Cyber-Physical Systems (CPS) Security Training Course

Professional Development Training Course Outline

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

Course Introduction

Cyber-Physical Systems (CPS) sit at the core of modern industrial automation, smart infrastructure, intelligent transportation, precision manufacturing, and critical national services. As digital controls, embedded sensors, IoT devices, and real-time communication networks converge, the security of CPS becomes an essential requirement for operational resilience, system integrity, and protection against advanced cyber threats. Cyber-Physical Systems (CPS) Security Training Course provides comprehensive knowledge on secure CPS architectures, vulnerability detection, threat modeling, safety–security integration, and defense strategies for interconnected environments. The course is designed to strengthen technical, operational, and governance capabilities required to safeguard systems that blend the digital and physical worlds.

Participants will explore emerging risks associated with industrial cyber-attacks, insecure IoT integration, autonomous systems vulnerabilities, and cross-domain exploitation. Through practical exercises and case-based learning, the course equips professionals with the competence to analyze system dependencies, implement layered defenses, design secure communication protocols, and prepare incident response strategies tailored for CPS environments. By the end of the program, learners gain a deep understanding of how to build, protect, and sustain secure cyber-physical infrastructures in rapidly evolving threat landscapes.

Programme Curriculum

Cyber-Physical Systems (CPS) Security Training Course

Introduction

Cyber-Physical Systems (CPS) sit at the core of modern industrial automation, smart infrastructure, intelligent transportation, precision manufacturing, and critical national services. As digital controls, embedded sensors,

IoT devices, and real-time communication networks converge, the security of CPS becomes an essential requirement for operational resilience, system integrity, and protection against advanced cyber threats. Cyber-Physical Systems (CPS) Security Training Course provides comprehensive knowledge on secure CPS architectures, vulnerability detection, threat modeling, safety–security integration, and defense strategies for interconnected environments. The course is designed to strengthen technical, operational, and governance capabilities required to safeguard systems that blend the digital and physical worlds.

Participants will explore emerging risks associated with industrial cyber-attacks, insecure IoT integration, autonomous systems vulnerabilities, and cross-domain exploitation. Through practical exercises and case-based learning, the course equips professionals with the competence to analyze system dependencies, implement layered defenses, design secure communication protocols, and prepare incident response strategies tailored for CPS environments. By the end of the program, learners gain a deep understanding of how to build, protect, and sustain secure cyber-physical infrastructures in rapidly evolving threat landscapes.

Course Objectives

1. Understand foundational concepts and architectures of cyber-physical systems.
2. Identify trending threat vectors targeting CPS environments.
3. Apply advanced vulnerability assessment methods for CPS components.
4. Integrate cybersecurity frameworks into physical systems operations.
5. Analyze system interdependencies and failure propagation risks.
6. Implement secure communication protocols for sensors, networks, and controllers.
7. Strengthen defense strategies against IoT-based and industrial cyber threats.
8. Conduct CPS threat modeling using modern analytical techniques.
9. Apply real-time monitoring solutions for anomaly and intrusion detection.
10. Develop incident response and recovery plans aligned with CPS requirements.
11. Implement risk management strategies for mission-critical CPS infrastructures.
12. Strengthen governance mechanisms and compliance structures for CPS security.
13. Build long-term resilience through continuous testing, audit, and optimization.

Organizational Benefits

- Enhanced protection of mission-critical infrastructure
- Reduced operational disruption through proactive CPS risk mitigation
- Improved resilience against advanced industrial cyber-attacks
- Increased system reliability, safety, and uptime
- Stronger compliance with cybersecurity regulatory standards
- Optimized security investments through structured CPS governance
- Improved integration of IT, OT, and physical security functions
- Strengthened organizational response to real-time threats
- Increased visibility of CPS vulnerabilities and system anomalies
- Enhanced reputation for innovation, safety, and data stewardship

Target Audiences

- Cybersecurity professionals and CPS security engineers
- Industrial control system operators and OT specialists
- ICT managers working with automation and smart infrastructure
- IoT and embedded systems developers
- Critical infrastructure security teams

- Risk management and compliance officers
- Systems integrators and engineering consultants
- Policy advisors and regulatory oversight bodies

Course Duration: 10 days

Course Modules

Module 1: Foundations of Cyber-Physical Systems

- Define CPS components, architectures, and integrations
- Assess digital-physical convergence and operational impact
- Identify typical CPS deployment environments
- Understand system control loops and real-time operations
- Analyze CPS system reliability and safety constraints
- Case Study: Failure analysis in a smart grid CPS

Module 2: CPS Threat Landscape and Emerging Risks

- Review industrial and IoT-based cyber threats
- Understand adversarial tactics against integrated systems
- Analyze vulnerabilities in sensors and control components
- Examine cross-domain exploitation patterns
- Assess nation-state and advanced persistent threats
- Case Study: Cyber attack on a smart manufacturing plant

