SIEMENS

Security in Industrial Networks with SCALANCE (IC-SECINP)

Type

Instructor-led Learning

Duration and Continuing Education Units (CEU)

3 Days
0 CEUs

Target Group

- Engineer
- Commissioning
- Operator
- Other
- Maintenance
- Programmer
- Reliability
- Sales

Short Description

It is difficult to imagine day-to-day industrial operations without Ethernet connections. From large-scale production systems to the smallest Industrial Ethernet communication networks, nearly everything has come to depend on their reliability and security. The opportunities on the one hand are countered by risks on the other hand. Access by outsiders or manipulation in the network always has catastrophic consequences for production or in-house expertise. Therefore, functioning security systems are an absolute must. In this course you will learn the potential dangers and risks in industrial networks and how to assess them. You will be shown numerous ways to improve the protection of know-how and process sequences from attacks, espionage, and manipulations. During the course you will become familiar with knowledge necessary to apply concepts mandated by common security standards. Because the course does not just cover theoretical security concepts, there is also ample opportunity to implement them in practical exercises.

Objectives

- At the end of this course, you will know the requirements and fundamentals needed to plan, implement, and provide support for industrial security measures.

Content

- Current trends and security risks
- Defense-in-depth with Siemens - a holistic security concept
- Update and replacement of security components
- Potential threats in a network
- Basic security measures (ports, passwords, protocols, etc.)
- Cell protection concept
- Access restriction
- Connection of standard machines to networks
- Remote access via VPN
- Comprehensive exercises using the SIMATIC NET product portfolio

Recommended Prerequisites

IC-ETHFU: IC-ETHFU

Language

English