XCELERATE TRAINING INSTITUTE
your learning & development partner

ELECTRICAL ENGINEERING

# OT and Industrial Cybersecurity (IEC 62443) Training Course

Protecting Control Systems in Oil, Gas, Power and Utilities

| DURATION | LANGUAGE | FORMAT | COURSE CODE |
|---|---|---|---|
| 5 days | English or Arabic | Classroom / Online | EE-101 |

## Upcoming dates

| Dates | Venue | Format | Fee |
|---|---|---|---|
| 4 – 8 ????? 2027 | Amman | Classroom | €3?800 |
| 8 – 12 ???? 2027 | Amsterdam | Classroom | €4?800 |
| 17 – 21 ???? 2027 | Barcelona | Classroom | €4?800 |
| 26 – 30 ????? 2027 | Berlin | Classroom | €4?800 |
| 6 – 10 ?????? 2027 | Boston | Classroom | €5?500 |
| 8 – 12 ?????? 2027 | Cairo | Classroom | €3?600 |

### Register or ask a question

Online: x8ti.com/course/ot-and-industrial-cybersecurity-iec-62443-training-c…
+491631686678 · info@x8ti.com

# OT and Industrial Cybersecurity (IEC 62443) Training Course

## Introduction

Industrial control systems that run refineries, power plants, water networks and factories are increasingly connected and increasingly targeted by attackers. A successful attack can cause shutdowns, environmental damage and safety incidents, not just data loss.

This course explains how to secure operational technology (OT) environments using the IEC 62443 series of standards. Participants learn the differences between IT and OT security, how to assess risk, design secure architectures and run an OT security programme without disrupting operations.

## Learning Objectives

By the end of this course, participants will be able to:

- Explain the architecture and vulnerabilities of industrial control systems
- Describe the structure and key concepts of IEC 62443
- Perform OT cybersecurity risk assessments
- Design zones, conduits and secure network architectures
- Apply security controls for OT assets, access and remote connections
- Plan OT incident response and an OT security programme

## Training Methodology

This course combines short expert presentations with practical exercises, case studies from the Gulf and international organisations, group discussions and work with real templates and tools. Participants are encouraged to bring examples from their own work so that the learning can be applied immediately.

Participants analyse industrial case studies and design a zoned architecture for a sample plant.

## Benefits for Your Organisation

- Reduced risk of operational disruption
- Protection of safety and critical infrastructure
- Compliance with industry and national OT requirements
- Better cooperation between IT, OT and safety teams
- Structured OT security programme

## Benefits for You

- Specialist OT security knowledge
- Understanding of IEC 62443 requirements
- Practical risk assessment and design skills
- Ability to bridge IT and engineering teams
- A rare and highly valued competence

## Who Should Attend

This course is designed for:

- Control and instrumentation engineers
- OT, SCADA and DCS engineers
- IT and cybersecurity professionals in industrial companies
- Operations and maintenance managers
- HSE and process safety professionals

## Course Outline

### Day 1: OT Environments and Threats

- Industrial control systems: PLC, DCS, SCADA and safety systems
- Differences between IT and OT security
- Major OT cyber incidents and lessons learned
- Threat actors and attack paths
- Safety and cybersecurity interaction

### Day 2: IEC 62443 Fundamentals

- Structure of the IEC 62443 series
- Roles: asset owner, integrator and product supplier
- Security levels and foundational requirements
- Security programme requirements
- Related standards and national OT guidelines

### Day 3: Risk Assessment and Architecture

- OT asset inventory
- Cybersecurity risk assessment for OT
- Zones and conduits
- Secure network segmentation
- Remote access design

### Day 4: Security Controls and Operations

- Access control and account management
- Patch and vulnerability management in OT
- Monitoring and anomaly detection
- Backup and recovery for control systems
- Supplier and integrator requirements

### Day 5: Incident Response and Programme

- OT incident response planning
- Exercises and drills
- Security metrics for OT
- Building the OT security programme

- Action plan for your facility

**Copyright and intellectual property**
This course, "OT and Industrial Cybersecurity (IEC 62443) Training Course", is an original course by Xcelerate Training Institute. All materials, content and structure are the intellectual property of Xcelerate Training Institute. Reproduction, distribution or use of any part of this course without written consent is prohibited.

# Registration Form

## OT and Industrial Cybersecurity (IEC 62443) Training Course

Preferred dates: ..... Venue or online: .....

Duration: 5 days Language: .....

Please complete and email this form to us, or register online. We confirm your place and send the invoice within one working day.

### Delegate information

Full name (Mr / Ms / Dr / Eng): .....

Position: ..... Telephone / mobile: .....

Official email: ..... Personal email: .....

### Company information

Company name: .....

Address: .....

City / country: ..... VAT / tax number: .....

### Person responsible for training & development

Full name (Mr / Ms / Dr / Eng): .....

Position: ..... Telephone / mobile: .....

Email: .....

### Payment

☐ Please invoice me ☐ Please invoice my company

Signature: ..... Date: .....

**Call**
+491631686678

**Email this form**
info@x8ti.com

**Register online**
Open the course page