SIEMENS

Basics of Industrial Security in the Factory Automation / 工业信息安全基础 (A7835)

Objectives

The training provides an overview of the defense-in-depth protection concept of plants. The aim is for participants to become familiar about dangers for plants with factory automation, analyze potential vulnerabilities and assess risks. In the course, participants will obtain knowledge on which countermeasures can be applied for the different areas of the concept.

Target Group

Programmers, Configuration engineers, Project planners

Content

- What are the differences between office and industrial security?
- What is industrial security required for (threats, incidents)?
- What is covered by the security concept defense in depth?
- An introduction to user management with the TIA Portal
- Controller security — system integrity for SIMATIC controllers
- An introduction to authentication and encryption mechanisms
- Secure communication mechanisms of the SIMATIC CPU S7-1500
- HMI security — HMIs and sm@rt Server protection mechanisms, user concept for HMI Runtime
- PC security — different measures for hardening as well as user and patch management of PC systems, detection of malware
- Network security — Hardening of network components
- The cell protection concept and the realization of remote maintenance access
- Mechanisms for access protection to networks
- Plant security — physical and organizational security measures and continuous processes

Prerequisites

Attendance of A7811 course and network knowledge is recommended

Type

Face-to-face training

Duration

2 days

Language

zh