25.05.2023

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

Communiqué de presse

Thomas Pilz : Sécurité et sûreté pour les automatismes numériques

Ostfildern, Allemagne, 25.05.2023 - **(Les paroles prononcées ont été rapportées)**

Thomas Pilz

Sûreté : cet aspect incombe juridiquement aux secteurs de l’industrie et de la construction de machines

Une profonde mutation est en cours concernant les normes et les législations relatives à la sécurité dans l’environnement industriel. Celle-ci est favorisée par les exigences de sûreté et le développement de l’intelligence artificielle (IA). Pour l’industrie en général et pour le secteur de la construction de machines et d’installations en particulier, trois textes légaux, nouveaux ou à venir, sont importants en matière de sûreté : la directive européenne NIS 2, la nouvelle ordonnance Machines ainsi que le Cyber Resilience Act.
Comme cela a été le cas lors de la dernière conférence de presse annuelle, je me concentrerai sur le thème de la sûreté et souhaiterais aujourd’hui vous exposer les importantes conséquences que ces textes légaux vont avoir sur l’industrie tout entière.

NIS 2 : plus d’obligations et plus de sanctions pour un plus grand nombre d’entreprises

La directive NIS (Network and Information Security, Sécurité des réseaux et des systèmes d’information) 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 sûreté, les fournisseurs de ces secteurs étaient tenus de prendre des « mesures de sécurité appropriées » et de signaler les incidents graves en matière de cybersécurité. Cette directive a été remplacée par la nouvelle directive NIS 2, qui est entrée

en vigueur au début de l’année 2023 et qui doit être transposée dans la législation nationale des États membres de l’UE d’ici l’automne 2024. Celle-ci concerne désormais également les secteurs de la construction de machines et de l’automobile, entre autres, et au sein de ces secteurs, les entreprises ayant plus de 50 salariés ou réalisant un chiffre d’affaires annuel de plus de 10 millions d’euros. Selon les données de la VDMA, quelque 9000 entreprises seraient ainsi concernées par la directive NIS 2 en Europe. Ces entreprises vont devoir prouver à l’avenir qu’elles prennent les mesures techniques, opérationnelles et organisationnelles nécessaires pour se protéger des incidents de sûreté. Elles devront ainsi, dans un premier temps, effectuer une analyse des risques des systèmes existants, y compris dans les environnements de production, c’est-à-dire des OT (Operations Technology). Elles devront ensuite élaborer et mettre en œuvre des processus et mesures spécifiques, tels qu’une protection par mot de passe ou un cryptage des données, et devront également mettre en place des formations et une formation continue à l’attention de leurs employés. Les incidents de cybersécurité devront être signalés aux autorités compétentes dans un délai de 24 h. Une autre nouveauté est l’intégration explicite des chaînes d’approvisionnement dans le champ d’application de la directive. Pour résumer, la directive NIS 2 concerne désormais un plus grand nombre d’entreprises, renforce les obligations et prévoit des sanctions plus sévères. Les entreprises qui ne prendront aucune mesure seront passibles de lourdes sanctions.

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

En septembre 2022, la Commission européenne a soumis un projet de règlement destiné à renforcer la cybersécurité des produits. Ce Cyber Resilience Act s'adresse aux fabricants de produits comportant des éléments numériques, ce terme englobant aussi bien le matériel que les logiciels (tels que les firmwares). Ce règlement concerne en l'occurrence aussi bien les produits de consommation que les produits destinés aux applications industrielles, tels que les commandes de machines. Selon le Cyber Resilience Act, seuls les produits garantissant un niveau de cybersécurité approprié pourront désormais être commercialisés. Les fabricants seront par ailleurs tenus d'informer leurs clients de tout problème de sécurité et d'y remédier aussi rapidement que possible. Ce règlement concerne donc l'intégralité du cycle de vie d'un produit. Cela signifie que le fabricant devra désormais proposer des mises à jour logicielles au-delà de la période de garantie habituelle afin de lutter également contre les menaces futures. Ce règlement devrait être adopté à la fin de l'année 2024.

