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

Protection for companies, machinery and products

Safety and Industrial Security – A one stop shop

Ostfildern, October 2025 - **Security incidents no longer affect IT systems alone, but increasingly also the production environment (OT). Industrial Security incidents include not only targeted attacks but also unintended manipulations. The mission of Industrial Security in production is to guarantee the availability of plant and machinery, as well as the integrity and confidentiality of machine data and processes. However, the highest protection goal is Functional Safety. Because ultimately, if companies do not have sovereignty over their data, then the company and the safety of its employees are at stake: without Security there is no Safety and without Safety, people are not protected!**

The increasing threat situation has been recognised within the EU and legislation has been adapted accordingly: at company level, the **NIS 2 Directive** calls for measures to ensure a high common level of cybersecurity within the Union, through an Information Security Management System for example.

The **Machinery Regulation 2023/1230** now stipulates protection against corruption for plant and machinery, and demands Industrial Security measures for parts of the machine that influence Functional Safety.

The **Cyber Resilience Act (CRA)** requires security measures for products with digital elements. These include controllers, IO systems and other components used in machinery.

Companies, machinery and products – At every level, machine builders and operators face different challenges and different legal frameworks.

State-of-the-art Security

Irrespective of the fact that legislation is making Industrial Security mandatory, there are a number of good reasons for dealing with the subject early and getting some advice. Established processes and conditions for operating machinery can encourage manipulation if they are not questioned regularly. For example, a long service life for machinery often leads to a situation where the corresponding systems become outdated, and at some point no longer meet the current security standards. These systems have security gaps that can no longer be closed, because the supplier has stopped providing security updates. Often, protection against malware cannot be implemented on end devices, as some are too old and their performance would suffer as a result, potentially leading to production downtimes.

Greater Industrial Security, step by step

Ultimately, the aim is to ensure that business operations remain protected, but to achieve this companies must overcome various challenges: these range from identification of the valid legal requirements and detection and fixing of vulnerabilities within systems, to raising awareness and training among employees, and subsequent enforcement of controls. Because Security is a moving target, a regular check of the Industrial Security status of machinery is also necessary. It is important to have clear responsibilities within the company and a systematic approach that includes building up the necessary expertise.

The automation company Pilz has prepared itself for these requirements and developed a tailored service portfolio for machine builders and users around the world, which holistically incorporates all aspects for the protection of human and machine. The experts at Pilz know the current legal and standardisation requirements and incorporate these into their advice. Training completes the offer, enabling companies to build or update their security knowledge. Pilz product solutions are also used for the practical implementation, such as the Identification and Access Management - I.A.M. system for greater Safety and Industrial Security.

Laying the right foundation

In order to guarantee Industrial Security on their own machinery, specialists in mechanical engineering require sound fundamental knowledge – particularly of legislation and applicable standards. Experts from Pilz share this expertise in the “Fundamentals of Industrial Security” training course. Delegates learn to understand security threats, suitable protective measures and best practices in the context of machinery and network security. So even those new to Security can learn about the measures they can take to effectively protect machinery from cyber attacks and manipulation at machine production level.

With the “CESA – Certified Expert for Security in Automation” qualification, Pilz offers a two-day expert course that provides participants with in-depth security knowledge in line with the latest standards, particularly with regard to the IEC 62443 series of standards (“Industrial communication networks - IT security for networks and systems”). What’s more, the training covers practical risk reduction measures, such as access control, increase of network security using technical means and organisational measures to avoid

security risks. Participants learn how to apply the standard correctly and demonstrate that their automation systems meet the cybersecurity requirements. After passing the exam, participants receive the globally recognised TÜV NORD certificate as “CESA – Certified Expert for Security in Automation”.

Putting theory into practice

Building on the theoretical foundations and training, the next step in strengthening Industrial Security is to apply structured, practical processes. Consulting in Operational Technology (OT) bridges the gap between the theoretical base and implementable strategies. Using a step-by-step approach, Industrial Security Services identify vulnerabilities in complex systems and develop measures to minimise risk. The result is a holistic security concept.

Four steps for greater Industrial Security

The OT security process has four steps: Protection Requirements Analysis, Industrial Security Risk Assessment, Industrial Security Concept and Industrial Security System Verification.

During the Protection Requirements Analysis, the company identifies the protection requirements of the individual “assets” in the plant or machine, along with their protection goals. Step two is the Risk Assessment, where all risks are considered along with the likelihood of them occurring, for each subsection over the system’s complete lifecycle. The next step is to create a detailed Industrial Security Concept with strategies and measures to defend against and mitigate risks caused by attacks, manipulation and operator errors. In addition, policies, rules and guidelines are created for the continued secure operation or structure of the system. The final step, the Industrial

Security System Verification, checks the effectiveness of the implemented countermeasures.

Secure machine availability

The Industrial Security Services process helps to mitigate or prevent cyberattacks. The number of security incidents triggered unintentionally also falls. This in turn increases machine availability and ultimately ensures cost savings, while maintaining economic efficiency.

This approach primarily protects people on the machine, using appropriate security measures. Because a security incident can obstruct safety measures. For example, a light curtain in front of machinery ensures that operators do not enter a danger zone. However, if an attacker can influence the relevant controller and mechanism, the protective function of the light curtain may no longer be guaranteed. Security protects Safety!

For the actual implementation of the machine, therefore, it makes sense to consider Safety and Security together. Because: there’s no Safety without Security, and without Safety, people are not protected!

Clearly regulated: Who can do what on the machine?

The safety of a machine and its operators stands and falls with the control of access – whether that’s for people or the network. Entry points must be protected against unauthorised access, so that nobody is inside the danger zone when the machine is in operation, for example. Even well-intentioned plant operation or maintenance – whether on site or via a network – could have fatal consequences.

