

Networks in Energy Automation - Module 2: Switching, Hacking and Protection (NT-2SWHS)

Objectives

To understand the distinctive features of automation system networks and their specific switching requirements; to apply theoretical knowledge in a LAB environment, using a typical network of automation units, like SIPROTEC and SICAM RTUs; to investigate redundancy requirements and possible security issues.

Target Group

Engineers and project leaders who are involved into the design of automation systems.

Content

Switching Technologies with special protocols (IEC 61850)

- Switching Basics (Layer-2)
- Switching Vulnerabilities and Hardening

Layer-2 redundancy protocols (STP, RSTP, MRP, HSR and PRP)

- LAB: STP/RSTP Vulnerabilities and Hardening

VLAN (Virtual Local Area Network)

- LAB: RSTP with SIPROTEC und SICAM RTUs
- LAB: Goose Hardening

Layer-2 Hardening

- LAB: Vulnerabilities and Hardening (RUGGEDCOM Switch)
- DHCP: Vulnerabilities and Hardening

Prerequisites

Basic knowledge of network and automation technology is necessary.

Note

Structure of the lecture: Theory 40 % / Practical Exercises 60 %

This training can be booked as [VIRTUAL CLASSROOM 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

Face-to-face training

Duration

2 days

Language

en

Fee

2,080 EUR