20.05.2025

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

Press Message

In terms of Safety, Security and AI: The European legal framework is changing

Ostfildern, 20.05.2025 - **Thomas Pilz, Managing Partner, Pilz GmbH & Co. KG**

(Check against delivery)

We all know the CE mark. You can see it on electrical appliances, toys or household goods, but also on plant and machinery of course. It stands for “Conformité Européenne”. The CE mark is effectively the seal that shows that products placed on the market within the European Economic Area (EU and EFTA) meet essential health, safety and environmental requirements. By attaching the mark, the person placing the product on the market signals that they have complied with the applicable legal requirements for the safety of the product within the EU. Every product that falls under an EU directive has required an EC Declaration of Conformity for the past 30 years.

These directives include the Machinery Directive, which has also been mandatory since 1995. It describes standardised health and safety requirements for interaction between human and machine, and replaced the host of individual state regulations that existed on Machinery Safety.

CE success model
What was initially a major challenge for companies is now something no one wants to do without. CE marking and the Machinery Directive create transparency and trust between manufacturers and users. They are therefore success stories. In other parts of the world, they have served as a model for establishing legal frameworks for Machinery Safety, and indeed continue to do so.

In Brazil, for example: since 2010 there has been a national law that stipulates minimum safety requirements for machinery and work equipment: Norma Regulamentadora 12 (NR-12) – MÁQUINAS E EQUIPAMENTO. Wherever possible, the safety requirements from Annex I of the Machinery Directive were actually adopted, including individual special requirements for certain types of machinery. That's why in Europe this law is also called the “Brazilian Machinery Directive”.

First legal framework for Machinery Safety in India
India, the fastest growing economy, is now also adopting a legal framework for Machinery Safety. The Ministry of Heavy Industries has published two relevant regulations. The Omnibus Technical Regulations specify safety requirements for the various types of machinery and electrical equipment. These are designed to ensure that they fulfil the safety standard before the machine is placed on the market in India.
Similar to Europe, there are mandatory certifications and a conformity mark. Most of the new requirements in India are in line with existing international standards.

Anyone wishing to export to India must appoint an authorised representative based in India. Our Indian subsidiary can help companies meet the requirements and export to India. Employees of Pilz India also work on the relevant committee of the Bureau of Indian Standards.

The subject of Machinery Safety will certainly continue to develop in India. What we can say with certainty, however, is that in future, it will not be possible to import any machinery or products into India that are not compliant (those that do not have the Indian CE mark, in other words). This could mean that machinery or products are held by Indian customs until the supplier has met the required specifications.

Security: 30 years later
Let's go back to the mid-1990s, when Tim Berners-Lee publicly released the technology for using the WWW at the CERN research centre in Switzerland. The breakthrough for networking and digitisation in society and industry.

30 years later, security is defined differently. Because as a result of this very networking and digitisation, products and machinery with digital elements are exposed to completely different risks, through data manipulation for example. European legislators have reacted: the principle of CE marking remains in place. The requirements for obtaining it have been adapted to the state of the art. The new Machinery Regulation was published in 2023 and will replace the Machinery Directive in 2027. I'd like to briefly introduce two innovations, Artificial Intelligence and Industrial Security.

Can Artificial Intelligence be safe?

“A robot may not injure a human being.”

That's how Isaac Asimov formulated a so-called robot law for intelligent machines in one of his science fiction stories back in 1942. Today, 83 years later, further developments in Artificial Intelligence mean that the rules for interaction between human and machine must be reconsidered. Legislators have also recognised this and taken the subject of Artificial Intelligence into account in the new Machinery Regulation. It talks about machines with self-evolving behaviour. How safe can a machine be if the way it reacts in dangerous situations is determined not by humans, but by an algorithm?

In an extreme case, consideration must be given as to whether self-learning software can potentially result in a new machine. An extremely interesting subject, not just for the manufacturer, but also for the notified bodies.

AI doesn't just affect the world of machinery. The EU Regulation on Artificial Intelligence, the so-called AI Act, regulates in general terms what AI systems may and may not do.

The regulation prohibits various AI practices, such as the manipulation of people. This means that AI must not lead people to make a decision that would cause significant harm to themselves or others. Also, certain applications, in the areas of education, critical infrastructure or law enforcement for example, have been categorised as high-risk AI systems, which must meet special requirements. These high-risk AI systems must also be CE marked in future.

