

Cyber Security in Energy Automation - Module 6: Best Practice Engineering (CS-6BPE)

Objectives

To practice in a LAB environment the theoretical knowledge gained in the course [Cyber Security in Energy Automation - Basics](#), especially with regard to hardening of network systems and components.
This course also provides a practical introduction to the security solutions recommended by Siemens as part of its product solution "Secure Substation".

Target Group

Technicians who are to design network devices and devices of the SICAM RTUs product line in automation systems and implement solutions regarding cyber security.

Content

Overview Products and Security Features
Encryption (symmetric/ asymmetric) theory
PSK (Pre Shared Key)
PKI (Private Public Key Infrastructure) theory
NTP Configuration

- Secure NTP (PSK)

VPN IPSec (PSK)

- Tunnel/Transport mode
- LAB IPSec

Use of certificates
IEC 60870-5-104 extension based on IEC 62351-3
Client certificates for engineering
Automated enrollment of certificates per GridPass
Extended network segmentation

- Network segmentation VLANs
- Practical exercises and UseCases

Next Generation Firewalls

- Rules and regulations for firewalls

FWI4 (internal IEC 60870-5-104 Application Layer Gateway)

- Use Cases

Central user/ password management

- Radius authentication
- Switches, Routers and SICAM RTUs

Logging and Reporting

- Switches, Routers and SICAM RTUs

SNMPv3

- Switches, Routers and SICAM RTUs

System hardening

Prerequisites

Basic knowledge of network and automation technology with SICAM RTUs is necessary.

Note

Structure of the lecture: Theory 30% / Practical Exercises 70%
al-Training"> 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

4 days

Language

en

