Process Control Cybersecurity Training Course

Professional Development Training Course Outline

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

Course Introduction

In today's increasingly interconnected industrial landscape, the security of **Process Control Systems (PCS)** is paramount. These systems, which underpin critical infrastructure and manufacturing processes, are becoming prime targets for sophisticated cyberattacks. A breach in **industrial control systems (ICS)** can lead to catastrophic consequences, including production shutdowns, environmental damage, financial losses, and even safety incidents. This comprehensive training course addresses the urgent need for robust **cybersecurity in operational technology (OT)** environments. Participants will gain a deep understanding of the unique challenges and vulnerabilities associated with **industrial cybersecurity**, learn to identify potential threats, and acquire practical skills in implementing effective security measures. This course emphasizes a proactive approach to safeguarding critical assets and ensuring the resilience of **critical infrastructure cybersecurity**.

This intensive program is designed to equip professionals with the knowledge and skills necessary to navigate the complex world of **OT security**. It delves into the specific protocols, architectures, and risks associated with **supervisory control and data acquisition (SCADA)** systems, distributed control systems (DCS), and programmable logic controllers [1] (PLCs). Through a blend of theoretical learning and practical exercises, participants will master techniques for **threat detection in ICS**, **vulnerability management in OT**, and the implementation of robust **security controls for industrial networks**. By focusing on real-world scenarios and industry best practices, this course empowers individuals to become effective cybersecurity practitioners in the **industrial automation and control systems (IACS)** domain, contributing significantly to the overall **cyber resilience of industrial operations**.

Programme Curriculum

Process Control Cybersecurity Training Course

Introduction

In today's increasingly interconnected industrial landscape, the security of **Process Control Systems (PCS)** is paramount. These systems, which underpin critical infrastructure and manufacturing processes, are becoming prime targets for sophisticated cyberattacks. A breach in **industrial control systems (ICS)** can lead to catastrophic consequences, including production shutdowns, environmental damage, financial losses, and even safety incidents. This comprehensive training course addresses the urgent need for robust **cybersecurity in operational technology (OT)** environments. Participants will gain a deep understanding of the unique challenges and vulnerabilities associated with **industrial cybersecurity**, learn to identify potential threats, and acquire practical skills in implementing effective security measures. This course emphasizes a proactive approach to safeguarding critical assets and ensuring the resilience of **critical infrastructure cybersecurity**.

Process Control Cybersecurity Training Course is designed to equip professionals with the knowledge and skills necessary to navigate the complex world of **OT security**. It delves into the specific protocols, architectures, and risks associated with **supervisory control and data acquisition (SCADA)** systems, distributed control systems (DCS), and programmable logic controllers [1] (PLCs). Through a blend of theoretical learning and practical exercises, participants will master techniques for **threat detection in ICS**, **vulnerability management in OT**, and the implementation of robust **security controls for industrial networks**. By focusing on real-world scenarios and industry best practices, this course empowers individuals to become effective cybersecurity practitioners in the **industrial automation and control systems (IACS)** domain, contributing significantly to the overall **cyber resilience of industrial operations**.

Course Duration

5 days

Course Objectives

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

1. Understand the fundamental concepts of **Process Control System (PCS) cybersecurity**.
2. Identify and analyze the unique **cyber threats to industrial control systems (ICS)**.
3. Evaluate the vulnerabilities within **operational technology (OT) environments**.
4. Implement effective **security controls for industrial networks**.
5. Apply best practices for **vulnerability management in OT**.
6. Develop strategies for **threat detection in ICS**.
7. Understand the principles of **critical infrastructure cybersecurity**.
8. Implement **security hardening techniques for industrial devices**.
9. Develop and implement an **incident response plan for OT environments**.
10. Understand and apply relevant **industrial cybersecurity standards and regulations**.
11. Perform basic **security assessments of industrial control systems**.
12. Implement **network segmentation and zoning in industrial environments**.
13. Understand the importance of **human factors in OT cybersecurity**.

Organizational Benefits

- **Reduced Risk of Cyber Incidents:** Proactive measures minimize the likelihood and impact of costly cyberattacks on critical operations.
- **Improved Operational Continuity:** Enhanced security ensures the availability and reliability of essential industrial processes.

