Cyber-Physical Systems (CPS) Risk for Critical Infrastructure Training Course

Professional Development Training Course Outline

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

Course Introduction

The escalating convergence of Information Technology (IT) and Operational Technology (OT) has birthed Cyber-Physical Systems (CPS), which are the backbone of global Critical Infrastructure (CI), including energy, water, transportation, and manufacturing sectors. This interdependence creates an exponentially expanding attack surface, moving beyond traditional cyber threats to encompass physical damage and real-world disruption. Recent high-profile incidents underscore the urgent necessity for robust cyber-resilience and specialized expertise. Cyber-Physical Systems (CPS) Risk for Critical Infrastructure Training Course is designed to equip security professionals and engineers with the advanced knowledge required for CPS risk management in an era of sophisticated, state-sponsored, and Advanced Persistent Threats (APTs) targeting the core functions of modern society.

Effective CPS security demands a holistic approach that integrates cyber defense principles with engineering and safety-critical system design. Understanding the unique characteristics of Industrial Control Systems (ICS) and SCADA environments specifically their need for stability, availability, and non-intrusive operations is paramount. This program focuses on developing the practical skills needed to perform detailed risk assessments, implement Zero Trust architectures within OT/ICS networks, and execute effective incident response plans that account for physical consequences. By mastering threat modeling and leveraging next-generation technologies like AI-enabled defense and Cyber-Physical Threat Intelligence (CPTI), participants will learn to build and maintain an enduring security and resilience posture for vital national assets.

Programme Curriculum

Cyber-Physical Systems (CPS) Risk for Critical Infrastructure Training Course

Introduction

The escalating convergence of Information Technology (IT) and Operational Technology (OT) has birthed Cyber-Physical Systems (CPS), which are the backbone of global Critical Infrastructure (CI), including energy, water, transportation, and manufacturing sectors. This interdependence creates an exponentially expanding attack surface, moving beyond traditional cyber threats to encompass physical damage and real-world disruption. Recent high-profile incidents underscore the urgent necessity for robust cyber-resilience and specialized expertise. Cyber-Physical Systems (CPS) Risk for Critical Infrastructure Training Course is designed to equip security professionals and engineers with the advanced knowledge required for CPS risk management in an era of sophisticated, state-sponsored, and Advanced Persistent Threats (APTs) targeting the core functions of modern society.

Effective CPS security demands a holistic approach that integrates cyber defense principles with engineering and safety-critical system design. Understanding the unique characteristics of Industrial Control Systems (ICS) and SCADA environments specifically their need for stability, availability, and non-intrusive operations is paramount. This program focuses on developing the practical skills needed to perform detailed risk assessments, implement Zero Trust architectures within OT/ICS networks, and execute effective incident response plans that account for physical consequences. By mastering threat modeling and leveraging next-generation technologies like AI-enabled defense and Cyber-Physical Threat Intelligence (CPTI), participants will learn to build and maintain an enduring security and resilience posture for vital national assets.

Course Duration

5 days

Course Objectives

Upon completion, participants will be able to:

1. Analyze the convergence of IT/OT domains and its implications for Critical Infrastructure Protection (CIP).
2. Differentiate between cyber and physical threats unique to Industrial Control Systems (ICS) and SCADA environments.
3. Conduct comprehensive, system-specific Cyber-Physical Risk Assessments utilizing industry-recognized frameworks.
4. Develop robust Threat Models that account for both remote cyber exploitation and insider or physical sabotage vectors.
5. Design and implement Zero Trust Architecture (ZTA) principles within sensitive OT networks for enhanced segmentation and access control.
6. Formulate and test a sector-specific CPS Incident Response plan that integrates cyber recovery with physical safety and operational continuity.
7. Identify and remediate common Vulnerabilities in legacy and modern HMI and embedded systems.
8. Evaluate and apply AI-enabled Defense mechanisms, including machine learning for anomaly detection in sensor data and network traffic.
9. Leverage and integrate Cyber-Physical Threat Intelligence (CPTI) feeds to proactively adjust security controls and defenses.
10. Implement continuous Security Monitoring strategies optimized for real-time, low-latency control system operations.
11. Understand global Compliance and regulatory mandates, such as NIST CSF and sector-specific standards
12. Apply principles of Resilience Engineering to ensure fast recovery and minimal downtime following a major Systemic Attack.

13. Communicate and articulate complex CPS Risk to executive leadership, technical teams, and cross-functional stakeholders.

