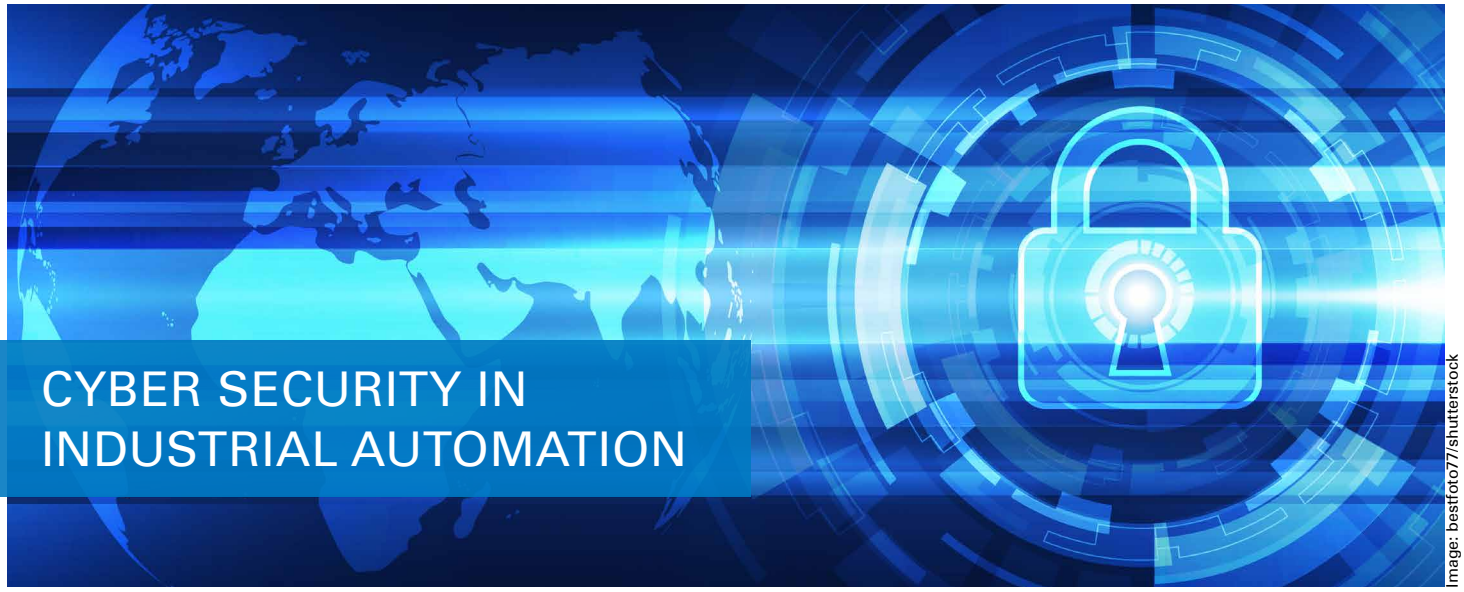


CYBER SECURITY IN INDUSTRIAL AUTOMATION

Image: bestfoto77/shutterstock

Organizations are becoming increasingly digitally connected. Industrial automation and process control systems are reachable through internal and external company networks. Data transfer across different systems and networks increases vulnerability to attacks and subsequent system failures. Preventive measures against internal and external unauthorized access to industrial control systems have, therefore, become necessary to ensure the availability and integrity of such systems.

Functional Safety and Security

Data capture, exchange and analysis is a valuable company practice today, as it is often used to increase efficiency. Many manufacturing control systems are now accessible online and thus subject to cyber threats. Security for industrial control systems follows the clear objective of ensuring the availability and integrity of safety data and functions.

The internationally accepted standard **IEC 62443** and **EDSA ISASecureTM** standard series specify cyber security as well as functional requirements over the life cycle of the automation system, aligned with the safety requirements stated in the **IEC 61508** standard for functional safety.

In addition to the qualification of components under functional safety, TÜV Rheinland now offers combined product safety testing and cyber security evaluation.

