Security Assessment of SCADA/DCS Networks Training Course

Professional Development Training Course Outline

Category	Data Security	**Duration**	5 Days
Base Fee	$1,500 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

The operational technology (OT) landscape, driven by Industrial Control Systems (ICS), has undergone a critical transformation from isolated, proprietary networks to interconnected systems leveraging Industrial Internet of Things (IIoT) principles. This digital convergence, while optimizing efficiency and enabling remote operations, has simultaneously erased the traditional air gap, exposing vital national and industrial critical infrastructure (CI) to unprecedented cyber threats. Supervisory Control and Data Acquisition (SCADA) and Distributed Control System (DCS) environments responsible for managing everything from power grids and water treatment to manufacturing and pipelines were historically designed for reliability and uptime, not security. This presents a massive attack surface vulnerability. The need is urgent for specialized cybersecurity professionals capable of bridging the gap between traditional IT security and the unique, safety-critical requirements of OT/ICS environments. Security Assessment of SCADA/DCS Networks Training Course focuses on developing the practical skills necessary to perform comprehensive, non-disruptive, and compliance-driven security assessments and vulnerability analyses in these highly sensitive industrial networks.

A single successful attack on a SCADA/DCS network can lead to catastrophic consequences, including physical damage, environmental disaster, financial loss, and risk to human life. Modern threat actors, from state-sponsored hackers to sophisticated cybercriminal organizations, are increasingly targeting Operational Technology (OT) assets using specialized malware like EKANS and TRITON. Effective defense requires a proactive, risk-based approach that goes beyond generic IT audits. This training is specifically engineered to equip participants with deep knowledge of Industrial Protocols, OT network architecture, and the latest assessment tools and techniques. By mastering ICS Penetration Testing, Digital Forensics in a live environment, and alignment with critical frameworks like IEC 62443 and NERC CIP, graduates will be positioned as elite security practitioners ready to strengthen the resilience and cyber-physical security posture of any industrial organization, ensuring system integrity and continuous operation.

Programme Curriculum

Security Assessment of SCADA/DCS Networks Training Course

Introduction

The operational technology (OT) landscape, driven by Industrial Control Systems (ICS), has undergone a critical transformation from isolated, proprietary networks to interconnected systems leveraging Industrial Internet of Things (IIoT) principles. This digital convergence, while optimizing efficiency and enabling remote operations, has simultaneously erased the traditional air gap, exposing vital national and industrial critical infrastructure (CI) to unprecedented cyber threats. Supervisory Control and Data Acquisition (SCADA) and Distributed Control System (DCS) environments responsible for managing everything from power grids and water treatment to manufacturing and pipelines were historically designed for reliability and uptime, not security. This presents a massive attack surface vulnerability. The need is urgent for specialized cybersecurity professionals capable of bridging the gap between traditional IT security and the unique, safety-critical requirements of OT/ICS environments. Security Assessment of SCADA/DCS Networks Training Course focuses on developing the practical skills necessary to perform comprehensive, non-disruptive, and compliance-driven security assessments and vulnerability analyses in these highly sensitive industrial networks.

A single successful attack on a SCADA/DCS network can lead to catastrophic consequences, including physical damage, environmental disaster, financial loss, and risk to human life. Modern threat actors, from state-sponsored hackers to sophisticated cybercriminal organizations, are increasingly targeting Operational Technology (OT) assets using specialized malware like EKANS and TRITON. Effective defense requires a proactive, risk-based approach that goes beyond generic IT audits. This training is specifically engineered to equip participants with deep knowledge of Industrial Protocols, OT network architecture, and the latest assessment tools and techniques. By mastering ICS Penetration Testing, Digital Forensics in a live environment, and alignment with critical frameworks like IEC 62443 and NERC CIP, graduates will be positioned as elite security practitioners ready to strengthen the resilience and cyber-physical security posture of any industrial organization, ensuring system integrity and continuous operation.