Target Audience

1. OT/ICS Security Engineers
2. Critical Infrastructure CISOs and Risk Managers
3. Control Systems Automation Engineers
4. Information Security Analysts with OT exposure
5. Compliance and Regulatory Auditors in CI sectors
6. Physical Security Professionals working with interconnected systems
7. IT/Networking Architects migrating to converged environments
8. Government Policy Makers focused on National Resilience and CIP

Course Modules

Module 1: Foundational CPS & CI Landscape

- Define and characterize Cyber-Physical Systems across sectors
- Analyze the IT/OT Convergence model and the unique security requirements of safety-critical environments.
- Distinguish between cybersecurity and Cyber-Safety objectives in control systems.
- Review international Critical Infrastructure Protection (CIP) frameworks and standards.
- Case Study: The Ukrainian Power Grid Attacks.

Module 2: OT/ICS & SCADA Security Essentials

- Deep dive into ICS, SCADA, DCS, and PLC architectures and communication protocols
- Examine the lifecycle of common SCADA Vulnerabilities and the principle of defense-in-depth for control networks.
- Explore network segregation techniques.
- Understand the challenges of securing Legacy Systems and devices with long operational lifecycles.
- Case Study: dissecting the world’s first-recognized cyber-weapon and its effect on PLCs controlling physical centrifuges.

Module 3: Advanced CPS Risk & Threat Modeling

- Methodologies for comprehensive Risk Assessment in CPS environments
- Techniques for Threat Modeling focused on the cyber-physical kill chain and attacker TTPs
- Quantifying Consequence Analysis.
- Establishing Risk Tolerance levels tailored to high-availability CI operations.
- Case Study: Colonial Pipeline Incident.

Module 4: Secure Architecture & Zero Trust in OT

- Designing Segmented Architectures using network firewalls, unidirectional gateways, and VLANS.
- Implementing Zero Trust principles for identity, access, and micro-segmentation in OT.
- Strategies for securing Remote Access to control systems
- Hardening the HMI and engineering workstations against endpoint compromise.
- Case Study: Implementing a ZTA pilot in a water treatment plant to secure contractor remote maintenance access and prevent lateral movement.

Module 5: Threat Detection and Real-Time Monitoring

- Deploying Passive Monitoring and specialized Intrusion Detection Systems non-intrusive to control systems.
- Utilizing Machine Learning and Anomaly Detection for behavioral baselining of process control variables.
- Developing Cyber-Physical Threat Intelligence feeds for proactive defense posture adjustment.
- Techniques for centralized Security Information and Event Management and log aggregation from diverse OT/ICS assets.
- Case Study: Analyzing a simulated man-in-the-middle attack on a wind farm SCADA network and using passive monitoring data for detection.

Module 6: Vulnerability Management & Patching in OT

- The unique challenges of Vulnerability Management in 24/7, high-availability OT environments
- Implementing compensating controls and Virtual Patching to mitigate known flaws without system reboot.
- Strategies for securing Industrial IoT devices and sensors connecting to the control network.
- Performing Non-Intrusive Network Audits and configuration baselining for security drift.
- Case Study: The exploitation of known vulnerabilities in an outdated, internet-exposed PLC platform and the mitigation strategy using network controls.

Module 7: Incident Response & Disaster Recovery

- Developing and testing a structured CPS Incident Response Plan that prioritizes safety and physical consequence mitigation.
- Defining and executing Playbooks for common ICS scenarios
- Techniques for Forensics and Root Cause Analysis within proprietary and volatile OT systems.
- Integrating Disaster Recovery (DR) and Business Continuity (BC) planning with cyber IR efforts.
- Case Study: Practicing a table-top exercise for a gas pipeline system facing a simultaneous cyber-attack and physical sabotage attempt.

Module 8: Emerging Threats & Future Resilience

- The risk of Quantum-Era Security threats and the need for Quantum-Ready cryptography in long-life systems.
- Securing modern concepts.
- The role of Blockchain and Distributed Ledger Technology (DLT) in enhancing CPS data integrity and supply chain security.
- Building a culture of cross-sector Information Sharing for collective Cyber-Resilience.
- Case Study: Exploring the hypothetical defense strategies against a future attack leveraging advanced Generative AI for zero-day exploitation against a smart factory.

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
21 Sep 2026	25 Sep 2026	Online	$1,000
21 Sep 2026	25 Sep 2026	Physical	$1,500
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0

Start Date	End Date	Location	Price
21 Sep 2026	25 Sep 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