OT Security with TIA Portal: Protection for Industrial Automation

OEM: Siemens • Code: TIA-OTSEC

COURSE DESCRIPTION

This training was conducted until March 03, 2026 under the course number ST-SECFAB.

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). Practical exercises in TIA Portal allow participants to better understand the concepts and apply them directly.

AUDIENCE PROFILE

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

PREREQUISITES

- Basic knowledge about industrial automation
- Basic knowledge about industrial communication
- Basic knowledge in SIMATIC TIA Portal Step 7
- Technical requirements
- Note
- Included in the course price: Free access to the digital learning platform SITRAIN access – starting one week before the start of the course until two weeks after the end of the course.
- With the Learning Membership, you can deepen or repeat the content of this Learning Event as well as continue your education on other interesting topics.

COURSE OBJECTIVES

By the end of this course, participants will be able to:

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

COURSE OUTLINE

Module 1: 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
- Drives – Hardening