

Industrial Security

Security Management, Firewalling and Safety in OT

While manufacturing environments were previously largely self-sufficient and isolated from other networks, Industry 4.0 is increasingly networking systems and controllers with the IT network. The aim is to optimize and automate processes. However, the first malware programs such as Stuxnet, Wannacry & Co. showed that this poses a massive threat to the security of entire industrial systems. Security through intelligent firewalls, IDS systems and other protective measures is therefore extremely important, although the requirements differ greatly between the classic IT world and a manufacturing environment. In addition, high standards are set for the operational safety of industrial networks.

Course Contents

- Typical attacks on factory environments and security vulnerabilities
- Risk analysis
- Communication routes in the ICS and their protection
- Security concepts for linking IT and manufacturing
- Identity and Access Management (IAM)
- Device Hardening and Virus Scanner – Design and Implementation in ICS
- Security through visibility and transparency
- Firewalls – Design and Implementation in ICS
- Intrusion Detection Systems (IDS) – Design and Implementation in ICS
- Remote maintenance access and VPNs for predictive maintenance – design and implementation in ICS
- Wireless LAN and WirelessHART: Security vulnerabilities and their protection
- Smartphones and tablets in the ICS
- Security Information and Event Management (SIEM) in the ICS
- Design and Architecture of Industrial Security Solutions: IEC-62443
- Protection of specific protocols such as PROFINET, Modbus, Ethernet/IP, etc.
- Further standards and best practices
- Safety – regulations and implementation

E-Book The detailed digital documentation package, consisting of an e-book and PDF, is included in the price of the course.

Target Group

This course is aimed at network administrators and network planners who need to plan and implement a security policy in industrial environments. Practical examples and traces deepen the knowledge gained.

Prerequisites

For successful participation, basic knowledge of industrial networks is required, as taught in the courses Industrial Ethernet I - Design and Implementation and Industrial Ethernet II - Special Requirements and Protocols.

This Course in the Web



You can find the up-to-date information and options for ordering under the following link:

www.experteach-training.com/go/SEFA

Reservation

On our Website, you can reserve a course seat for 7 days free of charge and in a non-committal manner. This can also be done by phone under +49 6074/4868-0.

Guaranteed Course Dates

To ensure reliable planning, we are continuously offering a wide range of guaranteed course dates.

Your Tailor-Made Course!

We can precisely customize this course to your project and the corresponding requirements.

Training	Prices, excl. of V.A.T.	
Classes in Germany	3 Days	€ 2,195
Online Training	3 Days	€ 2,195
Date/course venue	Course language German 	
22/10-24/10/25  Frankfurt	22/10-24/10/25  Online	

Status 05/07/2025



EXPERTeach



Table of Contents

Industrial Security – Security Management, Firewalling and Safety in OT

1 Grundlagen industrieller Sicherheit	Sicherheitslösungen	5.5 Anomalie und Threat Detection
1.1 Industrie 4.0: Neue Risiken und Herausforderungen	3.5.1 Visibility und Transparenz	5.6 Security Monitoring
1.2 Begriffe und ihre Bedeutung	3.5.2 Design von Fernwartungszugängen am Beispiel Siemens	5.7 Security Responding
1.3 Sicherheitsempfehlungen für industrielle Netzwerke	3.6 Zugriffsschutz auf Systeme und Netze	6 Best Practices und Trends
1.4 Maßnahmen und Tools zur Steigerung von Sicherheit und Verfügbarkeit in der Industrie	3.6.1 Komponenten	6.1 Best Practices
1.4.1 Lösungen zur Umsetzung der Sicherheitsmaßnahmen	3.6.2 MAC Address Bypass	6.2 Trends und Ausblick
1.4.2 Fernwartungszugang	3.6.3 Secure Group Tagging	
1.4.3 IDS/IPS-Systeme	3.7 Firewalls – Design und Umsetzung im ICS	
1.4.4 Security Information and Event Management – SIEM	4 Sicherheit von industriellen Netzwerkprotokollen	
1.5 Bekannte Bedrohungen und Trends	4.1 Entstehung Feldbus-Systeme und Industrielles Ethernet	
1.6 Risikoanalyse	4.2 Modbus	
1.7 Standards	4.3 Profibus	
1.8 Typische Anbieter	4.4 Profinet	
2 Safety – Vorschriften und Umsetzung	4.5 EtherNet/IP	
2.1 Definition	4.6 Wireless ICS-Technologien	
2.2 Entwicklung	4.6.1 WirelessHART	
2.3 Vorschriften	4.7 Wireless LAN (WLAN)	
2.4 Handlungsempfehlungen	4.7.1 Authentisierung im WLAN	
3 Sicherheitskonzepte für die Kopplung von IT und Fabrikation	4.7.2 Neue Mechanismen für mehr Sicherheit im WLAN	
3.1 Sicherheitsaspekte in Fabrikationsumgebungen	4.7.3 WPA: Wi-Fi Protected Access	
3.2 Kommunikationswege im ICS	4.7.4 Authentisierung nach IEEE 802.1X	
3.3 Typische Angriffe und Sicherheitslücken	4.7.5 IEEE 802.11i	
3.3.1 Angriff auf Netzwerke	4.7.6 Protected Management Frames	
3.3.2 Angriff auf Server	4.8 OPC – Open Platform Communications	
3.3.3 Client Site Attacks	4.9 Local Area Networks (LANs)	
3.3.4 Mobile Endgeräte angreifen	4.9.1 MAC Spoofing	
3.3.5 Social Engineering	4.9.2 ARP Cache Poisoning	
3.3.6 Angriffe im Internet of Things	4.9.3 Neighbor Solicitation	
3.3.7 Cloud Security	4.9.4 Flooding der Switching Table	
3.3.8 Advanced Persistent Threats	4.9.5 VLAN Hopping	
3.4 Typische Angriffe auf Fabrikumgebungen	4.9.6 Mirror Ports	
3.4.1 Physikalischer Zugriff	4.9.7 DHCP Spoofing	
3.4.2 Ungeschützte Netzzugänge	4.9.8 Router Advertisements	
3.4.3 Mobile Endgeräte und Wechseldatenträger	4.9.9 Schutz von LAN-Umgebungen	
3.4.4 Türschließsysteme und Thermostate	5 Cyber Risk: Erkennung, Auswertung und Reaktion	
3.4.5 Fernwartungszugänge	5.1 Cyber Risk in Fabrikumgebungen	
3.4.6 Watering Hole Attacks	5.2 Risiken	
3.5 Design und Architektur von industriellen	5.3 Sicherheitsmetriken	
	5.4 Situative Awareness	