The "Functional Safety and Security" Test Mark

The test mark "Functional Safety and Security" from TÜV Rheinland is applied to electronic / programmable electronic products, which are used in safety-related applications.

Manufacturers of such products need to implement additional measures according to the requirements of the standard IEC 62443. Such compliance can be demonstrated with the TÜV Rheinland test mark.

The following codes and guidelines are relevant, apart from the functional safety standards:

- **IEC 62443-3-3:** Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels
- **IEC 62443-4-1:** Industrial communication networks - Network and system security - Part 4-1: Product development requirements
- **IEC 62443-4-2:** Industrial communication networks - Network and system security - Part 4-2: Technical security requirements for IACS components
- **EDSA-311:2010:** ISA Security Compliance Institute - Embedded device security assurance functional security assessment
- **EDSA-312:2010:** ISA Security Compliance Institute - Embedded device security assurance software development security assessment

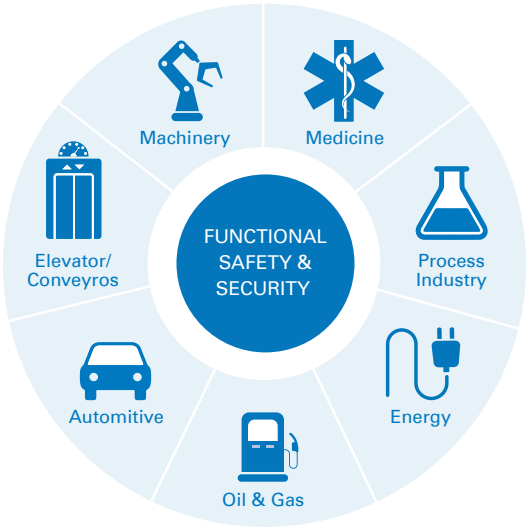
www.tuv.com

TÜVRheinland®
Precisely Right.

Functional Safety and Security Requirements

Functional safety-certified products are confirmed as reliable and safe in accordance with defined levels of the relevant standards (for example, Safety Integrity Level (SIL) in IEC 61508 and Performance Level (PL) in EN ISO 13489-1). Such products are then suitable for use in safety-related applications for the adequate protection of human beings and the environment.

Security requirements involve sufficient protection against manipulation and interference, in accordance with the defined levels (SL 1 to SL 4), in the development and integration phases of products in the same way as for functional safety requirements.



TÜV Rheinland Portfolio

Our range of industrial security-oriented services:

- Product testing and certification according to globally acknowledged functional safety and security standards
- Workshops and trainings
- Assessment and qualification of QM-systems under functional safety and security scheme
- Security threat and risk analysis
- Safety audits of networks
- Vulnerability scans

Workshop and Trainings

TÜV Rheinland has developed a detailed workshop and training on the topic "Security for Industrial Automation & Process Control Systems." The program focuses on the development of safety-ensuring components for automation systems.

The one-day workshop gives participants an overview of the normative requirements of system architecture, implementation and testing.
These topics are explained in greater detail in the 3-day training. Problems resulting from proving compliance to the relevant standards IEC 62443-3-3, IEC 62443-4-1 and IEC 62443-4- 2 are discussed and possible solutions presented.
All requirements necessary to develop a functionally safe and secure product are raised and considered.

After the training, you can take a final test. The "Security Engineer (TÜV Rheinland) (SecEng)" certificate will be awarded to successful exam participants.

Why TÜV Rheinland?

With our cyber security services for industrial automation, you can:

- Demonstrate product compliance to standards IEC 61508 and IEC 62443 with a TÜV Rheinland certificate.
- Profit from the knowledge, experience and global reputation of TÜV Rheinland in functional safety and security.
- Benefit from our international network of experts and one-stop shop service.
- Gain a competitive advantage and increased international market access with test marks and certificates from an internationally accepted and neutral testing institute.

TÜV Rheinland Group
Industrial Services
industrial-services@tuv.com
www.tuv.com

TÜVRheinland®
Precisely Right.