20.05.2025

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

Communiqué de presse

Sécurité, cybersécurité et IA : la sécurité nécessite un cadre législatif mondial

Ostfildern, Allemagne, 20.05.2025 - **Thomas Pilz, directeur associé de Pilz GmbH & Co. KG**

(Seules les paroles prononcées font foi)

Nous connaissons tous le marquage CE. On le retrouve sur les appareils électriques, les jouets ou encore les articles électroménagers, mais aussi bien entendu sur les machines et les installations. Il signifie « Conformité européenne ». Le marquage CE est en quelque sorte le gage que les produits mis sur le marché dans l'Espace économique européen (UE et AELE) répondent aux exigences essentielles en matière de sécurité, de protection de l'environnement et de santé. En apposant ce marquage, le responsable de la mise sur le marché déclare avoir respecté les obligations réglementaires applicables pour garantir la sécurité du produit dans l'Union européenne. Depuis 30 ans, chaque produit concerné par une directive européenne requiert obligatoirement une déclaration de conformité CE.

Parmi ces directives figure la directive Machines, également obligatoire depuis 1995. Elle décrit les exigences uniformes en termes de sécurité et de santé lors de l'interaction entre les hommes et les machines et a ainsi remplacé les nombreuses réglementations nationales qui existaient dans le domaine de la sécurité des machines.

Le marquage CE, un modèle de réussite
Ce qui a nécessité au départ un énorme investissement de la part des entreprises est devenu un atout incontournable de nos jours. En effet, le marquage CE et la directive Machines favorisent la transparence et instaurent une relation de confiance entre les fabricants et les utilisateurs, ce qui est indubitablement un progrès. C'est pourquoi ils sont considérés dans d'autres parties du monde comme des modèles à suivre pour établir un cadre législatif en matière de sécurité des machines.

Au Brésil, par exemple, une loi nationale a été adoptée en 2010 pour imposer le respect d'exigences minimales de sécurité relatives aux machines et à leurs équipements (Norma Regulamentadora 12 (NR12) – MÁQUINAS E EQUIPAMENTO). Concrètement, elle reprend une grande partie des exigences de sécurité énoncées dans l'annexe I de la directive Machines, y compris certaines exigences spécifiques à certains types de machines. De ce fait, cette loi est également appelée en Europe « directive Machines brésilienne ».

Premier cadre législatif pour la sécurité des machines en Inde

L'Inde, qui peut se targuer de la plus forte croissance démographique, adopte elle aussi un cadre législatif pour la sécurité des machines. Le ministère des industries lourdes (Ministry of Heavy Industries) a publié deux prescriptions en ce sens. Ainsi, les « Omnibus Technical Regulations » définissent les exigences de sécurité relatives aux différents types de machines et aux équipements électriques. Elles visent à garantir que ces machines répondent aux normes de sécurité avant d'être mises sur le marché indien.
Tout comme en Europe, il existe des certifications obligatoires et un marquage de conformité. La plupart des nouvelles exigences applicables en Inde correspondent aux normes internationales existantes.

Il est obligatoire de nommer un représentant agréé dont le siège se trouve en Inde pour exporter des produits vers le pays. Notre filiale indienne peut apporter son soutien aux entreprises pour satisfaire à ces exigences et ainsi exporter vers l'Inde. Des collaborateurs de Pilz Inde siègent par ailleurs dans le comité « Bureau of Indian Standard ».

Le thème de la sécurité des machines va certainement continuer à se développer en Inde. Mais ce que l'on peut affirmer avec certitude, c'est qu'à l'avenir, les machines ou les produits qui ne sont pas conformes (on pourrait dire qui ne possèdent pas le marquage CE indien) ne pourront pas être importés en Inde. Cela pourrait signifier que les machines ou les produits seront bloqués à la douane indienne jusqu'à ce que le fournisseur ait respecté les prescriptions requises.

Sécurité : 30 ans plus tard

Revenons au milieu des années 90 : c'est à cette époque que Tim Berners-Lee, chercheur au CERN, centre de recherche situé en Suisse, a rendu publique la technique permettant d'utiliser le WWW. C'est le point de départ de la mise en réseau et de la numérisation dans la société et l'industrie.

