Why functional safety without cybersecurity is no longer possible.

What needs to be considered for monitoring your assets to protect against cybersecurity attacks?

Technical assets that need regular inspection due to special hazards in the areas of steam, pressure, falling or fire or explosion also need to be inspected for cybersecurity in addition to functional safety. Digitalization is also impacting plants requiring monitoring through new information and communication technologies. The networking of plants and machines, their devices, actuators and sensors harbor security gaps that can be exploited by cyber criminals. Therefore, the comprehensive security of a technical asset consists not only of functional safety, but thus also of cybersecurity. Only if systems and processes are "secure", they are also „safe".

TECHNOLOGICAL CHANGES

- Networking of various plant components and controls via communication interfaces, e.g. Profi BUS (W-)LAN, TCP/IP
- Application of processes, methods and procedures of information and IT security in industrial automation
- Processes are digitalized and moved to the cloud

RISKS AND DANGERS

- Injuries, pollution of the environment and loss of production
- Unintentional, unauthorized or malicious interference with the IT/OT systems
- Malfunctions of machines and facilities
- Manipulation of control and processing systems
- Impairment of the functionality of safety-relevant MSR equipment

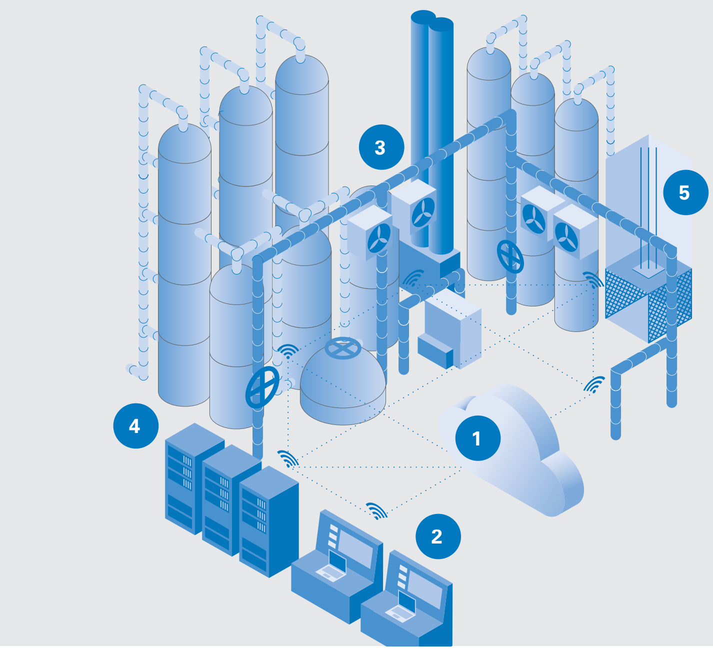
PROTECTIVE MEASURES

- Risk assessment with regard to functional safety and cybersecurity
- Identification of security zones and their protection needs
- Audits of the implemented cybersecurity measures
- Penetration tests
- Continuous identification of vulnerabilities and cybersecurity events

www.tuv.com/fscs

TÜVRheinland®
Genau. Richtig.

FUNCTIONAL SAFETY AND CYBERSECURITY TOUCHPOINTS FOR ASSETS REQUIRING MONITORING.



1 CLOUD COMPUTING & WORKFLOWS
2 HUMAN MACHINE INTERFACE AND IT
3 SENSORS AND ACTUATORS
4 PROGRAMMABLE LOGIC CONTROLLERS AND SERVERS
5 ELEVATOR AND CRANE CONTROL SYSTEMS.

INTERNATIONAL STANDARDS, NORMS AND GUIDELINES.

A large number of relevant standards and norms define safety requirements that operators of assets requiring monitoring must fulfil. These standards are valid and recommended worldwide.

The following standards are relevant for plant safety and cybersecurity aspects:

WORLDWIDE
- ISO 27001
- IEC 62443

VALID THROUGHOUT EUROPE
- EU Cybersecurity Act
- NIS Directive

VALID THROUGHOUT GERMANY
- BetrSichV
- 12. BImSchV
- EmpfBS 1115
- TRBS 1115
- IT Security Act 2.0
- BSI-ICS Security Compendium

ENSURING THE SECURITY OF THE FUTURE TODAY.

ew and smart technologies require expert knowledge. Benefit from our many years of expertise in the field of plant and cybersecurity. We support you in the risk assessment and implementation of the standards relevant to you. With our topic-specific trainings for functional safety and cybersecurity, you can further train your employees as FS Engineer (TÜV Rheinland) or CySec Specialist (TÜV Rheinland) with corresponding certificates.

RETHINK AND ACT DECISIVELY.

As one of the world’s leading testing service provider for functional safety and cybersecurity we offer plant operators a broad portfolio of services. Our experts analyse all aspects of functional safety and cybersecurity along the entire life cycle of your plant – from the concept through realization to commissioning and maintenance.Let us stand together today for the safety of tomorrow.

ONLINE CONTACT

TÜV Rheinland Industrial Service & Cybersecurity
Am Grauen Stein - 51105 Cologne, Germany
cybersecurity@tuv.com
www.tuv.com/fscs

TÜVRheinland®
Genau. Richtig.