Course description

IT Security for Production Systems

Level of difficulty	Medium
Learning time	6 h
Additionally recommended learning media	Basics of Network Technology (Evaluation), Commissioning IT Security Package (Video)
Course type	eLab
Theme category	Network and Security

After completion of the training, the learners know, among other things, the common terms in the context of cyber security. They will be able to analyze the security requirements of industrial communication systems and classify the different terms, such as switching and monitoring. They know the hazards and risks and can derive and apply security measures, such as protection against sabotage or securing manufacturing know-how.

No.	Task	Method	Competency level	Content	Competencies	Learning time	HW/ SW depending
Learning unit 1: Basics of IT Security							
1	Basics of network technology	Guidance text supported Method	Knowledge	▪ Network ▪ Task of the network technology ▪ advantages and disadvantages ▪ Wired and wireless transmission ▪ Range (WLAN/ LAN) ▪ Data transmission rate	▪ Can explain the structure and function of a network. ▪ Can name the background for the use of networks. ▪ Can name advantages and disadvantages of network technology. ▪ Can distinguish between wired and wireless transmission. ▪ Know the difference between WLAN and LAN range. ▪ Know the difference in data transmission rate between WLAN and LAN.	45 min.	No
2	Network components	Explore	Knowledge	▪ Router ▪ Repeater ▪ Switch ▪ Modem ▪ Hub ▪ Access point	▪ Can classify common terms related to network components. ▪ Can reproduce common terms such as router, switch, repeater, modem, hub, access point. ▪ Can describe the difference between switch, hub and repeater.	30 min.	No

No.	Task	Method	Competency level	Content	Competencies	Learning time	HW/ SW depending
3	IT security requirements in the production environment	Case study	Apply	▪ Security requirements ▪ Interference attacks ▪ Business models ▪ Access rights ▪ Requirements / specifications ▪ Federal Office for IT Security	▪ Can analyse safety requirements and functionalities of industrial communication systems and controls. ▪ Know the possible input channels of interference attacks. ▪ Know different types of platform-based business models. ▪ Can apply the regulations of the Federal Office for IT Security in Information Technology (BSI). ▪ Know the terms specifications and requirements and can reproduce them. ▪ Can classify the essential points such as access rights, type of data and regulatory requirements on the basis of specifications. ▪ Can comply with operational requirements and legal regulations on IT security and data protection. ▪ Can advise customers on IT security and data protection requirements.	30 min.	No

No.	Task	Method	Competency level	Content	Competencies	Learning time	HW/ SW depending
Learning Unit 2: Implementing and Monitoring Security Measures							
4	Commissioning network devices	Guidance text supported Method	Apply	▪ IP address ▪ Network scanning ▪ Switch technology ▪ Router ▪ Siemens Proneta ▪ Configuration	▪ Can configure an IP address in Windows. ▪ Can scan a PROFINET network with the commissioning tool. ▪ Can detect and physically locate devices based on scans. ▪ Know how to reset a network device to factory defaults. ▪ Can configure IP addresses on network devices. ▪ Can load a device configuration.	45 min.	Yes
5	Protection of a PLC	Guided text Method	Apply	▪ Password protection ▪ Password Policy ▪ Role-based access control ▪ PLC function sets	▪ Know the principles of authentication. ▪ Know the principles of software integrity protection. ▪ Know the background of the different user roles ▪ Know the basic password requirement and password management. ▪ Know the different access levels of a Siemens PLC. ▪ Can restrict access to a PLC according to the levels with specific passwords. ▪ Can specify network components. ▪ Can set up and assign access profiles (roles). ▪ Can configure different access levels for a PLC web server.	45 min.	Yes

No.	Task	Method	Competency level	Content	Competencies	Learning time	HW/ SW depending
6	Switching principles and monitoring of insecure connections	Guided text Method	Apply	▪ Ethernet protocol ▪ MAC addresses ▪ ARP protocol ▪ Wireshark	▪ Know the common terms and can classify them. ▪ Can capture network traffic with Wireshark. ▪ Can monitor ping with Wireshark. ▪ Can analyse and reproduce their findings using different types of filters. ▪ Know the principles of Layer 2 communications including address resolution. ▪ Can manage the ARP cache on a Windows PC. ▪ Can analyze the source address table in the switch. ▪ Can change ports of subscribers. ▪ Know the address table and its meaning. ▪ Can analyze the source address table and ARP cache of a switch. ▪ Know the security risks of unencrypted access protocols. ▪ Can monitor and read unencrypted messages on your own PC. ▪ Can redirect and monitor network traffic using a managed switch. ▪ Can prove the effectiveness of encryption protocols using traffic captures.	45 min.	Yes
7	Routing and firewalls	Guided text Method	Apply	▪ Routing Principles ▪ Network masks ▪ Firewall ▪ Example of communication ▪ Wireshark ▪ Protocols ▪ Security mechanisms ▪ DHCP	▪ Can verify the effectiveness and efficiency of the implemented IT security measures. ▪ Can manually evaluate permitted and prohibited accesses to the firewall. ▪ Can define security mechanisms, in particular access options and rights. ▪ Can load the configuration files for a router. ▪ Can work with different PLC protocols. ▪ Know the rules to ensure certain traffic. ▪ Can analyze and evaluate the communication with Wireshark. ▪ Know the different variations of the rules including logging.	45 min.	Yes

No.	Task	Method	Competency level	Content	Competencies	Learning time	HW/ SW depending
8	VPN connection	Guided text Method	Apply	▪ VPN ▪ Cryptography ▪ Introduction ▪ VPN function ▪ IPsec Overview	▪ Can verify the effectiveness and efficiency of the implemented IT security measures. ▪ Can evaluate the effectiveness of security measures using Wireshark. ▪ Can load a configuration file for a router. ▪ Can prepare and activate a VPN channel. ▪ Can load a configuration w / o VPN. ▪ Can configure a VPN connection. ▪ Can change the standard cryptographic protocols. ▪ Can perform various test configurations. ▪ Can check error messages in the log. ▪ Can modify standard cryptographic protocols. ▪ Can test and troubleshoot the configuration.	45 min.	Yes