Training Course on Cybersecurity for Industrial Control Systems (ICS) and SCADA

Professional Development Training Course Outline

Category	Engineering	**Duration**	10 Days
Base Fee	$3,000 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

Introduction

As industrial automation becomes increasingly interconnected, cybersecurity for Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) networks is critical to safeguarding infrastructure, operations, and national security. Training Course on Cybersecurity for Industrial Control Systems (ICS) and SCADA equips participants with practical, hands-on skills to secure ICS/SCADA environments from growing cyber threats, including malware, ransomware, zero-day attacks, and insider threats. It bridges the gap between traditional IT security and operational technology (OT) by integrating network security, threat detection, incident response, and vulnerability management strategies tailored to industrial systems.

This in-depth course covers the architecture of ICS/SCADA systems, security frameworks like NIST 800-82, threat modeling, and risk assessment in industrial environments. Through real-world case studies—such as the Stuxnet attack, Colonial Pipeline breach, and Ukrainian grid blackout—participants will explore how to design, implement, and maintain resilient security postures for critical infrastructure. Whether you are an ICS engineer, cybersecurity professional, or compliance officer, this course provides the cutting-edge knowledge required to meet the demands of Industry 4.0 and beyond.

Programme Curriculum

Training Course on Cybersecurity for Industrial Control Systems (ICS) and SCADA

Introduction

As industrial automation becomes increasingly interconnected, cybersecurity for Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) networks is critical to safeguarding infrastructure, operations, and national security. Training Course on Cybersecurity for Industrial Control Systems (ICS) and SCADA equips participants with practical, hands-on skills to secure ICS/SCADA environments from growing cyber threats, including malware, ransomware, zero-day attacks, and insider threats. It bridges the gap between traditional IT security and operational technology (OT) by integrating network security, threat detection, incident response, and vulnerability management strategies tailored to industrial systems.

This in-depth course covers the architecture of ICS/SCADA systems, security frameworks like NIST 800-82, threat modeling, and risk assessment in industrial environments. Through real-world case studies—such as the Stuxnet attack, Colonial Pipeline breach, and Ukrainian grid blackout—participants will explore how to design, implement, and maintain resilient security postures for critical infrastructure. Whether you are an ICS engineer, cybersecurity professional, or compliance officer, this course provides the cutting-edge knowledge required to meet the demands of Industry 4.0 and beyond.

Course duration

10 Days

Course Objectives

1. Understand the architecture and components of ICS and SCADA systems
2. Identify vulnerabilities and threats in industrial environments
3. Apply NIST 800-82 and ISA/IEC 62443 cybersecurity frameworks
4. Implement risk-based cybersecurity strategies for ICS networks
5. Detect and respond to cyber intrusions using SIEM tools
6. Perform security assessments and penetration tests on ICS networks
7. Deploy secure remote access and segmentation protocols
8. Mitigate ransomware and APTs in SCADA environments
9. Integrate IT and OT cybersecurity strategies
10. Design incident response and disaster recovery plans for ICS
11. Secure legacy systems with compensating controls
12. Analyze global cyberattacks targeting critical infrastructure
13. Implement continuous monitoring and patch management practices

Organizational Benefits

1. Strengthened protection of critical industrial infrastructure
2. Reduced risk of production downtime and data breaches
3. Improved regulatory compliance (NERC CIP, NIST, ISO 27001)
4. Enhanced visibility and control across OT and IT environments
5. Proactive threat detection and response capabilities
6. Increased trust from customers and stakeholders
7. Cost savings from avoiding security breaches and fines
8. Upgraded cybersecurity awareness among engineering staff
9. Better coordination between IT, OT, and security teams

10. Improved business continuity and operational resilience

Target Participants

- ICS/SCADA Engineers
- OT and IT Security Professionals
- Network Administrators
- Control Systems Designers
- Cybersecurity Auditors
- Critical Infrastructure Operators
- Utility Engineers (Power, Water, Oil & Gas)
- Industrial Automation Technicians
- Compliance and Risk Officers
- Government Cybersecurity Agencies

