STÖBER

Stay Ahead. Stay Secure.

STÖBER Security.

What is it about?

The growing threat from cyberspace and the increasing digitalization of production systems have already made security a key issue in drive technology in the past. This is also an issue for the EU. In line with its cyber strategy, the following directives will apply to mechanical and systems engineering in the near future.

EU Directive NIS 2.

The NIS (Network and Information Security) was adopted back in 2016 to strengthen cyber security in general. The successor, NIS 2, has been in force since the beginning of 2023. Although drive technology as an industry was not originally concerned, NIS 2 now also requires companies in the mechanical and systems engineering sector to prove that they are taking measures to protect themselves against security incidents. This initially includes the risk analysis of existing systems, including in production environments.

New Machinery Regulation (EU) 2023/1230.

The new Machinery Regulation (EU) 2023/1230 makes the topic of security obligatory for manufacturers. It replaces the previous Machinery Directive and came into force on July 19, 2023. Although machine manufacturers have 42 months for implementation, the new security requirements must be fully met by 2024. This means that, in the future, manufacturers must ensure that the security functions of a machine are not impaired in any way, either unintentionally or intentionally.

Cyber Resilience Act.

The European Commission presented a draft of the Cyber Resilience Act (CRA) in September 2022. The aim is to significantly improve the cyber security of products that can be connected to each other or to the Internet.

Main objectives of this regulation:

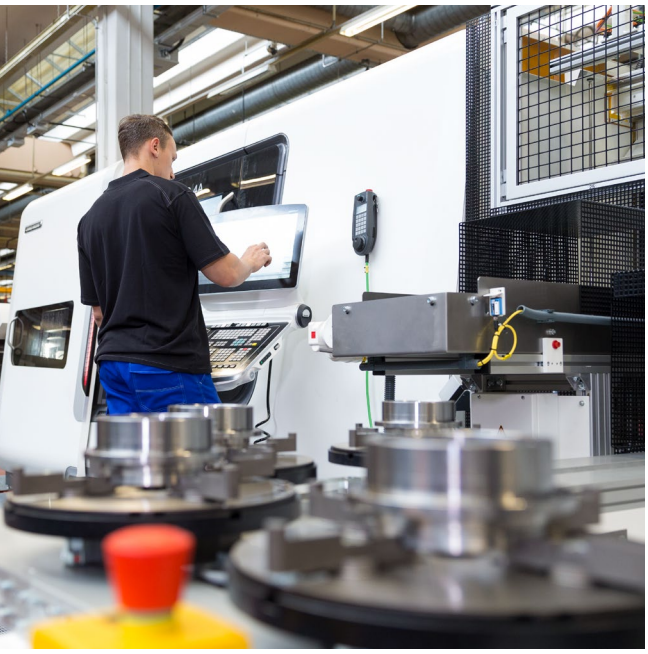
- Products with digital components that are placed on the EU market should have fewer vulnerabilities.
- Manufacturers are responsible for the cyber security of their products during a defined period of time, and …
- … they undertake to close security gaps throughout the entire product life cycle.
- More transparency about the security of hardware and software products.
- Greater security for users.

Manufacturers and developers are now required to implement the stringent requirements of the CRA. This is because products that do not comply with the regulations may no longer be launched on the market as of 2025.
And precisely this is what makes security an essential component for their sale in the EU.

Why is this so important?

The more digital the production, the greater the risk of cyber attacks. These can lead to espionage and sabotage. A single gap in the system is enough. And the longer production is paralyzed, the more dramatic the economic deficits are. On the one hand, financially due to missed revenue, and on the other hand, this damages the trust of customers and the company's reputation.

Other very serious consequences of cyber attacks can be personal injury, especially when safety is manipulated, i.e. functional safety, which is responsible for preventing damage to people and property.



Security at the operational level.

While continuous measures for cyber security at the IT level are a matter of course, the operational technology (OT) level is usually neglected. Yet systems are not closed units and, especially with increasing digitalization, they are opening up to data streams and remote access – and therefore also to hackers.

Our security strategy is based on the international standard IEC 62443, the security standard for industrial automation systems.

It includes

- Guidelines and best practices for the security of your information and control systems in industrial environments.
- Concrete measures to control access and protect networks.

The security-compliant design of processes, for example, to ensure that no unauthorized person can tamper with products between dispatch and arrival at the customer.

STÖBER Antriebstechnik GmbH + Co. KG
Kieselbronner Straße 12
75177 Pforzheim, Germany
Tel. +49 7231 582-0
mail@stoeber.de
www.stober.com