Course Duration

5 days

Course Objectives

Upon completion of this course, participants will be able to:

1. Map and inventory a complete ICS/OT network architecture
2. Perform passive traffic analysis and deep-packet inspection of proprietary Industrial Protocols.
3. Identify, analyze, and prioritize SCADA vulnerabilities on HMIs, PLCs, and engineering workstations using CVSS and OT-specific risk matrices.
4. Conduct non-disruptive vulnerability scanning and ICS penetration testing within live operational environments.
5. Assess and enforce network segmentation to achieve a robust Defense-in-Depth strategy.
6. Evaluate Security Policy and Access Control implementation on critical control devices and operator consoles.
7. Analyze and apply IEC 62443 and NIST SP 800-82 standards for compliance-driven security assessments.
8. Develop a comprehensive OT asset inventory and establish a secure Configuration Management plan.
9. Implement and monitor Intrusion Detection Systems specific to industrial protocol anomalies.
10. Formulate an effective Incident Response and Forensics plan for an OT/SCADA environment.

11. Secure remote access solutions to minimize external attack vectors.
12. Design and validate Secure Communication methods, including leveraging OPC UA security features.
13. Articulate and present Cyber-Physical Risk Assessment findings to both IT and OT engineering leadership.

Target Audience

1. OT Security Engineers and Technicians
2. IT Network Engineers transitioning to OT/ICS environments
3. Security Consultants specializing in Critical Infrastructure (CI)
4. Control System and Automation Engineers
5. Risk & Compliance Managers responsible for NERC CIP or IEC 62443
6. IT/OT Managers overseeing the convergence of enterprise and control networks
7. System Integrators and Vendors implementing SCADA/DCS solutions
8. Cyber-Physical Incident Responders and Security Analysts

Course Modules with 5 Bullets & Case Studies

Module 1: Fundamentals of ICS/SCADA/DCS Architecture

- ICS Taxonomy.
- The Purdue Model.
- Industrial Protocols.
- Physical Safety and Cybersecurity.
- Legacy Systems and Patch Management.
- Case Study: Maroochy Shire Sewage Hack (2000).

Module 2: OT Network & Threat Landscape Assessment

- Attack Surface Enumeration.
- Threat Intelligence for OT
- Vulnerability Disclosure & Prioritization.
- IT/OT Convergence Risks
- Secure Remote Access.
- Case Study: Stuxnet (2010)

Module 3: ICS Penetration Testing Methodologies

- Non-Intrusive Scanning.
- Credential and Configuration Flaws.
- HMI/Engineering Workstation Assessment.
- Protocol Fuzzing and Injection.
- Network Sniffing & Deep-Packet Analysis.
- Case Study: The Oldsmar Water Treatment Plant Intrusion (2021).

Module 4: Security Control Auditing and Defense-in-Depth

- Network Segmentation Validation
- Host-Based Security for HMIs
- Access Control Models.
- Physical Security Integration.
- Data Diode and Unidirectional Gateway Assessment.

- Case Study: Colonial Pipeline Ransomware (2021).

Module 5: Compliance and Governance Frameworks

- IEC 62443 Standard.
- NERC CIP Compliance.
- NIST SP 800-82.
- Security Policy Review.
- Risk Assessment Methodology.
- Case Study: BlackEnergy (2015/2016 Ukraine Power Grid).

Module 6: Detection, Monitoring, and Threat Hunting

- Industrial IDS/IPS Solutions.
- Log and Event Management.
- Baseline and Anomaly Detection.
- Active Defense Strategies.
- Secure Network Architecture Design.
- Case Study: TRITON/TRISIS (2017).

Module 7: Digital Forensics and Incident Response in OT

- OT Incident Response Plan (IRP).
- Live Forensics on Control Systems.
- Artifact Collection.
- Chain of Custody for Evidence.
- Post-Incident Remediation.
- Case Study: NotPetya (2017) Impact on Maersk.

Module 8: Advanced SCADA Security Topics and Future Trends

- Security for IIoT Devices.
- Cloud Integration Security.
- Zero Trust Architecture (ZTA) for OT.
- Vulnerability Remediation Planning.
- The Future of OT Security.
- Case Study: WannaCry Impact.

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.
- Peer-to-peer learning and networking.
- Expert-led Q&A sessions.
- Continuous feedback and personalized guidance.

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org or call *+254769199797*

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to Fineskill Training Center account, as indicated in the invoice so as to enable us prepare better for you.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
23 Nov 2026	27 Nov 2026	Online	$1,000
23 Nov 2026	27 Nov 2026	Physical	$1,500
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$4,500
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$6,000

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

Register Online Now

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