At Pilz we see the AI Regulation as an important regulation, which ensures that opportunities can be exploited, while also ensuring that the risks posed by AI are reduced.

No CE mark without security

Due to the rapid increase in cyber attacks and damage caused by manipulation, in future the new Machinery Regulation will also require protection against the corruption of safety functions, of controllers for example, and thus sets out requirements for Industrial Security. In the second part of the event, our expert Simon Nutz will provide detailed information on how companies should best react now to enable them to continue CE-marking their products. The concept of Machinery Safety is currently being redefined.

Security laws: All good things come in threes

Overall, the EU has introduced legal requirements for Industrial Security for engineering on three levels. There are requirements for machinery, products with digital elements and companies.

- The Machinery Regulation applies to machinery.
- The Cyber Resilience Act defines cybersecurity requirements on products with digital elements.
- And the EU Directive on measures for a high common level of cybersecurity across the Union, the so-called NIS 2 Directive, applies to almost every company in our sector with more than 50 employees.

This presents the industry with a huge task: all three laws have already been published by the EU. The clock is already ticking for two of these, namely the Machinery Regulation and CRA, and the industry now has around one and a half years to adapt development, production and engineering accordingly, including all associated processes and tasks such as training or documentation. A truly mammoth task – just like the implementation of the Machinery Directive back then.

We've already spoken about the Machinery Regulation. The CRA requires that products with digital elements are designed, developed and manufactured in accordance with basic cybersecurity requirements. In concrete terms this means that there are now requirements for risk assessment and assurance, vulnerability management, documentation and reporting obligations.

This affects us too. So in order to implement this, several years ago we introduced a certified “secure” development process in our product development areas in accordance with IEC 62443-4-1, and had it certified in 2022. That enables us to guarantee that our developments comply with the CRA. Pilz has a very extensive product portfolio and each product had to be assessed to determine the extent to which it is affected by the CRA and whether it may need to be adapted. This assessment has taken place and the corresponding measures were introduced at an early stage.

The third piece of legislation, the EU's NIS-2 Directive, which obliges companies to prepare for cyberattacks, has still to be transposed into national law. The date for this was actually by 18 October last year. Currently, 9 of the 27 EU member states have completed transposition. In the remaining countries, such as Germany or Austria, political circumstances often prevent laws from being passed.

Security not just for the law's sake

Pilz's plea: from our own experience of the cyberattack on Pilz in 2019, I can say that it would be disastrous to wait until there is agreement at political level before implementing security protection measures. It's not about fulfilling legal requirements, but about securing the company and its continued existence.

With all the new requirements, the question arises as to whether other markets besides the EU will also face the new challenges, such as Artificial Intelligence or cybercrime. To answer that, I 'd like to return to the successful CE marking model. As with the Machinery Directive, it is to be expected that European laws and standards will serve as a worldwide model when it comes to AI and cybersecurity. Most governments have a strong interest in ensuring that their citizens are as well protected as possible from hazards, while machine builders and producers are keen to be able to market their products worldwide. This means that economic operators outside the EU will also have to meet the new requirements if they wish to continue importing into the EU.

As you can see, security has many facets that affect us, our partners, customers and society in general. The new approval process in India and the new AI and security requirements in the EU are examples of how important it is to have functioning cross-market cooperation. Laws and international standards are key. They help us to rely on global technical security mechanisms.

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

You can find texts and images for downloading at: https://www.pilz.com/en-INT/company/press/messages/articles/245660

Pilz – The Spirit of Safety

Pilz is a global supplier of products, systems and services for automation technology. As a pioneer of safe automation, Pilz creates safety for human, machine and environment. Founded in 1948, today the family business with its head office in Ostfildern is represented worldwide with 2500 employees in 42 subsidiaries and branches. The technology leader offers complete automation solutions for Safety and Industrial Security on the machine. These include sensor, control and drive technology – as well as systems for industrial communication, diagnostics and visualisation. An international range of services with consulting, engineering and training completes the portfolio. Pilz solutions are used in many industries beyond mechanical engineering, such as intralogistics, packaging, railway technology, or the robotics sector for example.

Pilz in social networks

In our social media channels we give you background information concerning the company and the people at Pilz, and we report on current developments in Automation Technology.


https://www.facebook.com/pilzINT


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


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

Contact for journalists

Martin Kurth
Corporate and Technical Press
+49 711 3409 - 0
publicrelations@pilz.com

Sabine Karrer
Technical Press
+49 711 3409 - 7009
s.skaletz-karrer@pilz.de