An important element is Identification and Access Management (I.A.M.), which clearly regulates permissions and access to plant and machinery in companies. These include organisational measures and

specifications, as well as the appropriate Safety and Security functions. An access permission system such as PITreader from Pilz represents an appropriate product component. It means that users can meet the requirements with regard to employee protection, liability protection, maximum productivity and data protection.

Only a holistic approach to Safety and Security guarantees the comprehensive protection of human and machine. It is no longer at the company's discretion whether, and to what extent, it wishes to grapple with Security. It is now a legal requirement. In engineering, Security in the form of Industrial Security is not solely a task for IT, but is an integral part of the design and construction. To implement Security retrospectively is complex, and usually means reductions in user friendliness, functionality and productivity.

((Characters: 9,784))

((Box:))

An overview of EU legislation on Industrial Security

In Europe in particular, the legislator has reacted to the threat level with a series of laws. As a result, the world's strictest requirements apply in Europe. But agreements are already in place with other countries, and such laws will be introduced there too. So global harmonisation of Industrial Security is to be expected.

NIS 2: More obligations for companies

NIS (Network and Information Security) is a European Union Directive aimed at strengthening cybersecurity. This directive has been in existence since 2016 and so far has applied to critical infrastructure

providers, including energy, traffic, banks and finances, health, supply and distribution of drinking water and digital infrastructure. Providers in these sectors have had to implement “appropriate security safeguards” and report any serious cybersecurity incidents. The new NIS 2 Directive ((EU) 2022/2555 ... on measures for a high common level of cybersecurity across the Union) requires significantly more companies to take cybersecurity risk management measures in future. NIS 2 expands the sectors to include the manufacturing/producing trades for example, including engineering and manufacturers of electrical equipment.

Requirements include risk analyses and security concepts for information systems, protection of the supply chain and the safety of personnel. Concepts for access control and the management of plants are another requirement, along with mandatory training for management.

The directive was adopted at the end of 2022 by the European Parliament and the Council of the EU. As with all EU directives, NIS 2 is not immediately effective and binding in the individual EU member states, but must be incorporated into domestic law by the member states. Companies would be wise to deal with NIS 2 as soon as possible and carry out a comprehensive security assessment for the company. For example, this includes the development of an Information Security Management System (ISMS). In this context, certification in accordance with the information security standard ISO 27001 is helpful.

NIS 2, using wind turbines as an example: With NIS 2, machine builders such as manufacturers of power generation plants (e.g. wind turbines) will also have to meet the requirements in future. In turn, wind turbine manufacturers need automation solutions, controllers or

sensors. From a certain size, manufacturers of electrical components also fall under NIS 2. And as NIS 2 also stipulates that suppliers are considered, a company such as Pilz must also be concerned with safe supply chains and make demands of its suppliers. So NIS 2 covers the whole supply chain.

The new Machinery Regulation: No Security, no CE mark

The Machinery Directive 2006/42/EC has special significance in terms of the Functional Safety of machinery.

In order to import machinery into Europe, machine builders have always had to undergo a relevant conformity assessment procedure, ending with the CE mark.

Republished as the Machinery Regulation in June 2023, the specifications have been upgraded to the state of the art. As it is a regulation, it does not have to be converted into national law first. Machine manufacturers have until 20 January 2027 to adapt to the new requirements and to meet them from the key date.

The Machinery Regulation replaces the existing Machinery Directive and, in contrast to its predecessor, makes cybersecurity mandatory. Where the Machinery Directive purely examined Safety, the Regulation includes the Security protection goal in the “Essential health and safety requirements (EHSR)”, under “Protection against corruption”: the machine's safety functions must not be compromised by accidental or deliberate corruption.

This new route to CE marking raises a number of new issues for machine builders and operators, because they will need to revise their existing Safety and Security concepts.

Cyber Resilience Act: Security over the whole product lifecycle

As well as examining the company and the machinery, it is absolutely necessary also to implement security measures directly in the devices (such as controllers). In September 2022, the European Commission submitted a draft for a regulation intended to increase the cyber security of products. This Cyber Resilience Act (CRA) is directed toward manufacturers of products with digital elements (hardware and software) that are capable of communicating with other products. Products from the B2C segment such as smartphones or robotic vacuum cleaners are affected by this, as are those from the B2B segment such as controllers and sensors, as well as pure software products such as operating systems or the machine itself.

The reporting obligations for exploited vulnerabilities for manufacturers apply from 11/09/2026. Products with digital elements must satisfy the requirements of the CRA from 11/12/2027 in order to be able to be made available on the market in the EU. The CRA is an EU regulation and will thus be immediately valid in EU member states.

How great the impact of the CRA will actually be depends on the criteria that are ultimately established for classifying products. In accordance with the CRA, only products that guarantee an appropriate level of cyber security may be placed on the market – and that’s over the whole lifecycle of a product. Thus Security starts in product development. That’s why, for some years, Pilz has also aligned its development processes to IEC 62443-4-1 “Security for industrial automation and control systems – Part 4-1: Secure product development lifecycle requirements”, and developed SecurityBridge, for example, to be demonstrably secure.

((Characters: 6,062))

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.

www.pilz.com

Pilz on social networks:

On our social media channels we provide background information about the company as well as the people at Pilz and report on the latest news from automation technology.

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

Press contact:

Martin Kurth
Corporate and Technical Press
Tel.: +49 711 3409-158
m.kurth@pilz.de

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

Jenny Skarman
Technical Press
Tel.: +49 711 3409-1067
j.skarman@pilz.de

Eva Gellner-Rössle
Technical Press
Tel.: +49 711 3409-7147
e.roessle@pilz.de