SIEMENS

Cybersecurity in the factory automation (ST-SECFAB)

Short Description

The training provides an overview of protection concepts against current cyber threats in industry and how industrial plants and machines can be effectively protected using a comprehensive approach. The participants should learn how and which security measures can be implemented using concrete examples using the security portfolio of Siemens Digital Industries (DI).

Objectives

In the course, participants acquire knowledge of which countermeasures and portfolio elements can be used to protect industrial plants and machines against cyber threats.

Target Group

Machine builders, system integrators, plant operators
Cybersecurity Officers, those responsible for cybersecurity
Project manager, project staff
Technologists
Project planners, programmers
Commissioning engineer

Content

Awareness and understanding of cyber security threats & risks for industrial production facilities
Demonstration of security concepts, standards and best practices adapted and optimized for the industry based on use cases and by using the automation portfolio of Siemens Digital Industries.
How the integrated security functions in the DI Security Portfolio can be configured and used in combination with a holistic security concept.
What does the Defense in Depth security concept include?
Getting started with user administration with 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
Network security – the cell protection concept and the implementation of remote maintenance access
Plant security – physical and organizational security measures

Prerequisites

Basic knowledge about industrial automation
Basic knowledge about industrial communication

Type

Face-to-face training

Duration

3 days

Language

nl

Fee

1,750 EUR