



Online Training: Fundamentals of Electrical Substation Cybersecurity

 2 days

 English

 oCcyb03en

Ethernet is a fast, reliable, and scalable Local Area Network (LAN) technology that is becoming the predominant standard within modern digital substations. This two-day course provides participants with a solid foundation in Operational Technology (OT) LAN cybersecurity fundamentals. Through a blend of lectures, instructor-led demonstrations, and hands-on lab exercises, participants will learn how to recognize cybersecurity risks and apply practical mitigation strategies in substation environments.

Objectives

- ▶ Recognize and analyze common cybersecurity attacks relevant to substations
- ▶ Differentiate between IT cybersecurity and OT substation cybersecurity
- ▶ Understand and apply the principles of Defense-in-Depth
- ▶ Interpret and apply the NIST Security Framework in OT environments
- ▶ Identify typical substation attack vectors and potential vulnerabilities
- ▶ Understand the different techniques utilized by intrusion detection systems (IDS): signature-based, learning-based, system-model based
- ▶ Configure and monitor a functional security monitoring system using StationGuard

Content

- ▶ Case Studies: Cybersecurity Attacks We Can Learn From
- ▶ IT vs OT security within substation environments
- ▶ Regulatory Overview: FERC, NERC-CIP
- ▶ Defense-in-Depth principles applied to electrical substations
- ▶ Typical electrical OT substation communications architecture (the Purdue Model)
- ▶ The NIST Cybersecurity Framework
- ▶ Typical substation attack vectors and mitigation examples
- ▶ IPv4 addressing and subnetting
- ▶ Introduction to static routing
- ▶ Network Address Translation (NAT/PAT)
- ▶ Introduction to firewalling (Layers 1–4)
- ▶ IPsec/VPN Tunneling concepts
- ▶ Intrusion Detection concepts
 - ▶ Signature-Based IDS
 - ▶ Learning-Based IDS
 - ▶ System-model based IDS (StationGuard)
- ▶ Vulnerability management and grid visibility (GridOps)

Solutions

StationGuard, GridOps OMICRON
DANEO 400, IEDScout,
StationScout

Audience

Electrical engineering staff from
transmission and distribution utilities,
IT and cybersecurity officers from
utilities, service companies, and
manufacturers involved in protection
system design and maintenance

Prerequisites

Completion of LAN Design course
preferred