SIEMENS

On line-Training Configurazione e Programmazione Sicura dei Sistemi di Automazione (DI-S7HARD)

Short Description

Cyber incidents involving automation and control systems at industrial sites continue to grow exponentially. The impact they have can have very serious consequences, not only for the production cycle but also for the protection of people and property.
Malware come **WannaCry**, **Industroyer** e **Petya/NotPetya** since 2016 have given rise to large-scale attacks. The solution, however, is not only the adoption of the latest technology, but above all the proper preparation of personnel throughout the company, who very often represent the weakest link in the entire security chain. For this reason, we offer a training course dedicated to the configuration and programming of automation systems (PLC, HMI, Drive) with a cybersecurity-oriented approach, providing programmers with the necessary skills to implement hardening of the various devices and security 'by design' in the application software and thus increase the level of resilience of the entire automation system. The course is based on more than 20 years of experience with SCADA, PLC, fieldbus, remote I /O systems.

Objectives

- Understand cybersecurity aspects specific to OT applications
- Identify the potential cyber risks of an automation system
- Design a PLC, HMI and SCADA system that offers enhanced protection against cyber attacks
- Write a PLC application that includes cyber security "by design
- Diagnosing and correcting PLC program execution problems with an impact on cyber

Target Group

- PLC and HMI/SCADA programmers
- Maintenance and installation technicians
- Machine and plant operators and operators

Content

Cybersecurity OT:
- The impact of cyber security
- The scenarios and technologies
- The characteristics of ICS and SCADA applications
- The different types of attacks
- The MITRE ATT&CK for ICS
- Vulnerabilities in automation products
- References to the IEC62443 standard

The basics of networking and security:
- The elements of a network, network types and zones
- Secure communication protocols
- Basic concepts of cryptography and hashing
- Segmentation, segregation and isolation of networks
- Tunnelling and VPN
- Security devices
- OT/ICS architecture monitoring

Safe PLC programming:
- Modular and structured programming
- Monitoring of correct PLC operation
- Safe management of the programme execution and recovery cycle
- PLC memory management and optimisation
- Software and data integrity check
- Validation of input/output and internal resources (timers, counters, function blocks)
- Secure interaction with HMI and SCADA devices
- Monitoring, logging and management of alerts and events
- Secure communication with other devices

PLC Hardening (SIMATIC S7-300/400, SIMATIC S7-1200/1500):
- Physical protection of a control system (padlock, display password in SIMATIC S7-1500, disabling unused ports)
- Hardware access protection (write/read password management)
- Software protection (know-how protection, project copy)
- Project protection (user and role definition)
- Data protection (confidential PLC configuration, secure S7/OUC/OPC UA communication, web server)
- Remote access with dedicated CP (VPN, SINEMA)
- Monitoring of potential unauthorised access (access log, cycle time monitoring, ...)

HMI Hardening (SIMATIC WinCC Comfort, SIMATIC WinCC Unified):
- Physical protection of a supervisory system (user management for device access, USB port management)
- Project transfer using a private key
- Secure communication with a control system (Secure S7, OPC UA)
- Functionality protection (user authorisation management)

- Remote access (Sm@rt options)

Type

Online-Training

Duration

2 days

Language

it