Trente ans plus tard, la définition de la sécurité n'est plus la même. Car en raison de cette mise en réseau et de cette numérisation, les produits et les machines comportant des éléments numériques sont exposés à des risques tout à fait différents, tels que la falsification de données. Le législateur européen a réagi : le principe du marquage CE est maintenu. Les exigences à respecter pour l'obtenir ont été adaptées à l'état actuel de la technique. Le nouveau règlement machines a remplacé la directive Machines en 2023. J'aimerais évoquer ici brièvement deux nouveautés : l'intelligence artificielle et la cybersécurité industrielle.

Est-il possible de garantir la sécurité de l’intelligence artificielle ?

« Un robot ne peut pas blesser un être humain »
, c’est ainsi qu’Isaac Asimov formulait déjà en 1942, dans l’un de ses récits de science-fiction, ce que l’on appelle la loi sur les robots pour les machines intelligentes.
Aujourd’hui, 83 ans plus tard, l’évolution de l’intelligence artificielle impose de reconsidérer les règles du jeu de la cohabitation entre les hommes et les machines.
Le législateur l’a également reconnu et a intégré le thème de l’intelligence artificielle dans le nouveau règlement machines, lequel traite de machines au comportement auto-évolutif. À quel point est-il possible de garantir la sécurité d’une machine si ce n’est pas l’homme, mais un algorithme qui détermine comment elle réagit dans les situations dangereuses ?
Dans en cas extrême, il convient de se demander si un logiciel d’auto-apprentissage peut, dans certaines circonstances, donner naissance à une nouvelle machine.
Un sujet extrêmement intéressant non seulement pour les fabricants, mais aussi pour les organismes de contrôle notifiés.

L’IA ne concerne pas seulement le monde des machines.
Le règlement européen relatif à l’intelligence artificielle, appelé « AI Act », régit de manière très générale ce que les systèmes d’intelligence artificielle peuvent et ne peuvent pas faire.
Le règlement proscrit différentes pratiques liées à l’IA, notamment la manipulation des personnes. En d’autres termes, il est interdit d’utiliser l’intelligence artificielle pour inciter les personnes à prendre une décision qui leur causerait un préjudice important à elles-mêmes ou à d’autres personnes De plus, certaines applications, notamment dans les domaines de l’éducation, de l’infrastructure critique ou des poursuites pénales, ont été classées comme des systèmes d’IA à haut risque qui nécessitent de satisfaire à des exigences particulières. Ces systèmes d’IA à haut risque devront eux aussi être dotés d’un marquage CE à l’avenir.

Chez Pilz, nous considérons le règlement sur l'IA comme une réglementation importante qui, d'une part, garantit que les opportunités peuvent être exploitées et, d'autre part, assure que les risques liés à l'IA sont réduits.

Pas de marquage CE sans cybersécurité

En raison de l'explosion des cyberattaques et des dommages causés par la fraude, le nouveau règlement machines exige également à l'avenir une protection contre la corruption des fonctions de sécurité, notamment des systèmes de commande, et impose ainsi des prescriptions en matière de cybersécurité industrielle. Dans la deuxième partie de l'événement, notre expert Simon Nutz expliquera en détail comment les entreprises doivent maintenant réagir au mieux pour pouvoir continuer d'apposer le marquage CE sur leurs produits. Le terme de sécurité des machines fait l'objet d'une redéfinition totale.

Législations sur la cybersécurité : jamais deux sans trois

Globalement, les prescriptions légales relatives à la cybersécurité industrielle instaurées par l'Union européenne pour la construction de machines se répartissent sur trois niveaux : les machines, les produits intégrant des éléments numériques et les entreprises.

- Le règlement machines s'applique aux machines.
- Le Cyber Resilience Act définit des exigences de cybersécurité pour les produits contenant des éléments numériques.
- Et la directive européenne concernant des mesures relatives à un niveau commun élevé de cybersécurité dans l'Union, dite directive NIS 2, s'applique dans notre secteur à presque toutes les entreprises de plus de 50 collaborateurs.