Module 3: CPS Security Architecture and Design

- Integrate layered security approaches
- Implement segmentation between IT, OT, and IoT networks
- Apply secure hardware and embedded system practices
- Strengthen authentication and authorization methods
- Implement secure-by-design engineering principles
- Case Study: Redesigning CPS architecture for an industrial site

Module 4: IoT and Embedded Device Security

- Identify risks in low-power embedded devices
- Apply secure firmware and update mechanisms
- Implement device identity management
- Analyze IoT communication vulnerabilities
- Strengthen perimeter and device-level protections
- Case Study: IoT device compromise affecting CPS stability

Module 5: Network Security for CPS

- Secure industrial communication protocols
- Manage segmentation across heterogeneous networks
- Implement intrusion detection for CPS traffic
- Monitor network anomalies and sensor activity
- Apply encryption and secure routing strategies
- Case Study: Protocol-level attack on industrial control networks

Module 6: Sensor and Actuator Security

- Identify vulnerabilities in sensor data pipelines
- Strengthen signal authentication mechanisms
- Mitigate physical tampering and spoofing
- Manage sensor-to-controller communication security
- Apply redundancy and validation techniques
- Case Study: Sensor manipulation affecting industrial output

Module 7: Industrial Control Systems (ICS) Security

- Review PLC, SCADA, DCS security principles
- Protect control logic and firmware
- Apply segmentation and access controls
- Integrate secure system configuration practices
- Monitor control system anomalies
- Case Study: Compromise of PLC logic in a power plant

Module 8: CPS Risk Management and Assessment

- Apply CPS-specific risk frameworks
- Conduct high-impact system risk evaluations
- Map operational dependencies and vulnerabilities
- Prioritize risks using structured methodologies
- Integrate risk findings into strategic decision-making
- Case Study: Risk assessment of an automated logistics system

Module 9: Real-Time Monitoring and Anomaly Detection

- Implement real-time CPS monitoring tools
- Identify abnormal patterns in CPS operations
- Apply intrusion detection targeting OT networks
- Correlate sensor, network, and control anomalies
- Strengthen automated alerting mechanisms
- Case Study: Real-time detection of a coordinated CPS breach

Module 10: CPS Vulnerability Assessment Techniques

- Conduct testing across hardware, software, and network layers
- Use specialized OT and ICS assessment tools
- Apply penetration testing adapted to physical systems
- Evaluate system resilience under simulated attack
- Document findings and mitigation recommendations
- Case Study: Vulnerability assessment of smart water infrastructure

Module 11: Incident Response for CPS

- Activate incident response tailored to CPS operations
- Coordinate remediation across IT and OT teams
- Preserve physical and digital evidence securely
- Restore systems with minimal operational disruption
- Review and update response procedures

- Case Study: Incident response during industrial cyber intrusion

Module 12: CPS Governance and Compliance

- Implement policies for cybersecurity and physical safety
- Align CPS operations with regulatory requirements
- Develop governance structures for integrated environments
- Monitor compliance through internal audit mechanisms
- Strengthen documentation and reporting procedures
- Case Study: Governance gaps identified in a CPS audit

Module 13: Safety and Security Integration

- Align safety engineering with cybersecurity practices
- Manage cascading effects across systems
- Apply holistic risk mitigation strategies
- Develop secure safety control mechanisms
- Implement cross-functional collaboration processes
- Case Study: Safety-security conflict in automated operations

Module 14: CPS Resilience and Recovery Planning

- Develop resilience strategies for integrated systems
- Create redundancy plans for mission-critical operations
- Strengthen system recovery capabilities
- Test continuity plans in CPS environments
- Integrate recovery lessons into long-term strategy
- Case Study: Recovery planning for autonomous transportation CPS

Module 15: Building Future-Ready CPS Security Programs

- Integrate innovation and scaling strategies
- Identify long-term CPS security investment priorities
- Adopt next-generation technologies for system protection
- Implement continuous improvement mechanisms
- Strengthen workforce capacity and institutional readiness
- Case Study: Implementation of enterprise-wide CPS security upgrade

Training Methodology

- Instructor-led presentations and demonstrations
- Practical CPS security simulations and hands-on exercises
- Group-based threat modeling and system analysis activities
- Review of real-world attacks and CPS case studies
- Guided development of CPS security action plans
- Interactive discussions and feedback sessions

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	04 Dec 2026	Online	$2,000
23 Nov 2026	04 Dec 2026	Physical	$3,000
23 Nov 2026	04 Dec 2026	Physical	$6,000
23 Nov 2026	04 Dec 2026	Physical	$6,000
23 Nov 2026	04 Dec 2026	Physical	$12,000
23 Nov 2026	04 Dec 2026	Physical	$9,000
23 Nov 2026	04 Dec 2026	Physical	$12,000
23 Nov 2026	04 Dec 2026	Physical	$12,000

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

Register Online Now