25.05.2023

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

Press Message

Thomas Pilz: The future of safe automation

Ostfildern, 25.05.2023 - **(Check against delivery)**

Thomas Pilz

Security: Legislation will apply to industry and engineering

The standards and laws for safety in an industrial environment are currently facing upheaval. This is being driven by the issues of security and Artificial Intelligence (AI). For industry in general and for mechanical engineering, there are three new or upcoming legal requirements for security that are relevant: EU Directive NIS 2, the new Machinery Regulation and the Cyber Resilience Act.

As in the last Annual Press Conference, I will focus on the issue of security, and today would like to show you how far-reaching the effects will be for the whole of industry.

NIS 2: More obligations and more sanctions for more 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 successor is NIS 2, which came into force at the beginning of 2023 and must be adopted into national law by EU member states by autumn 2024. Now, the directive also applies within the engineering and automotive sectors, among others, for companies with over 50 employees or an annual turnover of more than 10 million Euro. According to the German Mechanical Engineering Industry Association VDMA, this will affect around 9,000 companies across Europe. In future these companies will need to prove that they have taken technical, operational and organisational measures to protect against security incidents. Firstly this will include a risk analysis of existing systems, including in production environments, in other words OT (Operations Technology). This will be followed by the development and implementation of specific processes and measures such as password protection or encryption, as well as continuing education and training for employees. Cybersecurity incidents must be reported to the relevant authorities within 24 hours. The explicit inclusion of supply chains is also new. To summarise, NIS 2 now affects more companies, extends the obligations and provides for stricter sanctions. Companies that fail to take measures are threatened with severe penalties.

Cyber Resilience Act – Security for the whole product lifecycle

In September 2022, the European Commission submitted a draft for a regulation intended to increase the cybersecurity of products. This Cyber Resilience Act is directed toward manufacturers of products with digital elements. This means hardware as well as software (e.g. firmware). The regulation refers to both consumer products as well as products for industrial applications, such as machine controllers for example. In accordance with the Cyber Resilience Act, only products that guarantee an appropriate level of cybersecurity may be placed on the market. Manufacturers are also obliged to inform customers of security vulnerabilities and close them as quickly as possible. Thus the regulation applies to the whole of a product's lifecycle. This means that manufacturers must now offer software updates beyond the usual warranty period, so that future threats are also repelled. We assume that the regulation will be adopted at the end of 2024.

The new Machinery Regulation – Mandatory cybersecurity

The third new statutory security requirement is the EU Machinery Regulation. Its publication is imminent. As it is a regulation, it does not have to be converted into national law first. Machine manufacturers have 42 months in which to meet the new requirements. 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. So far it is known that meeting the requirements of the Cyber Resilience Act leads to presumption of conformity for the Machinery Regulation.

And now: Who needs to be concerned with what?
What do the statutory requirements mean? I'd like to use the power generation sector to illustrate the correlations: Until now, only energy suppliers were affected by the NIS Directive. 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, for example, from Pilz. From a certain size, manufacturers of electrical components also fall under NIS 2. And as NIS 2 also stipulates that suppliers are taken into consideration, 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.

In order to import machinery into Europe, machine builders have always had to undergo the conformity assessment procedure, ending with the CE mark.
Now, with the new Machinery Regulation, machine builders must prove that their machines are also protected against manipulation. And finally, electrical component manufacturers are subject to the future requirements of the planned Cyber Resilience Act.

To sum up: It is no longer at the company's discretion whether, and to what extent, it wishes to grapple with security. No, it is a legal requirement! Companies would be wise to deal with NIS 2 as soon as possible and carry out a holistic security assessment for the company. For example, this includes the development of an Information Security Management System (ISMS), with certification in accordance with the information security standard ISO 27001.

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 always complex, and usually means reductions in user friendliness, functionality and productivity. The risk assessment now also includes security as well as safety.
No security, no CE mark!

And for manufacturers of products with digital elements, the IEC 62443 series of standards provides a good orientation. The subordinate standard IEC 62443-4-1, for example, describes the requirements of a “Secure development lifecycle process”.

The EU has been quick off the mark with security legislation; the world’s strictest requirements will apply in Europe. But agreements are already in place with other countries, and such laws will be introduced there too. For example, Australia is currently in talks with the EU and will presumably follow the European standards. So global harmonisation of industrial security is to be expected.

Thomas Pilz

Open communication standards as historic mission

At Pilz, openness and user friendliness are key characteristics of the portfolio. We want to offer customers products that are always state of the art, remain easy to use and can be added to any automation architecture.

With SafetyBUS p, the first safe fieldbus system, and with the safe real-time Ethernet SafetyNET p, we have shaped the development of safe industrial communication. But the days of proprietary business solutions are gone. We are fully committed to creating industry standards. That is a historic mission!