- **Compliance with Regulations:** The course helps organizations meet relevant cybersecurity standards and legal requirements.
- **Enhanced Reputation and Trust:** Demonstrating a commitment to security builds confidence among stakeholders and customers.
- **Skilled Workforce:** Equipping employees with specialized cybersecurity knowledge strengthens the organization's security posture.
- **Protection of Intellectual Property:** Safeguarding sensitive data and control system configurations.
- **Cost Savings:** Preventing cyber incidents avoids significant financial losses associated with downtime, recovery, and fines.
- **Increased Resilience:** Organizations become better equipped to withstand and recover from cyberattacks.

Target Participants

1. Control Systems Engineers
2. Automation Specialists
3. IT Security Professionals expanding into OT
4. Plant Operations Personnel
5. Risk and Compliance Managers
6. Cybersecurity Analysts focusing on industrial environments
7. Critical Infrastructure Operators
8. System Integrators working with industrial control systems

Course Outline

Module 1: Introduction to Process Control Systems and Cybersecurity

- Overview of Industrial Control Systems (ICS): SCADA, DCS, PLC
- Key differences between IT and OT environments
- The evolving landscape of cyber threats in industrial settings
- Understanding the potential impact of cyberattacks on ICS
- Introduction to relevant cybersecurity frameworks and standards for OT

Module 2: Industrial Network Architectures and Protocols

- Common industrial network topologies and architectures
- In-depth review of key OT protocols (e.g., Modbus, Profinet, DNP3)
- Security considerations for industrial communication protocols
- Network segmentation and zoning strategies in OT environments
- Wireless technologies in industrial automation and their security implications

Module 3: Threat Landscape and Vulnerabilities in ICS

- Identifying common cyber threats targeting industrial control systems
- Understanding advanced persistent threats (APTs) in the OT context
- Analyzing vulnerabilities in industrial hardware and software components
- The role of human factors in OT security breaches
- Case studies of significant cybersecurity incidents in industrial sectors

Module 4: Security Controls and Defense-in-Depth for OT

- Implementing the principle of defense-in-depth in industrial environments

- Access control and authentication mechanisms for OT systems
- Intrusion detection and prevention systems (IDPS) for industrial networks
- Endpoint security considerations for industrial devices
- Secure configuration and hardening of industrial control systems

Module 5: Vulnerability Management and Security Assessments in OT

- Establishing a robust vulnerability management program for OT assets
- Conducting risk assessments and vulnerability scans in industrial environments
- Understanding the challenges of patching and updating OT systems
- Performing security audits and penetration testing of ICS
- Compliance considerations for vulnerability management in OT

Module 6: Incident Response and Recovery for Industrial Cybersecurity

- Developing an effective incident response plan for OT environments
- Identifying and classifying security incidents in industrial control systems
- Containment, eradication, and recovery procedures for OT cyber incidents
- Forensic analysis techniques for industrial cybersecurity incidents
- Lessons learned and post-incident activities in OT cybersecurity

Module 7: Industrial Cybersecurity Standards, Regulations, and Best Practices

- Overview of key industrial cybersecurity standards (e.g., IEC 62443, NIST CSF)
- Understanding relevant regional and international regulations for OT security
- Adopting industry best practices for securing process control systems
- Developing and implementing cybersecurity policies and procedures for OT
- The importance of continuous improvement in industrial cybersecurity

Module 8: Emerging Trends and Future of OT Cybersecurity

- The impact of IoT and IIoT on industrial cybersecurity
- Cloud computing and its implications for OT security
- Artificial intelligence (AI) and machine learning for threat detection in ICS
- The role of threat intelligence in proactive OT security
- Future challenges and opportunities in the field of process control cybersecurity

Training Methodology

This training course will employ a blended learning approach, incorporating:

- Interactive lectures and presentations
- Real-world case studies and scenario analysis
- Hands-on lab exercises and simulations (where feasible and safe)
- Group discussions and knowledge sharing
- Q&A sessions and expert insights

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