Course Outline

Module 1: Introduction to ICS and SCADA Systems

1. ICS/SCADA architecture and communication protocols
2. Differences between IT and OT environments
3. Components: PLCs, RTUs, HMIs, DCS
4. ICS lifecycle and operations
5. Case Study: ICS structure in an energy utility

Module 2: Threat Landscape in Industrial Environments

1. Common ICS cyber threats
2. Attack vectors in SCADA systems
3. Insider threats and third-party risks
4. Nation-state and APT actors
5. Case Study: Ukraine power grid cyberattack

Module 3: ICS Cybersecurity Standards and Regulations

1. Overview of NIST 800-82
2. ISA/IEC 62443 series
3. NERC CIP requirements
4. ENISA and global frameworks
5. Case Study: Compliance audit in an oil refinery

Module 4: Network Architecture and Segmentation

1. Purdue Model for ICS networks
2. Network zoning and segmentation
3. Demilitarized Zones (DMZs)
4. Firewalls and secure protocols
5. Case Study: ICS network redesign in manufacturing

Module 5: ICS Asset Inventory and Risk Assessment

1. Building a real-time asset inventory
2. Vulnerability scanning tools for OT

3. Asset risk scoring and prioritization
4. Risk matrices and impact evaluation
5. Case Study: Risk prioritization in water treatment

Module 6: Secure Communication Protocols

1. Modbus, DNP3, OPC UA security
2. Use of VPNs and encrypted tunnels
3. Application whitelisting
4. Secure firmware and patching
5. Case Study: Secure communication in chemical plants

Module 7: Malware and Ransomware in ICS

1. ICS-specific malware overview
2. Ransomware attack lifecycle
3. ICS honeypots and threat intelligence
4. Mitigation strategies
5. Case Study: Colonial Pipeline ransomware attack

Module 8: Security Information and Event Management (SIEM)

1. SIEM for OT environments
2. Log collection and correlation
3. Real-time alerts and dashboards
4. Threat hunting using SIEM
5. Case Study: Incident detection using Splunk

Module 9: Intrusion Detection and Prevention in ICS

1. IDS/IPS technologies for industrial systems
2. Signature-based vs. anomaly-based detection
3. Network behavior analysis
4. Deployment of sensors and probes
5. Case Study: Use of Snort in ICS intrusion monitoring

Module 10: ICS Penetration Testing and Red Teaming

1. Legal and ethical considerations
2. Tools: SHODAN, Metasploit, Wireshark
3. Red team vs. blue team exercises
4. Exploiting ICS vulnerabilities safely
5. Case Study: Pen test in a smart factory

Module 11: Secure Remote Access and Remote Work Risks

1. Remote access tools and vulnerabilities
2. Multi-factor authentication for OT
3. Secure tunneling protocols
4. Vendor access control
5. Case Study: Remote breach in a SCADA system

Module 12: Incident Response and Recovery in ICS

1. ICS-specific IR plans and playbooks
2. Forensics and post-incident analysis
3. System backup and restoration
4. Legal and reporting considerations
5. Case Study: Response to a SCADA hijack attempt

Module 13: Legacy Systems and Compensating Controls

1. Challenges of outdated ICS assets

2. Risk mitigation for unsupported systems
3. Network isolation strategies
4. Application control and hardening
5. Case Study: Legacy control system in rail networks

Module 14: Cybersecurity in Industry 4.0

1. Smart factories and IIoT integration
2. Cybersecurity for edge computing
3. Data integrity in predictive analytics
4. 5G and cloud risks in OT
5. Case Study: IIoT security in food processing

Module 15: Future Trends and AI in ICS Security

1. Role of AI in threat detection
2. Machine learning in anomaly detection
3. Blockchain for data integrity
4. Quantum computing and OT security
5. Case Study: AI-based ICS defense model

Training Methodology

This course employs a participatory and hands-on approach to ensure practical learning, including:

- Interactive lectures and presentations.
- Group discussions and brainstorming sessions.
- Hands-on exercises using real-world datasets.
- Role-playing and scenario-based simulations.
- Analysis of case studies to bridge theory and practice.
- Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
21 Sep 2026	02 Oct 2026	Online	$2,000
21 Sep 2026	02 Oct 2026	Physical	$3,000
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com