CORE CONCEPT

OT Cybersecurity Course: IEC 62443 Zones and Conduits, Risk Assessment and ICS Incident Response

OT Cybersecurity Course: IEC 62443 Zones and Conduits, Risk Assessment and ICS Incident Response

Introduction:

OT cybersecurity, covering IEC 62443 zones and conduits, risk assessment and ICS incident response, is a 1-week course for control systems, automation, OT security and IT security staff in energy, utilities, manufacturing and process facilities, ending with an OT Security Improvement Plan. Many plants connect control systems to business networks and remote vendors without segmentation, asset visibility or a tested response plan, leaving production and safety exposed to cyber incidents. Nominees already maintain or secure control systems or networks, and teaching is by case study on plant architectures and incident scenarios. CoreConcept Training Center delivers this OT cybersecurity course.

Course Objectives:

- Map an industrial control system architecture against the Purdue reference model and identify its critical assets and data flows
- Partition a facility into zones and conduits and set target security levels using the ISA/IEC 62443 series
- Conduct an OT cybersecurity risk assessment that weighs safety, production and environmental consequences
- Design network segmentation, an IT/OT DMZ and secure remote access for vendors and engineers
- Plan asset inventory, passive monitoring, patching and vulnerability management that respect plant availability
- Prepare an ICS incident response playbook and an OT Security Improvement Plan aligned with NIST SP 800-82 Rev. 3

Target Audience:

- Control systems engineers responsible for DCS, PLC and SCADA design and maintenance
- Automation technicians responsible for field devices, controllers and engineering workstations
- OT security staff responsible for industrial network protection and monitoring
- IT security staff responsible for extending security operations to plant networks
- Plant operations and maintenance leads responsible for production continuity and system changes
- Project and integration engineers responsible for supplier and system integrator deliverables

Course Outline:

Day 1: Industrial Control Systems and the OT Threat Landscape

- Purdue Reference Model Levels and OT Data Flows
- DCS, PLC, SCADA and Safety System Architecture Review
- IT and OT Security Priority Differences and Constraints
- Industrial Cyber Incident Case Histories and Lessons
- Current Plant Architecture Baseline and Asset Criticality

Day 2: Security Standards, Zones and Risk Models

- ISA/IEC 62443 Series Structure and Stakeholder Roles
- Zone and Conduit Partitioning of an Industrial Facility
- Security Levels and Foundational Requirements Assignment
- OT Cybersecurity Risk Assessment With Consequence Ranking
- NIST SP 800-82 Rev. 3 OT Overlays and Controls

Day 3: Securing Industrial Networks and Operations

- Network Segmentation and Industrial Firewall Rule Design
- IT/OT DMZ Architecture for Historians and Data Transfer
- Secure Remote Access for Vendors and Engineers
- OT Asset Inventory and Passive Network Monitoring
- Patch and Vulnerability Management Within Plant Availability

Day 4: Incidents, Supply Chain and Problem Cases

- ICS Incident Detection, Triage and Escalation Paths
- OT Incident Containment Without Unsafe Plant Shutdown
- Safety Instrumented System Protection and Separation Checks
- Supplier and System Integrator Security Requirements
- Removable Media and Engineering Workstation Hardening Controls

Day 5: Case Study Work and the OT Security Improvement Plan

- Gas Processing Plant Case Study on Zone Design
- Water Utility Case Study on Remote Access Risk
- Manufacturing Plant Case Study on Ransomware Response
- ICS Incident Response Playbook Drafting and Tabletop Review
- OT Security Improvement Plan Completion and Prioritisation

Skills You Will Gain:

- OT Architecture Analysis
- Zone and Conduit Design
- Industrial Cyber Risk Assessment
- Network Segmentation Design
- Secure Remote Access Planning
- OT Vulnerability Management
- ICS Incident Response
- Supplier Security Requirements

Why Attend This Course:

- Deliver an OT Security Improvement Plan with a zone and conduit model, risk register and incident playbook to the plant manager and the chief information security officer
- Decide which zones, conduits and security levels a facility needs and which controls to fund first
- Avoid production outages, unsafe shutdowns and uncontrolled vendor access caused by flat networks and untested response plans
- Brief operations and maintenance colleagues on the remote access, media and incident procedures practised in the case studies

Conclusion:

Back at work, the participant gives the OT Security Improvement Plan to the plant manager, the chief information security officer and the engineering and maintenance leads. They use it to agree segmentation changes, remote access rules and the incident response roles for control systems. After the first improvement cycle or tabletop exercise, the organisation should review asset coverage, open vulnerabilities and response times against the plan and adjust priorities where risks remain high.

Frequently Asked Questions FAQ:

What should participants know before an OT cybersecurity course?

Participants should understand either industrial control systems or IT networks and security, and be willing to learn the other side. Bringing a simplified network diagram or asset list from their facility helps them apply the case studies to their own plant.

How does an OT cybersecurity course differ from a general IT cybersecurity course?

IT courses protect data and office systems where confidentiality comes first. This course protects control systems where safety and availability come first, using ISA/IEC 62443 zones and conduits, plant-safe monitoring, patching limits and incident response that avoids unsafe shutdowns.

Why are zones and conduits central to OT cybersecurity under IEC 62443?

Zones group assets with similar security needs and conduits control the communication between them. This lets a facility apply stronger protection to critical systems, limit how an attack spreads and justify controls by risk rather than by product.

What do participants take back from the OT cybersecurity course?

Participants take back an OT Security Improvement Plan with a zone and conduit model, OT risk register, segmentation and remote access designs and an ICS incident response playbook for their facility.