Informations d’ordre général

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

Octobre 2025

Protection des entreprises, des machines et des produits

Sécurité et cybersécurité industrielle – tout d’un même fournisseur

Ostfildern, octobre 2025 – **Les incidents de cybersécurité ne concernent plus seulement les systèmes informatiques, mais de plus en plus l’environnement de production (technologie opérationnelle). Dans le domaine de la cybersécurité industrielle, les incidents désignent non seulement des attaques ciblées, mais aussi des contournements et fraudes involontaires. La tâche de la cybersécurité industrielle en production consiste à garantir la disponibilité des machines et des installations, ainsi que l’intégrité et la fiabilité des données et des process des machines. L’objectif de protection ultime est toutefois la sécurité fonctionnelle. Il est en effet évident que si les entreprises ne maîtrisent pas leurs données, c’est leur existence même et la sécurité de leurs collaborateurs qui sont menacées : sans cybersécurité, pas de sécurité et sans sécurité, pas de protection des personnes !**

Au sein de l’Union européenne, l’augmentation des menaces ne fait plus de doute et la législation a été adaptée en conséquence : au niveau des entreprises, la **directive NIS 2** exige des mesures visant à mettre en place un niveau de cybersécurité commun élevé au sein de l’Union, par exemple par le biais d’un système de gestion de la sécurité de l’information.

Le **règlement européen sur les machines 2023/1230** prévoit désormais la protection des machines et des installations contre la corruption et exige la mise en place de mesures de cybersécurité

industrielle pour les parties d'une machine ayant une incidence sur la sécurité fonctionnelle.

Le **Cyber Resilience Act (CRA)** exige quant à lui la mise en place de mesures de cybersécurité pour les produits contenant des éléments numériques. Il s'agit notamment des systèmes de commande, des systèmes d'entrées / sorties et d'autres composants utilisés dans les machines.

Entreprise, machines et produits – à chaque niveau, les constructeurs et exploitants de machines sont confrontés à des défis différents et à des cadres réglementaires différents.

Une sécurité à la pointe de la technologie

Indépendamment du fait que la législation rend la cybersécurité industrielle obligatoire, il existe toute une série de bonnes raisons de se pencher sur la question et de se faire conseiller suffisamment tôt. Si elles ne sont pas régulièrement remises en question, les processus et les conditions établies pour l'utilisation des machines peuvent favoriser les fraudes. Par exemple, une longue durée de vie des machines conduit souvent à la vétusté des systèmes associés qui, à un moment ou à un autre, ne sont plus conformes aux normes de cybersécurité actuelles. Ces systèmes présentent des failles en matière de sécurité qui ne peuvent plus être comblées, car le fournisseur ne propose plus de mises à jour. De plus, bien souvent, il n'est pas possible d'implémenter la protection contre les logiciels malveillants sur les terminaux, car ces derniers sont en partie trop anciens et leurs performances en pâtiraient, entraînant au final des défaillances en production.

Évolution progressive vers une cybersécurité industrielle accrue

Il s’agit en fin de compte de veiller à ce que les activités de l’entreprise restent protégées, mais pour cela, les entreprises doivent relever différents défis : cela va de l’identification des prescriptions légales en vigueur, de la détection et de la suppression des failles au sein des systèmes, à la mise en œuvre ultérieure de contrôles, en passant par la sensibilisation et la formation des collaborateurs. La cybersécurité étant ce que l’on appelle un « objectif mouvant », un contrôle régulier de l’état de la cybersécurité industrielle des machines est par ailleurs nécessaire. Il est important à cet égard de définir clairement les responsabilités au sein de l’entreprise et d’adopter une approche systématique qui inclut le développement des connaissances spécifiques nécessaires.

Pilz, société spécialisée dans les automatismes, s’est penchée sur ces exigences afin de concevoir une gamme de prestations de services sur mesure à destination des constructeurs et utilisateurs de machines du monde entier, couvrant tous les aspects de la protection des hommes et des machines. Les experts de Pilz connaissent les exigences réglementaires et normatives en vigueur et en tiennent compte dans leurs conseils. Des formations visant à développer ou à mettre à jour les connaissances en matière de cybersécurité dans les entreprises viennent compléter l’offre. La mise en œuvre pratique s’effectue également à l’aide de solutions intégrant des produits Pilz, par exemple l’offre Identification and Access Management, ou I.A.M., destinée à renforcer la sécurité et la cybersécurité industrielle.