La nouvelle ordonnance Machines : la cybersécurité érigée en obligation

Le troisième nouveau texte légal en matière de sûreté est l'ordonnance Machines de l'UE. Celle-ci devrait être publiée très bientôt. S'agissant d'une ordonnance, elle n'a pas besoin d'être transposée dans la législation nationale. Les fabricants de machines ont 42 mois pour se mettre en conformité avec les nouvelles exigences. L'ordonnance Machines remplace la directive Machines jusqu'alors en vigueur et, contrairement à cette dernière, fait de la cybersécurité une obligation. Si la directive Machines se contentait de fournir une approche en matière de sécurité, la nouvelle ordonnance intègre l'objectif de protection de la sûreté dans les « exigences essentielles de santé et de sécurité » énoncées dans la section « Protection contre la corruption » : les fonctions de sécurité de la machine ne doivent pas être compromises par une corruption délibérée ou accidentelle. On sait pour l'instant que le fait de satisfaire aux exigences du Cyber Resilience Act constituera une présomption de conformité à l'ordonnance Machines.

Les questions qui se posent maintenant sont les suivantes : Qui doit s'occuper de quoi ?

Quel est l'impact actuel de ces textes légaux ? Je souhaiterais répondre à ces questions en prenant l'exemple du secteur de la production d'électricité. Jusqu'à présent, seuls les fournisseurs d'électricité étaient concernés par la directive NIS. Avec la directive NIS 2, les constructeurs de machines comme, par exemple, les fabricants d'installations de production d'électricité (éoliennes, par exemple), devront eux aussi satisfaire à l'avenir aux exigences. Les fabricants d'éoliennes ont à leur tour besoin de solutions d'automatismes, de systèmes de commande ou de capteurs, par exemple de Pilz. À partir d'une certaine taille, même les fabricants de composants électriques tomberont sous le coup de la directive NIS 2. Et dans la mesure où la directive NIS 2 impose également de prendre en compte les fournisseurs, une entreprise comme Pilz sera également tenue de veiller à la sécurité de ses chaînes d'approvisionnement et d'imposer des exigences à ses fournisseurs. La directive NIS 2 couvre donc l'intégralité de la chaîne d'approvisionnement.

Pour pouvoir commercialiser leurs machines en Europe, les constructeurs de machines ont toujours dû se soumettre à la procédure d'évaluation de la conformité aboutissant à l'obtention du marquage CE.
Désormais, avec la nouvelle ordonnance Machines, ils devront prouver que leurs machines sont également protégées contre toute manipulation frauduleuse. Et, pour finir, les fabricants de composants électriques seront également soumis aux futures exigences du Cyber Resilience Act à venir.

Pour conclure, ce n'est plus l'entreprise qui décide si, et dans quelle mesure, elle va aborder le problème de la sûreté. Non, c'est désormais une obligation légale ! Les entreprises feraient bien de se préoccuper dès que possible de la directive NIS 2 et de mettre en place une approche de sûreté globale. Celle-ci peut inclure par exemple la mise en place d'un système de management de la sécurité de l'information (SMSI) certifié conformément à la norme de sécurité de l'information ISO 27001.

Dans le secteur de la construction de machines, la sûreté 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 sûreté se révèle toujours coûteuse et est la plupart du temps synonyme de pertes en matière de convivialité, de fonctionnalité et de productivité. En matière d'appréciation du risque, les aspects relatifs à la sûreté viennent désormais également s'ajouter aux aspects relatifs à la sécurité. Sans sûreté, pas de marquage CE !

Pour les fabricants de produits comportant des éléments numériques, la série de normes CEI 62443 constitue une bonne orientation. La norme CEI 62443-4-1 définit par exemple les exigences d'un processus de cycle de vie de développement sécurisé (« Security Development Lifecycle »).

L’Union européenne est en avance en matière de législation relative à la sûreté et l’Europe pourra se targuer d’avoir les exigences les plus strictes au monde en la matière. Mais des concertations sont déjà en cours avec d’autres pays qui, bientôt, adopteront également de telles législations. L’Australie, par exemple, est actuellement en contact avec l’UE et s’inspirera vraisemblablement des normes européennes. Une harmonisation mondiale en matière de sûreté industrielle est également à prévoir.

Thomas Pilz

Des standards de communication ouverts comme mission historique

Chez Pilz, l’ouverture et la convivialité sont des caractéristiques essentielles de la gamme. Nous voulons proposer à nos clients des produits toujours à la pointe de la technique, simples d’utilisation et pouvant être intégrés à n’importe quelle architecture d’automatismes.

