

CS 930 | Cyber Security Fundamentals (TÜV Rheinland)

TrainingFacts

Presence Training

Fundamentals of Cyber Security of the TÜV Rheinland Cyber Security Training Program

Today, the worlds of functional safety and cyber security are inseparably linked in modern plant and process control systems.

This is also reflected by relevant standards regarding functional safety e.g. IEC 61511 with requirements to conduct a security risk assessment to identify the security vulnerabilities for SIS and to provide the necessary resilience against the identified security risks.

Engineers, Project Managers, Plant Managers, Technicians, and all who may be directly or indirectly involved are faced to handle, describe and understand principles of security management.

The 3.5 day Training will provide you with valuable skills and knowledge. This training ends with an exam. Successful participants will receive a written confirmation from TÜV Rheinland indicating that they have passed the exam. This document is a prerequisite to attend the advanced trainings of the TÜV Rheinland Cyber Security Training Program and to obtain the CySec Specialist (TÜV Rheinland) certificate.

Certificate

The successful completion of the final exam will provide you with a "Fundamentals of Cyber Security Certificate", issued by TÜV Rheinland.

Duration: 3,5 days,
beginning Monday ending Thursday

Number of participants: minimum 4, maximum 16 participants

Registration: <http://academy.hima.com>

Contact: training@hima.com

Course Content

Terms and Definitions

- Safety and Security
- Defense-in-Depth, Zones and Conduits IEC 62443)
- ISO/IEC 2700x, IEC 62351, National Standards
- Principals "Cyber Kill Chain"
- CIA-Triade, Scopes and Measurement
- Understanding CVE/CVSS/ CWE/NVD

Network Communication

- Basic Terms and Definitions (ISO/OSI, NAT, Protocol Architecture)

Technical measures

- Firewall (SPI/DPI)
- 2-FA, PKI, VPN (IPSec / OpenVPN)
- Multi-Layer Security Models (e.g. Data-Diodes)

Organizational measures

- ISMS, Policies, Guidelines
- Risk Assessment
- Asset, Change-, and Patch-Management