

20.05.2025

Press Message

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

Industrial Security is a management issue: how companies get started

Ostfildern, 20.05.2025 - **Simon Nutz, Consultant**
Industrial Security

“Security? That's not our concern!” – When asked about security, that's still a common response from machine manufacturers and operators. “Our IT department is responsible for security”, they add, slightly apologetically. In practice, however, IT lacks the specific knowledge, particularly with regard to automation networks. On the other hand, design engineers or even health and safety managers (HSE) are unsure how to deal with cybersecurity. So how do you prepare for Industrial Security?

Application of the Machinery Regulation (MR) is mandatory in the European Union from January 2027. It applies to all companies that want to import or operate machinery in the EU. The MR prescribes Industrial Security in the form of protective measures against corruption. Industrial Security is therefore becoming business-critical and thus a management task. Management must ensure that Industrial Security is firmly entrenched within the company.

Bring everyone to the table

For this to succeed, the first step is to bring together everyone involved. For machine builders, this means IT and development/design and – if available – those responsible for security (e.g. CISO). For users it's IT, production technology, production management, HSE and CISO.

Step one is to build knowledge and develop a common understanding of Industrial Security: what are the legal obligations facing the plant and machinery industry? How are Safety and Security connected? Where do IT and OT interfaces meet?

In step two, these interdisciplinary teams develop a suitable strategy for the company, including an implementation concept. It's about finding a position within the internal structure: where will responsibilities lie in future? What does the network topology of your machinery look like? How does this fit with the new legal requirements?

Implementation begins with the risk assessment

Only then is the company in a position to implement Industrial Security. It starts with the assessment and quantification of potentially damaging events and the production of a protection requirements analysis. Possible vulnerabilities and potential for attacks and manipulation due to networking, digitisation and AI are also identified as part of this process. Important: in addition to classic IT protection goals such as confidentiality, integrity and availability, the protection goals for Industrial Security also include Safety, i.e. the Functional Safety of the machine.

A security risk assessment is always the starting point. It's about analysing the threats and risks that result from security gaps. This means that security measures must be monitored and adapted continuously. That often involves complex IT infrastructures and networks, which requires additional technical expertise and resources.

Security and Safety expert wanted!

Anyone looking for external support when getting started with Industrial Security in automation should be aware that IT security expertise is only of limited help. That's because the processes for reducing the risk of attacks on machinery (Industrial Security) are very similar to the procedures for reducing the risks that can stem from machinery (Safety). Anyone wanting to implement Industrial Security must be an expert in Machinery Safety and be familiar with the respective specifications and standards, above all the Machinery Regulation.

Specific implementation of the legislation is currently in flux. In some places, the harmonised standards are still being drawn up. As an expert in Machinery Safety, Pilz is closely involved and plays an active role in shaping relevant standards. Pilz passes this expertise on to its customers in the form of services and training. The “Fundamentals of Industrial Security” training is aimed at beginners. Delegates learn about terminology and requirements, and to understand cybersecurity in the context of machine and network security. Best practices contribute to the understanding of cybersecurity risks in production.

The “Certified Expert for Security in Automation (CESA)” training provides the tools needed to implement effective organisational and technical measures in industrial automation networks.

In addition to the training programme, Pilz also has the “Identification and Access Management” (I.A.M.) portfolio to offer. Products and individual solutions for a number of tasks relating to employee protection, liability protection, maximum productivity and data protection. Applications include user authentication, safe operating mode selection, data and network security as well as access management, for example. In this way it is possible to cover Safety and Security in one system.

Machine manufacturers and operators worldwide should address the issue now, so they are prepared in time for the challenges of Industrial Security. It is necessary to build knowledge, define responsibilities and interfaces, and develop an individual strategy. Ideally, management initiates this process.

Caption:

You can find texts and images for downloading at:

<https://www.pilz.com/en-INT/company/press/messages/articles/245666>

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