Pose des bonnes bases

Pour garantir la cybersécurité industrielle de leurs propres machines, les professionnels de la construction de machines et d’installations ont besoin de solides connaissances de base – en particulier sur la législation et les normes en vigueur. Les experts de Pilz transmettent

ce savoir-faire dans le cadre de la formation « Principes fondamentaux de la cybersécurité industrielle ». Les participants apprennent à maîtriser les menaces de cybersécurité, les mesures de protection appropriées et les meilleures pratiques dans le contexte de la sécurité des machines et des réseaux. Ainsi, même les débutants dans le domaine de la cybersécurité apprennent avec quelles mesures ils peuvent protéger efficacement les machines contre les cyberattaques et la fraude au niveau de la production.

Avec sa qualification « CESA – Certified Expert for Security in Automation », Pilz propose une formation experte de deux jours offrant aux participants des connaissances approfondies sur la situation normative actuelle en matière de cybersécurité, en particulier en tenant compte de la série de normes CEI 62443 (« Réseaux de communication industriels – Sécurité informatique des réseaux et systèmes »). D'autre part, la formation aborde des mesures pratiques de réduction du risque, telles que le contrôle des accès, l'amélioration de la sécurité du réseau par des moyens techniques ainsi que les mesures organisationnelles permettant de réduire les risques en lien avec la cybersécurité. Les participants apprennent à appliquer correctement la norme et à démontrer que leurs systèmes d'automatismes répondent aux exigences de cybersécurité. Après avoir réussi leur examen final, les participants reçoivent la certification « CESA – Certified Expert for Security in Automation » délivrée par TÜV NORD et reconnue dans le monde entier.

Mise en pratique des connaissances théoriques

S'appuyant sur les bases théoriques et les formations, l'étape suivante de renforcement de la cybersécurité industrielle consiste à appliquer des processus structurés et axés sur la pratique. Les

conseils fournis dans le domaine de la technologie opérationnelle (OT) permettent le passage de la base théorique à des stratégies pouvant être mises en œuvre. Les prestations de cybersécurité industrielle identifient les vulnérabilités existant au sein des systèmes complexes et élaborent des mesures de réduction du risque en suivant une approche progressive. Il en résulte des solutions d'amélioration conçues de manière globale.

Quatre étapes pour une cybersécurité industrielle accrue

Le processus de renforcement de la cybersécurité de la technologie opérationnelle comprend quatre étapes : l'analyse des besoins en protection, l'évaluation du risque de cybersécurité industrielle, le concept de cybersécurité industrielle et la vérification du système de cybersécurité industrielle.

Lors de l'analyse des besoins en protection, l'entreprise détermine les besoins en protection des différents « actifs » de la machine ou de l'installation ainsi que les objectifs de protection correspondants. Lors de la deuxième étape, à savoir l'évaluation du risque, l'ensemble des risques et leur probabilité d'occurrence sont examinés pour chaque sous-zone tout au long du cycle de vie du système. L'étape suivante prévoit l'élaboration d'un concept de cybersécurité industrielle détaillé avec des stratégies et des mesures de défense et de réduction des risques provoqués par les attaques, les fraudes et les utilisations inappropriées. À ceci s'ajoute la création de politiques, de règles et de directives afin de garantir la poursuite de l'exploitation ou du développement du système en toute sécurité. Lors de la dernière étape, à savoir la vérification du système de cybersécurité industrielle, l'efficacité des contre-mesures mises en place est vérifiée.

Sécurisation de la disponibilité des machines

Le processus des prestations de cybersécurité industrielle contribue à contrer ou à prévenir les cyberattaques. Le nombre d'incidents de cybersécurité déclenchés de manière fortuite chute également. En retour, cela entraîne une augmentation de la disponibilité des machines et, au final, une réduction des coûts et la préservation de la rentabilité.

Cette procédure protège avant tout les personnes travaillant sur une machine grâce aux mesures de cybersécurité correspondantes. En effet, un incident de cybersécurité peut nuire à l'efficacité des mesures de sécurité. Par exemple, les barrières immatérielles installées devant les machines veillent à ce que l'opérateur ne pénètre pas dans une zone dangereuse. Toutefois, si une personne malveillante parvient à prendre la main sur le système de commande associé et le mécanisme, la fonction protectrice des barrières immatérielles n'est plus garantie. La cybersécurité protège la sécurité !

Lors de la mise en œuvre concrète sur la machine, une prise en compte globale de la sécurité et de la cybersécurité est donc judicieuse. En effet, sans cybersécurité, pas de sécurité, et sans sécurité, pas de protection des personnes.

Des règles claires : qui a le droit de faire quoi sur la machine ?