OPC UA

Industry has agreed on OPC UA (Open Platform Communications Unified Architecture) for safe, cross-vendor networking for industrial plants. This communication protocol provides a standardised (IEC 62541) interface for communication between different data sources in industry. As a member of the OPC Foundation, Pilz employees are active both in the steering committee and the technical working groups of the Field Level Communication (FLC) group. Pilz's focus lies in the working group that deals with safety (Safety over OPC UA).

Of particular value is our expertise in the use of Publisher/Subscriber technology (Pub/Sub), in connection with the requirements of functionally safe fieldbus protocols. In comparison with the classic Master/Slave architecture, with Pub/Sub, data can be exchanged directly between subscribers. This enables OPC UA to also be used for demanding, distributed automation tasks. Pilz has particular expertise in this area because our SafetyNET p is the only safe, Ethernet-based fieldbus system to support Pub/Sub from the start.

We are progressing well with work on functional safety issues. The group is working hand in hand with the inspection authorities on test specification and test systems, as well as certification of communication stacks for OPC UA Safety. Version 1.05 has already been released.

IO-Link Safety

At sensor level, automation has already taken a great step forward in terms of openness. The communications protocol IO-Link Safety is on the verge of being available commercially. Point-to-point communication offers many benefits, such as simpler installation (e.g. through standardised cabling and the absence of parallel wiring), automated, tool-supported parameterisation and advanced diagnostic options.

So that IO-Link can also be used for safety-related automation tasks, as part of the IO-Link community Pilz has been working intensively on the corresponding extension with the associated tests and certifications. Experts from Pilz lead both IO-Link Safety working groups (for marketing and technology).

We will introduce the first market-ready sensors at SPS in November. Pilz’s approach is to offer a complete system, i.e. sensors, actuators plus Master modules. That simplifies the customer’s application and increases performance.

We are convinced that future automation solutions will be differentiated even more by their functionalities: how good are the user interfaces, how simple are they to operate, what additional benefits do they offer? There is great innovation strength behind this, resulting in huge potential for new applications.

Thomas Pilz

The future of safety is dynamic

What does further digitisation mean for the protection of human and machine? Which technologies meet the safety requirements? What role do humans play? Today we also want to glimpse into the future. First the good news: the focus is on the human, whose role will even be strengthened.

The human as an active shaper

As, for example, in the “Fluid Production” project at Arena 2036. Pilz is working with partners to develop and implement a human-centred, cyber-physical production concept, specifically for automotive production. The idea behind the project is to break down production plants into location-flexible modules, so as to form and then disband dynamic units, entirely according to need. The modules are designed with a central focus on the role of the human as an active shaper of their production environment.

From these requirements there is a growing desire for dynamic safety, i.e. the ability to adapt safety functions to changing production processes and the associated protection requirements with greater flexibility. For example, rather than immediately having to come to a hard stop, they allow robots or mobile platforms to continue working at a reduced (and therefore safer) speed when a person enters the workspace or, even better, to incorporate safe evasion strategies. Intelligent sensors and actuators in distributed systems will take over more and more functions from controllers, leading to better interaction between individual machine modules and between human and machine.

Real-time safety
With regard to safety, dynamic situations in future production environments must be checked and enabled in real-time, so that the protection of human and machine is guaranteed at all times. The keyword here is “Real-time safety”. In the future it’s conceivable that various machines – or general assets – share safety devices. That’s the “Shared Safety” that we are testing in the SmartFactory KL. When safety is understood in this way, classic CE marking as the result of an analogue conformity assessment procedure is ruled out. Information on all the assets involved must be currently available at runtime; keywords here are digital type plate and administration shell.

In the “Fluid Production” project I mentioned earlier, we are working on other future topics such as identification (and therefore differentiation) of humans and objects. This lends itself to the use of artificial intelligence. Risks can then be identified and assessed by adaptive AI algorithms In this case the “analogue” CE mark provides basic protection. But additional risk reduction measures can be introduced, which make safety even more flexible and contribute towards greater productivity.

Caption:

You can find texts and images at www.pilz.com also for downloading. To go directly to the relevant internet pages in the press centre, enter the following Web code in the search of the home page.: **237512**

The Pilz Group

The Pilz Group is a global supplier of products, systems and services for automation technology. Based in Ostfildern, near Stuttgart, the family-run company employs around 2,500 people. With 42 subsidiaries and branches around the world, Pilz supplies safe solutions for people, machinery and the environment. The technology leader offers complete automation solutions comprising sensors as well as control and drive technology – including systems for industrial communication, diagnostics and visualisation. Consulting, engineering and training round off its international range of services. In addition to mechanical and plant engineering, solutions from Pilz are used in many sectors such as wind energy, railway technology and robotics.

www.pilz.com

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://twitter.com/Pilz_INT

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

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

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

Contact for journalists

Martin Kurth
Corporate and Technical Press
+49 711 3409 - 158
publicrelations@pilz.com

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