Avec le SafetyBUS p, le premier bus de terrain de sécurité, et le système Ethernet en temps réel de sécurité SafetyNET p, nous avons façonné l’évolution de la communication industrielle de sécurité. L’époque des solutions d’entreprise propriétaires est bel et bien révolue. Nous œuvrons de toutes nos forces pour la création de standards industriels. C’est pour nous une mission historique !

OPC UA

Pour la mise en réseau des installations industrielles en toute sécurité et indépendamment des fabricants, le secteur de l’industrie s’est entendu sur le standard OPC UA (Open Platform Communications Unified Architecture). Ce protocole de communication établit une interface standardisée (CEI 62541) pour la communication entre différentes sources de données dans le secteur industriel. En tant que membres de l’OPC Foundation, les collaborateurs de Pilz sont actifs au sein du comité de pilotage et des groupes d’études techniques du groupe Field Level Communication (FLC). Pilz concentre son attention sur le groupe d’études qui s’intéresse au thème de la sécurité (Safety over OPC UA).

Le savoir-faire de Pilz en matière d'utilisation de la technologie Publisher / Subscriber (Pub / Sub) combiné aux exigences des protocoles de bus de terrain à sécurité fonctionnelle est particulièrement précieux. Contrairement à l'architecture maître / esclave classique, avec la technologie Pub / Sub, les données peuvent être échangées directement entre les abonnés. Cela permet d'utiliser également le standard OPC UA pour les tâches d'automatismes réparties exigeantes. Pilz dispose à cet égard d'une expertise certaine : notre SafetyNET p, le seul bus de terrain de sécurité basé sur Ethernet, prend en charge Pub / Sub depuis le début.

Nous progressons bien sur les thèmes de la sécurité fonctionnelle. Le groupe travaille en collaboration avec les autorités de contrôle à l'élaboration de spécifications et de systèmes de test ainsi qu'à la certification de piles de communication pour OPC UA Safety. La version 1.05 est déjà publiée.

IO Link Safety
Au niveau des capteurs, les automatismes constituent déjà un grand pas en avant en matière d'ouverture. À cet égard, le protocole de communication IO Link Safety est en passe d'être commercialisé. La communication point à point offre de nombreux avantages, dont la simplification de l'installation (exemple : grâce à un câblage standardisé et à l'absence de câbles parallèles), un paramétrage automatisé assisté par logiciel et des possibilités de diagnostic étendues.

Pour pouvoir également utiliser IO Link pour les tâches d'automatismes relatives à la sécurité, Pilz a, dans le cadre de la communauté IO Link, travaillé de manière intensive à l'élaboration de l'extension correspondante, y compris aux tests et à la certification associés. Les experts de Pilz pilotent les deux groupes de travail IO Link Safety (pour le marketing et la technique).

Nous présenterons les premiers capteurs prêts à être commercialisés en novembre, lors du salon SPS. L'approche de Pilz consiste à proposer un système complet, comprenant à la fois les capteurs, les actionneurs et les modules maîtres. Cela simplifie l'utilisation pour les clients et augmente les performances.

Nous sommes convaincus qu'à l'avenir, les solutions d'automatismes se différencieront encore plus par leurs fonctionnalités : les interfaces utilisateur sont-elles pratiques ? L'utilisation est-elle simple ? Quels avantages supplémentaires offrent-elles ? Elles portent en elles une grande force d'innovation et un fort potentiel de création de nouvelles applications.

Thomas Pilz

L'avenir de la sécurité est dynamique

Que signifie une numérisation accrue pour la protection des hommes et des machines ? Quelles technologies résistent aux exigences de sécurité ? Quel est le rôle joué par l'homme ? Nous voulons aujourd'hui nous tourner également vers l'avenir. La bonne nouvelle, pour commencer : l'homme est au centre de cette évolution. Son rôle est même renforcé.

L'homme en tant que concepteur actif

Le projet « Fluide Produktion » d'Arena 2036 en est un bon exemple. Pilz travaille avec différents partenaires au développement et à la mise en œuvre d'un concept de production cyberphysique centré sur l'humain et destiné plus particulièrement à la production automobile. L'idée du projet est de décomposer les installations de production en modules mobiles afin de pouvoir monter et démonter des unités dynamiques selon les besoins. Les modules sont conçus de manière à mettre l'accent sur le rôle de l'homme en tant que concepteur actif de son environnement de production.