La sécurité d'une machine et de ses utilisateurs dépend de la gestion des accès – qu'il s'agisse des personnes ou du réseau. Les accès doivent être protégés contre tout accès non autorisé afin, par exemple, qu'aucune personne ne se trouve dans une zone dangereuse lors de l'utilisation de la machine. Effectivement, même l'utilisation ou la maintenance d'une installation à bon escient – que ce soit sur site ou via un réseau – peut avoir des conséquences fatales.

L’Identification and Access Management (I.A.M.) qui réglemente clairement les autorisations et les accès aux machines et installations au sein d’une entreprise constitue un élément important. Elle regroupe notamment des mesures et des prescriptions organisationnelles, ainsi que des fonctions de sécurité adaptées. Un système d’autorisations d’accès tel que le PITreader de Pilz est l’élément approprié pour ce faire. Il permet aux utilisateurs de satisfaire aux exigences en matière de sécurité des employés, de responsabilité civile, d’optimisation de la productivité et de protection de leurs données.

Seule une considération globale de la sécurité et de la cybersécurité garantit une protection complète des hommes et des machines. Ce n’est plus l’entreprise qui décide si, et dans quelle mesure, elle va aborder le problème de la cybersécurité. Désormais, il s’agit d’une obligation réglementaire. Dans le secteur de la construction de machines, la cybersécurité industrielle n’est pas seulement du ressort du service informatique, mais fait partie intégrante du processus de conception et de construction. La mise en œuvre a posteriori de la cybersécurité se révèle coûteuse et implique généralement des pertes en termes de convivialité, de fonctionnalité et de productivité.

((Caractères : X XXX))

((Encadré :))

Vue d’ensemble de la législation de l’Union européenne en matière de cybersécurité industrielle :

En Europe en particulier, le législateur réagit à cette menace en promulguant une série de législations. Par conséquent, en Europe,

les prescriptions sont les plus drastiques au monde. Mais des concertations sont déjà en cours avec d'autres pays qui, bientôt, adopteront également de telles législations. Une harmonisation mondiale en matière de cybersécurité industrielle est donc à prévoir.

NIS 2 : plus d'obligations pour les entreprises

NIS (Network and Information Security) est une directive de l'Union européenne visant à renforcer la cybersécurité. Cette directive a été adoptée en 2016 et concernait jusqu'à présent les fournisseurs du secteur des infrastructures critiques, dont l'énergie, le transport, les banques et la finance, la santé, l'approvisionnement et la distribution d'eau potable ainsi que les infrastructures numériques. Dans une optique de cybersécurité, les fournisseurs de ces secteurs étaient tenus de prendre des « mesures de sécurité adéquates » et de signaler les incidents graves en matière de cybersécurité. La nouvelle directive NIS 2 ((UE) 2022/2555 relative aux mesures destinées à assurer un niveau de cybersécurité commun élevé au sein de l'Union) obligera à l'avenir beaucoup plus d'entreprises à prendre des mesures de gestion des risques en matière de cybersécurité. La directive NIS 2 étend les secteurs concernés, par exemple, aux métiers de la construction et de la production, parmi lesquels la construction de machines et la fabrication d'équipements électriques.

La législation requiert des analyses des risques et des solutions d'amélioration des systèmes d'information, la protection de la chaîne d'approvisionnement, ainsi que la sécurité du personnel. De même, elle impose des concepts pour le contrôle des accès et la gestion des installations, ainsi que des formations obligatoires pour la direction.

La directive a été adoptée fin 2022 par le Parlement européen et le Conseil de l'Union européenne. Comme toutes les directives de l'Union européenne, la directive NIS 2 n'est pas directement

applicable et contraignante dans les différents États membres, mais doit tout d'abord être transposée dans leur droit national. Les entreprises ont donc tout intérêt à se pencher dès que possible sur la directive NIS 2 et à réaliser une analyse complète de leur cybersécurité. Cela implique notamment la mise en place d'un système de gestion de la sécurité des informations (ISMS). Dans ce contexte, une certification de conformité à la norme de sécurité des informations ISO 27001 peut être utile.

NIS 2 et l'exemple des éoliennes : à l'avenir, les constructeurs de machines, tels que les fabricants d'installations de production électrique (par exeemple, les éoliennes) devront également se conformer aux prescriptions de la directive NIS 2. Les fabricants d'éoliennes ont donc besoin notamment de solutions d'automatismes, de systèmes de commande ou de capteurs. À partir d'une certaine taille, même les fabricants de composants électriques sont soumis à la directive NIS 2. De plus, dans la mesure où la directive NIS 2 impose également de prendre en compte les fournisseurs, une entreprise telle que Pilz est également tenue de veiller à la sécurité des chaînes d'approvisionnement et d'imposer des exigences à ses fournisseurs. La directive NIS 2 couvre donc l'intégralité de la chaîne d'approvisionnement.

