA – Certified Expert for Security in Automation », ainsi que des prestations sur la cybersécurité industrielle. Ils ne se contentent pas d'expliquer comment développer des concepts robustes de « Cybersécurité au service de la sécurité » à partir des différents blocs constitutifs, mais vont bien au-delà : ils montrent comment gérer systématiquement les risques de sécurité et développer des solutions d’amélioration globales, comment intégrer les exigences de la norme CEI 62443, comment mettre en place l'architecture d'un réseau de machines sécurisé et comment évaluer l'efficacité des mesures prises et l'améliorer en continu.

Un avantage décisif de cette approche : les opérateurs chez l'utilisateur final n’ont pas besoin d'être formés en profondeur aux questions de cybersécurité, étant donné que la protection des fonctions de cybersécurité est déjà garantie par la conception architecturale. Ces formations s'adressent donc principalement aux personnes chargées de prendre des décisions en matière de cybersécurité ou de concevoir des systèmes – tout en permettant aux opérateurs de continuer à travailler en toute sécurité sans avoir à suivre de formation supplémentaire dans le domaine de la cybersécurité industrielle. Il en résulte une répartition des rôles

adaptée à la pratique, qui simplifie l'exploitation de l'installation tout en augmentant durablement le niveau de protection.

Plus de sécurité grâce à une structure claire – et au savoir-faire adéquat

Une stratégie « La cybersécurité au service de la sécurité » efficace ne repose pas sur des mesures isolées, mais sur une architecture bien pensée, des responsabilités clairement définies et un développement ciblé des compétences. C'est précisément là qu'intervient Pilz. En mettant résolument l'accent sur la « Defence-in-Depth » et en opérant une séparation claire entre la sécurité et l'automatisation standard, Pilz établit les bases de machines résilientes – et complète cette approche par des formations et des conseils axés sur la pratique, afin que les entreprises puissent s'engager dans cette voie en toute confiance. Il en résulte un niveau de sécurité qui non seulement répond aux exigences standard, mais apporte également une valeur ajoutée tangible au quotidien : plus simple, plus robuste et durable à long terme.

((Caractères : 9 640))

comprenant les conseils, l'ingénierie et les formations, complète la gamme. Au-delà de la construction de machines et d'installations, les solutions de Pilz sont utilisées dans de nombreux secteurs d'activités, comme l'intralogistique, l'emballage et le ferroviaire ou dans le domaine de la robotique.

www.pilz.com

Pilz sur les réseaux sociaux :

Sur nos réseaux sociaux, nous fournissons des informations d'ordre général concernant l'entreprise et les ressources humaines chez Pilz et communiquons sur les nouveautés à propos des techniques d'automatismes.

www.pilz.com/facebook
www.pilz.com/xing
www.pilz.com/youtube
www.pilz.com/linkedin

Interlocuteurs pour la presse :

Martin Kurth

Presse d'entreprise et presse spécialisée
Tél. : +49 711 3409-158
m.kurth@pilz.de

Sabine Karrer

Presse spécialisée et presse d'entreprise
Tél. : +49 711 3409-7009
s.skaletz-karrer@pilz.de

Jenny Skarman

Presse spécialisée

Tél. : +49 711 3409-1067
j.skarman@pilz.de

Eva Gellner-Rößle

Presse spécialisée

Tél. : +49 711 3409-7147
e.roessle@pilz.de