Background information

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

16 May 2024

Protection for companies, machinery and products

Safety and Industrial Security - One-stop shop

Ostfildern, May 2024 - **Security incidents no longer affect just IT systems, but increasingly the production environment (OT) also. 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. Ultimately, if companies are not in control of their data, then both the company and employee safety are at stake: there's no Safety without Security, and without Safety, people are not protected!**

The EU legislator has reacted to the rising threat level: at corporate level, the **Directive for Network and Information Security NIS 2** requires the overall implementation of an Information Security Management System.

The **new Machinery Regulation 2023/1230** now stipulates protection against corruption for plant and machinery and demands 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.

Irrespective of the fact that the legislator is making Industrial Security mandatory, there are a number of good reasons for dealing with the subject early and getting some advice. That's because many procedures and factors for the operation of machinery encourage manipulations, and should be scrutinised and modified urgently. For example, a long service life for machinery often leads to a situation where the corresponding systems become outdated, and at some point no longer meet the current security standards.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.

Comprehensive service package from Pilz

The ultimate goal is to protect business operations, but to do this companies need to overcome a variety of challenges: this ranges from identification of the valid legal requirements and detection and rectification of weak points in systems, to raising awareness of and training employees, and to subsequent enforcement of controls. Because Security is a goal that is constantly changing, a regular check of the Industrial Security status of machinery is also necessary.

The automation company Pilz has prepared itself for these requirements and developed a service package for machine builders and users around the world that holistically incorporates all aspects for the protection of human and machine. The services range from basic information, orientation guides and training, through to the Industrial Security Consulting Service (ISCS), in which actual projects are implemented.

With the qualification “CESA – Certified Expert for Security in Automation”, since last year Pilz has offered a two-day expert course, which gives delegates concise Security knowledge in line with the current status of the standards. 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. When delegates pass the test, they receive the TÜV NORD certificate for "CESA - Certified Expert for Security in Automation", which is recognised worldwide.

With the new Industrial Security Consulting Service (ISCS), Pilz is expanding the safety-related inspection of machinery to create a holistic approach to Safety and Security. Pilz has developed the service package, building on the proven methodology for functional machinery safety services and based on the security standard series IEC 62443. Once companies have used this service, they will be well equipped in terms of Industrial Security and will meet the current legal requirements.

Four modules for greater Industrial Security

ISCS consists of four modules: Protection Requirements Analysis, Industrial Security Risk Assessment, Industrial Security Concept and Industrial Security System Verification.

In the Protection Requirements Analysis, experts from Pilz visit the company to identify the protection requirement of the individual "assets" in the plant or machinery, and 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. Then the Pilz experts meet with the customer to discuss solution approaches to mitigate the identified risks and potential hazards.

In step three, experts from Pilz create an Industrial Security Concept with strategies and measures to defend against and mitigate risks arising from attacks, manipulations and misuse. 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

Industrial Security Consulting Service helps to mitigate or prevent cyber attacks. The number of security incidents triggered unintentionally also falls. In turn this increases machine availability and ultimately brings cost savings and maintains economic efficiency.

Above all, ISCS ensures that appropriate security measures are used to protect people on the machine. 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!

Thus machine builders and users receive a service package from Pilz, which takes into account all aspects for the protection of human and machine.

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 controlled: 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. If an authorised machine operator is in this danger zone for maintenance purposes, it is essential to ensure that nobody else accesses the plant at the same time. Otherwise, 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.

With the operating mode selection and access permission system PITmode fusion, Pilz offers functionally safe operating mode selection and the control of access permissions on plant and machinery. Each operator is given an RFID-coded transponder, which contains the machine enables that match their responsibilities and qualifications. So the plant can only be operated and controlled by authorised personnel in defined operating modes. This provides a high degree of protection against unintended actions and manipulations.

Add the components of a modular safety gate system to the operating mode selection and access permission system and the result is a coherent machine access concept – from Safety and Security perspectives.

The best safety gate guarding is worthless if data, know-how and operations are not sufficiently secured against unauthorised access

and manipulation and an external attacker is able to penetrate the control system.

Industrial firewall protects against external access

The mission of the SecurityBridge industrial firewall from Pilz is to safeguard against external access to automation networks. It monitors the data traffic between the PC and controller and thus reduces the attack surface for hacker attacks and manipulation. SecurityBridge not only protects Pilz controllers but also third-party controllers from manipulation.

Pilz is convinced that only a holistic approach to Safety and Security can guarantee 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: 10,173))

((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. In future, the new directive for Network and Information Security 2 EU 2022/2555 (NIS 2) will oblige many more companies to take risk management measures for cyber security. 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 safety 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 EU member states, but must be incorporated into domestic law by the member states. The EU member states have until 18/10/2024 to adopt the directive into domestic law. 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, with wind turbines as an example: With NIS 2, machine builders such as a manufacturer 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 20/01/2027 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. If 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 corruption, whether intentional or unintentional.

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.

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: 5,826))

Figures

Fig. 1

Grafik_aus_Prospekt_Schulungen_mit_Pilz_3c_en_ppt

One-stop Safety and Security: Pilz offers a comprehensive solution package with services and products for Industrial Security on machinery. (Foto: © Pilz GmbH & Co. KG)

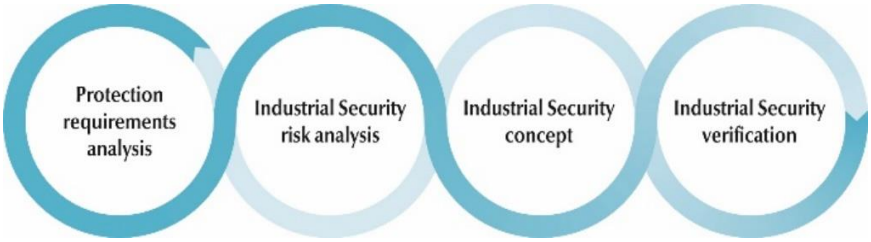
Fig. 2:

F_Services_ISCS_two_men_tablet_in_discussion_get1150297892_cold1

Pilz launches its Industrial Security Consulting Service, helping companies to make their plant and machinery secure. (Foto: © Westend61/[westend61] via Getty Images, © Pilz GmbH & Co. KG)

Fig. 3:

G_Cycle_Industrial_Security_en



The Industrial Security Consulting Service from Pilz consists of four modules: Protection Requirements Analysis, Industrial Security Risk Assessment, Industrial Security Concept and Industrial Security System Verification. (Foto: © Pilz GmbH & Co. KG)

Fig. 4:

F_Press_IAM_Man_using_PITreader_Key_Get1169337234_Get1169337153_cold1

Comprehensive Identification and Access Management controls access to the application, thereby ensuring the integrity of the safety functions and measures –

including Safety and Industrial Security. (Foto: © Westend61/[Westend61] via Getty Images, © Pilz GmbH & Co. KG)

Fig. 5:

F_security_robot_man_virtual_world_Fot208731449_cold1_2019_06

Industrial Security describes the protection of production and industrial plants from faults, whether intentional or unintentional. The aim is to guarantee plant and machine availability, as well as the integrity and confidentiality of machine data and processes. (Foto: © ipopba/Fotolia.com; © Pilz GmbH & Co. KG)

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/X
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

Eva Rössle

Technical Press

Tel.: +49 711 3409-7147
e.roessle@pilz.de

Hansjörg Sperling-Wohlgemuth

Conference and Presentation Management
Tel.: +49 711 3409-239
h.sperling@pilz.de