Nouveau règlement machines : pas de marquage CE sans cybersécurité

Dans le cadre de la sécurité fonctionnelle des machines, la directive Machines 2006/42/CE est particulièrement importante.

Depuis tout temps, pour pouvoir commercialiser leurs machines en Europe, les constructeurs doivent se soumettre à une procédure

d’évaluation de conformité à l’issue de laquelle ils obtiennent le marquage CE.

Publiées en juin 2023 en tant que nouveau règlement machines, les prescriptions ont été mises à jour pour refléter l’état actuel de la technologie. S’agissant d’un règlement, il n’a pas besoin d’être transposé dans le droit national. Les fabricants de machines ont jusqu’au 20 janvier 2027 pour adopter les nouvelles exigences et devront s’y conformer à compter de cette date butoir.

Le règlement machines remplace la directive Machines jusqu’alors en vigueur et, contrairement à cette dernière, rend la cybersécurité obligatoire. Alors que la directive Machines considérait uniquement la sécurité, le règlement a intègré l’objectif de protection de la cybersécurité dans les exigences essentielles de santé et de sécurité (Essential health and safety requirements, EHSR) au titre de la protection contre la corruption (Protection against corruption) : les fonctions de sécurité d’une machine ne doivent pas être compromises par une falsification involontaire ou intentionnelle.

Cette nouvelle approche du marquage CE soulève une série de nouvelles questions pour les constructeurs et les exploitants de machines, car ils sont désormais contraints de revoir leurs concepts de sécurité et de cybersécurité existants.

Cyber Resilience Act : la cybersécurité tout au long du cycle de vie des produits

En plus de la prise en compte de l’entreprise et des machines, il est impératif de mettre en œuvre des mesures de cybersécurité directement sur les appareils (notamment dans les systèmes de commande). En septembre 2022, la Commission européenne a

soumis un projet de règlement destiné à renforcer la cybersécurité des produits. Ce Cyber Resilience Act (CRA) concerne les fabricants de produits intégrant des éléments numériques (matériels et logiciels) capables de communiquer avec d'autres produits. Il s'applique aussi bien à des produits du secteur B2C tels que les smartphones ou les robots-aspirateurs qu'à des produits du secteur B2B comme les systèmes de commande et les capteurs, ou encore à des produits purement logiciels tels que les systèmes d'exploitation ou la machine proprement dite.

Le devoir de signalement par les fabricants des vulnérabilités ayant été exploitées s'appliquera à compter du 11/09/2026. Les produits intégrant des éléments numériques devront satisfaire aux exigences du CRA d'ici le 11/12/2027 pour que leur commercialisation soit autorisée sur le marché européen. Le CRA est un règlement de l'Union européenne et entrera donc immédiatement en vigueur au sein des États membres.

La portée réelle des conséquences du CRA dépend des critères qui sont imposés au final pour la classification des produits. Selon le CRA, seuls les produits garantissant un niveau de cybersécurité adapté – et ce, sur l'ensemble du cycle de vie du produit – peuvent encore être mis en circulation. La cybersécurité commence donc dès le développement des produits. Pour cette raison, depuis quelques années, Pilz aligne également ses process de développement sur la norme CEI 62443-4-1 « Sécurité des automatismes industriels et des systèmes de commande – Partie 4-1 : exigences relatives au cycle de développement de produit sécurisé » et a par exemple conçu le SecurityBridge de façon à ce qu'il soit incontestablement « sécurisé ».

((Caractères : 15 860))

Pilz – The Spirit of Safety

Pilz est un fournisseur mondial de produits, de systèmes et de prestations de services pour les techniques d'automatismes. En tant que pionnier des automatismes de sécurité, Pilz fournit la sécurité pour les personnes, les machines et l'environnement. Fondée en 1948, l'entreprise familiale dont le siège social se trouve à Ostfildern est aujourd'hui représentée dans le monde entier et compte 2 500 collaboratrices et collaborateurs répartis dans 42 filiales et succursales.

Le leader technologique propose des solutions complètes pour les automatismes concernant la sécurité et la cybersécurité industrielle des machines. Celles-ci intègrent les capteurs ainsi que les systèmes de contrôle-commande et le Motion Control – y compris les systèmes pour la communication industrielle, le diagnostic et la visualisation. Une offre internationale de prestations de services, 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