5 Minute Guide

Why functional safety without cybersecurity is no longer possible.

In the process, petrochemical and oil & gas industry.

Artificial intelligence, Industry 4.0, Internet of Things (IoT), modular automation – this is the future in the process industry, which has already begun. The increasing and comprehensive digitalization and thus the interaction of information- and communication technologies in industrial production plants enables the networking of machines, devices, sensors and people. Products can be brought to market more flexibly and efficiently and costs can be reduced. At the same time, functional safety and cybersecurity requirements must be met in order to achieve safe automation in the process industry. Only if a process plant is "secure", can it also be „safe".

CHANGES

- Smart equipment: intelligent components and facilities
- Increased use of Artificial Intelligence (AI)
- Modular automation
- Technology of the digital twin of a plant leads to merging of Engineering, Operational and Information Technology

RISKS AND DANGERS

- Hurting people, 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
- Manipulation of sensors

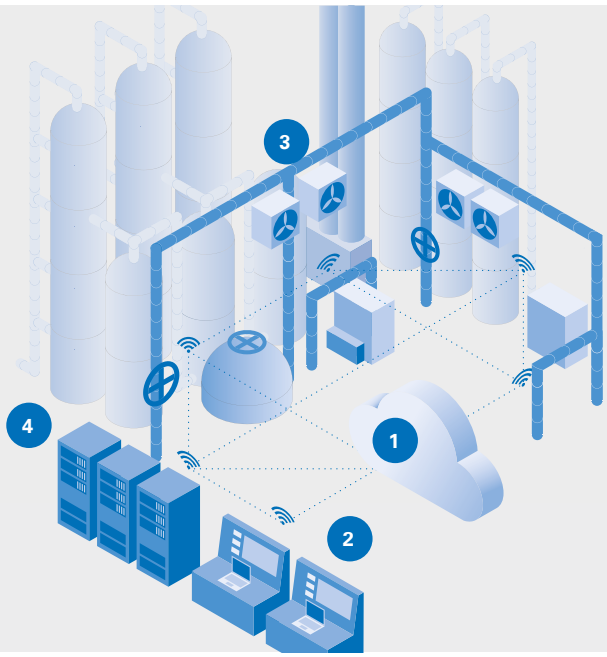
PROTECTIVE MEASURES

- Risk assessment with regard to functional safety and cybersecurity
- IT/OT security analyses for the identification of security vulnerabilities
- Evaluation and testing of the functional safety for installations as well as penetration tests before commissioning
- plant supervision during operation

www.tuv.com/fscs

TÜVRheinland®
Precisely Right.

FUNCTIONAL SAFETY AND CYBERSECURITY TOUCHPOINTS IN THE PROCESS, PETROCHEMICAL AND OIL AND GAS INDUSTRY.



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

INTERNATIONAL STANDARDS, NORMS AND GUIDELINES.

A large number of relevant standards and norms define safety requirements that operators of a plant, manufacturers of machines as well as system integrators of safety-related components and systems must fulfil these standards are valid and recommended worldwide.

For functional safety and cybersecurity aspects, the following standards are relevant:

WORLDWIDE

- IEC 61511
- IEC 61508
- IEC 62443
- VDI/VDE 2180
- Recommendations of the Namur (NA 163, NA 169)

VALID THROUGHOUT EUROPE

- NIS Directive
- EU Cybersecurity Act
- GDPR (DSGVO)

VALID THROUGHOUT GERMANY

- IT-Security Act
- 12th BImSchV
- DSGVO
- Commission guidance documents for plant safety (KAS 44, KAS 51)

ENSURING THE SECURITY OF THE FUTURE TODAY.

New and smart technologies require expert knowledge. With our topic-specific trainings for functional security and cybersecurity, you can further train your employees as FS Engineer (TÜV Rheinland) or Cybersecurity Specialist (TÜV Rheinland) with corresponding certificates.

RETHINK AND ACT DECISIVELY.

As the world's leading testing service provider and consultant in functional safety and cybersecurity we offer machine manufacturers, system integrators and plant operators a broad portfolio of services. Our Experts analyze all aspects of functional safety and cybersecurity along the entire life-cycle of your product, system or plant - from the concept through realization to commissioning and maintenance. Let us stand together today for the safety of tomorrow.

Contact us for your individual IT/OT security analysis.

ONLINE CONTACT

TÜV Rheinland Industry Service & Cybersecurity
Am Grauen Stein · 51105 Cologne
Industrial-services@tuv.com
www.tuv.com/fscs

TÜVRheinland®
Precisely Right.