SIEMENS

Industrial Networking

Security in Industrial Networks

General Information

Course Code: IEN-SECINS1A
Length: 3 Days

Audience

This course is for users who are involved with developing or sustaining automation networks in an industrial environment. This includes, but is not limited to the following:

- Plant Engineers
- Control Engineers
- System Engineers
- Commission Engineers
- Application Engineers
- Operations or IT Network Engineers
- Facility Managers
- Project Engineers

Prerequisites

- Basic knowledge of the topic "Ethernet".
- Familiar with network topologies, transfer processes, addressing, data transport, and understand the associated technical vocabulary.
- Familiar with the principles of router operations, switches and an OSI reference model.
- Recommended: Completion of the web-based Initial Training for Industrial Networks (ITIN) course. (https://sitrain.automation.siemens.com/sitrain/open_wbt/ie_data_communication/index.html)

Profile

This course is one of three certification courses offered under the Siemens Certified Engineer for Industrial Networks (CEIN) program. The curriculum includes an introduction of the potential threats and risks associated with industrial networks, as well as a deep dive into defense in depth strategies. Students will be shown numerous ways to implement access control measures to protect and mitigate security incidents.

Throughout the course, students will have ample time for practical exercises, diagnostics, and troubleshooting. The course uses a hands-on model for realistic demonstrations.

At the end of the course, students are equipped with the knowledge to plan, configure, implement and provide support for industrial security measures in automation networks.

Objectives

Upon completion of this course, the student shall be able to:

- Current trends and security risks
- Defense in depth strategies
- Update and replacement of security components
- Potential threats in a network
- Basic security measures (ports, passwords, protocols, etc.)
- Network segmentation (VLAN, routing)
- Cell protection concept
- Access restriction
- Remote access via VPN
- Diagnostics / troubleshooting
- Comprehensive exercises using the SIMATIC NET product portfolio

Topics

1. Comprehensively protecting productivity
2. Maintenance
3. Risks
4. Basics of security
5. Cell protection
6. Access protection
7. Standard machines
8. Remote maintenance