De ces exigences découle le souhait d’une sécurité dynamique, c’est-à-dire d’une adaptation plus flexible des fonctions de sécurité aux processus de fabrication changeants et aux exigences de protection associées. Dans le cadre d’une telle sécurité, les robots ou les plateformes mobiles peuvent, par exemple, ne pas s’arrêter immédiatement et brusquement lorsqu’une personne se déplace dans la zone de travail, mais peuvent continuer à travailler avec une vitesse réduite (et par conséquent moins dangereuse) ou, mieux encore, maîtriser des stratégies de repli en toute sécurité. Des capteurs et des actionneurs intelligents dans des systèmes répartis prendront de plus en plus en charge les fonctions des systèmes de commande et entraîneront une meilleure interaction entre les modules des machines entre eux et entre l’homme et la machine.

La sécurité en temps réel

Les situations dynamiques dans les environnements de production futurs doivent être contrôlées et approuvées au regard de la sécurité en temps réel, afin que la protection des hommes et des machines soit garantie en permanence. Le mot-clé est à cet égard « la sécurité en temps réel ». Il est possible qu’à l’avenir, différentes machines – ou les ressources en général – se partagent des dispositifs de sécurité. C’est le principe de la « Shared Safety », ou sécurité partagée, que nous testons dans la SmartFactory KL. Une telle conception de la sécurité exclut un processus d’évaluation de la conformité analogique donnant lieu à l’obtention d’un marquage CE classique. Les informations à destination de toutes les ressources impliquées doivent être disponibles en temps réel pendant le fonctionnement, deux concepts clés étant à cet égard la plaque signalétique numérique et l’enveloppe de gestion.

Dans le cadre du projet « Fluide Produktion » déjà mentionné, nous travaillons à d'autres thèmes d'avenir tels que l'identification des hommes et des objets (et donc la distinction entre ces deux entités). L'intelligence artificielle entre ici en application. Les risques peuvent être détectés et appréciés par des algorithmes d'IA capables d'apprendre. Dans un tel environnement, le marquage CE « analogique » constitue une protection de base. Mais d'autres mesures de réduction du risque sont prises, celles-ci rendant la sécurité encore plus flexible et contribuant à une augmentation de la productivité.

Légende:

Vous pouvez également télécharger les textes et les images sur www.pilz.com. Pour accéder directement aux pages internet importantes du centre de presse, veuillez indiquer le code web suivant dans la fonction de recherche de la page d'accueil.: **237512**

Groupe Pilz

Le groupe Pilz est un fournisseur mondial de produits, de systèmes et de prestations de services pour les techniques d'automatismes. L'entreprise familiale dont le siège se trouve à Ostfildern (Allemagne) emploie environ 2 500 employés, répartis dans 42 filiales et succursales. Pilz fournit dans le monde la sécurité pour les hommes, les machines et l'environnement. Leader technologique, elle propose des solutions complètes pour les automatismes, qui englobent les capteurs, les systèmes de contrôle-commande et le Motion Control – systèmes pour la communication industrielle, diagnostic et visualisation inclus. Une offre internationale de prestations de services, comprenant les conseils, l'ingénierie et les formations, complètent 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 notamment l'énergie éolienne, les techniques ferroviaires ou le domaine de la robotique.

www.pilz.com

Pilz sur les réseaux sociaux

Sur nos réseaux sociaux, vous trouverez des informations concernant la vie de l'entreprise et les dernières nouveautés de nos systèmes d'automatismes.

 https://www.facebook.com/pilzINT

 https://twitter.com/Pilz_INT

 https://www.youtube.com/user/PilzINT


https://www.xing.com/companies/pilzgmbh%26co.kg

 https://www.linkedin.com/company/pilz

Interlocuteur

Martin Kurth
Presse d’entreprise et presse spécialisée
+49 711 3409 - 158
publicrelations@pilz.com

Sabine Skaletz-Karrer
Presse spécialisée
+49 711 3409 - 7009
s.skaletz-karrer@pilz.de