# Cybersecurity in Substations –
# Important Basics for Protection and SCADA Engineers

| 🕐 1 hour | 🗨 English | # Wpuc04en |
|---|---|---|

Cybersecurity requirements are increasingly becoming part of the daily work of protection and control engineers. The aim of this webinar is therefore to gain some important basic knowledge of Cybersecurity in substations. In addition, the technical mechanisms of cyber attacks will be explained in order to gain a deeper understanding of Cybersecurity.

After this webinar you will be familiar with the basic concepts of a comprehensive Cybersecurity strategy for substation networks.

## Objectives

> Understanding the basic concepts of OT Cybersecurity
> Learning how cyber attacks on substations work
> Applying the NIST Security Framework v1.1 in substations
> Understanding the security mechanisms in IEC 61850 communication

## Content

> Cybersecurity frameworks and legal requirements
> How to apply the NIST Security Framework in substations
> Previous cyber attacks and what we can learn from them
> Basics of attacks, security holes and exploits
> Security in IEC 61850 communication

## Solutions

Intrusion Detection System StationGuard, cyber-secure IEC 61850 testing with StationScout

## Audience

Protection, and SCADA engineers and security officers in utilities

## Prerequisites

Basic knowledge about protection and SCADA systems

OMICRON
Academy