L'industrie est donc confrontée à une tâche colossale : les trois législations ont déjà été publiées par l'Union européenne. Pour deux d'entre elles, à savoir le règlement machines et le CRA, le compte à rebours est lancé. L'industrie ne dispose plus que d'un an et demi environ pour adapter le développement, la production et l'ingénierie en conséquence, y compris toutes les procédures et tâches associées telles que la formation ou la documentation. Un chantier véritablement titanesque – comme à l'époque de l'adoption de la directive Machines.

Nous avons déjà parlé du règlement machines. Le CRA exige que les produits contenant des éléments numériques soient conçus, développés et fabriqués conformément aux exigences fondamentales de cybersécurité. Concrètement, cela signifie qu'il existe désormais des prescriptions relatives à l'évaluation du risque et à sa garantie, à la gestion des vulnérabilités, à la documentation ainsi qu'au devoir de signalement.

Nous sommes également concernés. Pour mettre cela en œuvre, nous avons donc instauré il y a quelques années déjà un process de développement « cybersécurisé » certifié selon la norme CEI 62443-4-1 dans nos domaines de développement de produits et nous l'avons fait certifier en 2022. Nous pouvons ainsi garantir que nos développements satisfont aux exigences du CRA. La gamme de produits de Pilz est très vaste, et chaque produit a dû être évalué pour déterminer dans quelle mesure il était concerné par le CRA et s'il devait être adapté le cas échéant. Cette évaluation a eu lieu et les mesures adéquates ont été prises très tôt.

Le troisième acte législatif, à savoir la directive NIS 2 de l'Union européenne, qui oblige les entreprises à se préparer aux cyberattaques, doit encore être transposé dans le droit national. Et ce, en principe, avant le 18 octobre de l'année dernière. Or, seuls 9 des 27 États membres de l'Union européenne ont déjà procédé à cette transposition. Dans les autres pays, comme l'Allemagne ou l'Autriche, ce sont souvent des circonstances politiques qui empêchent l'adoption de la législation.

La cybersécurité ne doit pas attendre la loi

Pilz lance un appel : ayant nous-mêmes été la cible d'une cyberattaque en 2019, je peux témoigner qu'il serait désastreux d'attendre qu'un accord soit trouvé au niveau politique pour mettre en œuvre des mesures de protection en matière de cybersécurité. Il ne s'agit pas simplement de respecter les obligations réglementaires, mais bien de protéger l'entreprise et sa pérennité.

Avec toutes ces nouvelles prescriptions, il convient de se demander si d'autres marchés en dehors de l'Union européenne vont relever les nouveaux défis tels que l'intelligence artificielle ou la cybercriminalité. Pour répondre à cette question, j'aimerais revenir une fois de plus sur le modèle de réussite qu'est le marquage CE. Tout comme pour la directive Machines, on peut s'attendre à ce que la législation et les normes européennes en matière d'IA et de cybersécurité servent également de modèle pour le reste du monde. D'une part, la plupart des gouvernements ont tout intérêt à ce que leurs citoyens soient protégés le mieux possible contre les dangers et, d'autre part, les constructeurs de machines et les producteurs souhaitent pouvoir commercialiser leurs produits dans le monde entier. Cela signifie que tous les acteurs économiques extérieurs à l'Union européenne devront également se conformer aux nouvelles prescriptions s'ils veulent continuer à importer dans l'Union européenne.

Vous voyez, la sécurité comporte de nombreuses facettes qui nous concernent, nous, nos partenaires, nos clients et notre société en général. La nouvelle procédure d'homologation en Inde, les nouvelles exigences relatives à l'IA et à la cybersécurité dans l'Union européenne sont autant d'exemples de l'importance d'une coexistence harmonieuse entre les marchés. Les législations et les normes internationales sont la clé pour y parvenir. Grâce à elles, nous pouvons compter sur des mécanismes de sécurité techniques à l'échelle mondiale.

Légende: *Thomas Pilz, Managing Director (Photo: © Pilz GmbH & Co. KG)*

Vous trouverez des textes et des images à télécharger ci-dessous :
https://www.pilz.com/fr-INT/company/press/messages/articles/245660

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 comprennent 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 par exemple l'intralogistique, l'emballage et le ferroviaire ou dans le domaine de la robotique.

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

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

Interlocuteur

Martin Kurth
Presse d’entreprise et presse spécialisée
+49 711 3409 - 0
publicrelations@pilz.com

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