SIEMENS

Cyber Security in Energy Automation - Module 4: Threat Scenarios for Industrial Networks (Virtual Training) (CS-4AWA)

Objectives

To familiarize participants with current Cyber Security issues and recognized dangers, using interesting Live Demos to underscore the importance of Cyber Security measures.

Target Group

Interested computer and network users.

Content

ICS (Industrial Control System) Threats with Live Demos
- Man in the Middle
- Malicious Traffic
- Phishing
- Virus, Worms, Trojans (Code Red, Stuxnet)
- Data Theft
- Ransom ware (Krypto trojans)
- Remote Access
- Shodan ICS Radar (https://ics-radar.shodan.io)
- Access to Local Service LAN
- Layer-2 Hacking
- D(D)os

Prerequisites

Interest in technical issues.

Note

Structure of the lecture: Theory 100 %

This training can be booked as FACE-TO-FACE Training too.

CONTACT
If you have any questions, please contact directly **Power Academy Vienna**
power-academy.at@siemens.com
Mrs. Monika Schuecker
monika.schuecker@siemens.com
+43 51707 31143

Type

Online-Training

Duration

1 day

Language

en