Renewable Energy Cyber-Physical Systems Training Course

Professional Development Training Course Outline

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

Course Introduction

Renewable Energy Cyber-Physical Systems (CPS) Training Course equips professionals with practical knowledge to secure the increasingly connected infrastructure behind solar PV, wind power, battery energy storage systems (BESS), microgrids, smart inverters, distributed energy resources (DERs), IoT devices, industrial control systems (ICS), SCADA, and smart grids. Renewable-energy environments combine physical equipment, software, communications, sensors, automation, and data-driven control, making cybersecurity, resilience, safety, reliability, interoperability, and real-time situational awareness essential design priorities. NIST describes cyber-physical systems as interacting computational and physical components and emphasizes cybersecurity, privacy, timing, dependability, and data interoperability as important CPS considerations. The course therefore connects OT cybersecurity with renewable-energy engineering, helping participants understand how cyber events can affect physical operations, grid stability, energy availability, and business continuity.

The program is aligned conceptually with established smart-grid cybersecurity, DER security, risk-management, and cybersecurity-framework practices. NIST guidance highlights the need to protect communications and data integrity across DER environments and identifies capabilities such as network monitoring, malware detection, authentication, access control, cloud analytics, and trusted data flows. Recent NIST guidance also addresses cybersecurity considerations for smart inverters, including vulnerabilities and security capabilities for residential and light-commercial solar systems. Through interactive lectures, scenario-based learning, architecture exercises, tabletop simulations, threat modeling, incident-response exercises, and real-world case studies, participants develop a holistic understanding of how to design, assess, monitor, and improve secure renewable-energy CPS environments.

Programme Curriculum

Renewable Energy Cyber-Physical Systems Training Course

Introduction

Renewable Energy Cyber-Physical Systems (CPS) Training Course equips professionals with practical knowledge to secure the increasingly connected infrastructure behind solar PV, wind power, battery energy storage systems (BESS), microgrids, smart inverters, distributed energy resources (DERs), IoT devices, industrial control systems (ICS), SCADA, and smart grids. Renewable-energy environments combine physical equipment, software, communications, sensors, automation, and data-driven control, making cybersecurity, resilience, safety, reliability, interoperability, and real-time situational awareness essential design priorities. NIST describes cyber-physical systems as interacting computational and physical components and emphasizes cybersecurity, privacy, timing, dependability, and data interoperability as important CPS considerations. The course therefore connects OT cybersecurity with renewable-energy engineering, helping participants understand how cyber events can affect physical operations, grid stability, energy availability, and business continuity.

The program is aligned conceptually with established smart-grid cybersecurity, DER security, risk-management, and cybersecurity-framework practices. NIST guidance highlights the need to protect communications and data integrity across DER environments and identifies capabilities such as network monitoring, malware detection, authentication, access control, cloud analytics, and trusted data flows. Recent NIST guidance also addresses cybersecurity considerations for smart inverters, including vulnerabilities and security capabilities for residential and light-commercial solar systems. Through interactive lectures, scenario-based learning, architecture exercises, tabletop simulations, threat modeling, incident-response exercises, and real-world case studies, participants develop a holistic understanding of how to design, assess, monitor, and improve secure renewable-energy CPS environments.

Course Duration

5 days

Course Objectives

By the end of the course, participants will be able to:

1. Understand Renewable Energy Cyber-Physical Systems (RE-CPS) architecture, components, dependencies, and operational workflows.
2. Identify OT/IT convergence risks across renewable-energy facilities and smart-grid environments.
3. Analyze cyber-physical attack surfaces involving SCADA, PLCs, RTUs, HMIs, sensors, gateways, and controllers.
4. Apply risk assessment and threat modeling techniques to renewable-energy infrastructure.
5. Develop zero-trust security concepts for connected energy assets and remote-access environments.
6. Strengthen smart-inverter, DER, BESS, and microgrid cybersecurity awareness.
7. Apply network segmentation, secure communications, identity management, and access control principles.
8. Improve security monitoring, anomaly detection, threat intelligence, and situational awareness capabilities.
9. Understand incident response, containment, recovery, and cyber-resilience for energy-sector CPS.
10. Evaluate IoT/IIoT, cloud, edge-computing, and digitalization risks in renewable-energy systems.
11. Integrate security-by-design and secure-by-default principles into renewable-energy projects.
12. Develop practical cybersecurity governance, compliance, risk, and resilience strategies.
13. Build an actionable renewable-energy CPS cybersecurity improvement roadmap for an organization.

Target Audience

1. Renewable Energy Engineers and electrical engineers
2. OT/ICS Cybersecurity Professionals
3. SCADA, PLC, and Control-System Engineers
4. Smart Grid and DER Specialists
5. Solar PV, Wind, BESS, and Microgrid Professionals
6. IT Security, SOC, and Network Security Teams
7. Energy Managers, Risk Managers, and Compliance Professionals
8. Utility Executives, Project Managers, Regulators, and Policy Professionals

Course Modules

Module 1: Renewable Energy Cyber-Physical Systems Fundamentals

- CPS architecture
- Renewable-energy ecosystem
- IT/OT convergence
- CPS security principles.
- **Case Study:** Mapping the cyber-physical architecture of a **utility-scale solar farm** and identifying critical digital-to-physical dependencies.

Module 2: Renewable Energy Threat Landscape & Risk Assessment

- Threat modeling
- Attack surfaces
- Cyber-physical risk assessment
- Critical-asset identification
- **Case Study:** Risk assessment for a **distributed solar portfolio** containing thousands of remotely managed DER devices.

Module 3: SCADA, ICS, IoT & IIoT Security

- SCADA security
- IIoT cybersecurity
- Network segmentation
- Identity and access management
- **Case Study:** Securing a **wind-farm SCADA environment** against unauthorized remote access and anomalous network activity.

Module 4: Smart Inverters, DERs, BESS & Microgrid Cybersecurity

- Smart-inverter cybersecurity
- DER security
- BESS cybersecurity
- Microgrid resilience
- **Case Study:** Assessing the cybersecurity posture of a **solar-plus-storage microgrid** with remote operational control.

Module 5: Zero Trust, Network Security & Secure Communications

- Zero Trust for OT
- Network architecture
- Secure communications

- Remote operations
- **Case Study:** Designing a **secure remote-access architecture** for geographically distributed renewable-energy assets.

Module 6: Monitoring, Detection & Cyber Threat Intelligence

- Security monitoring
- Anomaly detection
- SOC/OT-SOC integration
- Threat intelligence
- **Case Study:** Building a **renewable-energy security monitoring scenario** to detect abnormal communications between DER devices and grid-control infrastructure.

Module 7: Incident Response, Resilience & Recovery

- OT incident response
- Cyber-resilience.
- Business continuity
- Recovery planning
- **Case Study:** Tabletop exercise involving a **hypothetical compromise of renewable-energy control communications**, requiring coordinated technical and operational response.

Module 8: Governance, Compliance & Secure Renewable-Energy Design

- Cybersecurity governance
- Security-by-design
- Framework alignment
- Third-party and supply-chain security
- **Case Study:** Developing a **cybersecurity roadmap for a renewable-energy operator** expanding its solar, wind, and BESS portfolio.

Training Methodology

- 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
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