

On line-Training Configurazione e Programmazione Sicura dei Sistemi a Controllo Numerico (DI-CNHARD)

Short Description

Cyber incidents involving the automation and control systems of 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 such as **WannaCry**, **Industroyer** and **Petya/NotPetya** have given rise to large-scale attacks since 2016. However, the solution is not only the adoption of the latest technological advances, but above all the adequate preparation of the staff of the entire company, which very often represents the weak 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, CN) with a cybersecurity-oriented approach, which provides programmers with the skills necessary to implement the hardening of the various devices and security "by design" in the application software and therefore increase the level of resilience of the entire automation system. The course is the result of over 20 years of experience on SCADA, PLC, fieldbus, remote I/O and numerical control systems.

Objectives

After attending the course you will be able to:

- Understand aspects of cybersecurity specific to OT applications
- Identify potential cyber risks of an automation system
- Design a PLC, HMI and CN system that offers greater protection against cyber attacks
- Write an industrial application that includes cyber security "by design"
- Diagnose and correct automation program execution problems impacting cyber

Target Group

- CNC programmers
- Maintenance workers and installers
- Operators and managers of machines and systems

Content

OT cybersecurity

- The impact of cybersecurity
- Scenarios and technologies
- The characteristics of ICS and SCADA applications
- The different types of attacks
- The MITER ATT&CK for ICS
- Vulnerabilities in automation products
- Notes on the IEC62443 standard

The basics of networking and security

- The elements of a network, types of networks and zones
- Secure communication protocols
- Basic concepts of encryption and hashing
- Segmentation, segregation and isolation of networks
- Tunneling and VPN
- Safety devices
- Monitoring of the OT/ICS architecture

Safe PLC programming

- Modular and structured programming
- Monitoring the correct operation of the PLC
- Safe management of the program execution and recovery cycle
- PLC memory management and optimization
- 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

CN Hardening

- Physical separation of machine networks from the company network
- Password and keyswitch
- Automatic Password deactivation via PI_SERV
- Data access management via USER_CLASS
- Customization of softkey display via access level
- Lock MyCycle option
- CNC Lock Function option (only for SINUMERIK 828d)
- Know How drive protection (parameter exception list)
- Use of the network/MMP drive for sharing Part Programs, avoiding the use of USB Stick

IPC/PCU Hardening

- Obsolete products (little or no IT security) PCU Retrofit
- Firewall (manual activation of ports on the company network)
- Basic Software Update
- Windows Updates
- Whitelisting

Corporate and remote connection protection

- VNC password on corporate network
- SSH Key file for connection via Access MyMachine
- OPC UA (encryption, anonymous access, data write rights)
- Using SCALANCE S
- SINEMA Remote Connect

Security of the machine in case of external attack

- External backup of machine archives (to avoid loss of archives)
- External backup of PartPrograms (to avoid loss of programs)
- Centralized tool management (MMR/Tools) (to avoid losing tools)
- Collision Avoidance/Protect MyMachine option (to avoid collisions)
- Monitoring Tool Speed/Acceleration option (to avoid tool damage)

Fast system recovery

- NC recovery: frequent archives, backup of updated PLC program (SIMATIC STEP 7, TIA Portal)
- IPC/PCU Reset: Updated Ghost
- CF/SD Card recovery: updated TGZ, paper management of licenses

Type

Online-Training

Duration

2 days

Language

it