Airport Operational Technology (OT) Security Training Course

Professional Development Training Course Outline

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

Course Introduction

Airport Operational Technology (OT) Security has become a strategic priority as airports accelerate digital transformation, smart airport initiatives, Industrial Internet of Things (IIoT), automation, and integrated cyber-physical systems. Critical airport infrastructure including baggage handling systems, airfield lighting, access control, SCADA, Building Management Systems (BMS), fuel distribution, surveillance systems, and communication networks require advanced cybersecurity frameworks to ensure operational continuity, resilience, safety, and regulatory compliance. Airport Operational Technology (OT) Security Training Course equips professionals with practical knowledge to identify vulnerabilities, mitigate cyber threats, and strengthen airport OT environments using globally recognized security standards and best practices.

The training explores OT governance, cyber risk management, industrial control system protection, network segmentation, threat intelligence, incident response, vulnerability assessment, Zero Trust Architecture, NIST Cybersecurity Framework, IEC 62443 standards, ransomware defense, digital resilience, and emerging technologies. Participants will gain practical skills to secure mission-critical airport infrastructure, enhance business continuity, improve operational resilience, and protect aviation assets against evolving cyber threats while supporting sustainable and secure airport operations.

Programme Curriculum

Airport Operational Technology (OT) Security Training Course

Introduction

Airport Operational Technology (OT) Security has become a strategic priority as airports accelerate digital transformation, smart airport initiatives, Industrial Internet of Things (IIoT), automation, and integrated cyber-physical systems. Critical airport infrastructure including baggage handling systems, airfield lighting, access

control, SCADA, Building Management Systems (BMS), fuel distribution, surveillance systems, and communication networks require advanced cybersecurity frameworks to ensure operational continuity, resilience, safety, and regulatory compliance. Airport Operational Technology (OT) Security Training Course equips professionals with practical knowledge to identify vulnerabilities, mitigate cyber threats, and strengthen airport OT environments using globally recognized security standards and best practices.

The training explores OT governance, cyber risk management, industrial control system protection, network segmentation, threat intelligence, incident response, vulnerability assessment, Zero Trust Architecture, NIST Cybersecurity Framework, IEC 62443 standards, ransomware defense, digital resilience, and emerging technologies. Participants will gain practical skills to secure mission-critical airport infrastructure, enhance business continuity, improve operational resilience, and protect aviation assets against evolving cyber threats while supporting sustainable and secure airport operations.

Course Objectives

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

1. Understand airport OT security architecture and ecosystem.
2. Identify emerging cyber threats affecting airport infrastructure.
3. Apply NIST Cybersecurity Framework within airport OT environments.
4. Implement IEC 62443 industrial cybersecurity controls.
5. Strengthen SCADA and Industrial Control System security.
6. Perform OT cyber risk assessments and mitigation planning.
7. Secure Industrial Internet of Things (IIoT) devices.
8. Design resilient network segmentation strategies.
9. Develop effective airport OT incident response plans.
10. Conduct vulnerability assessments and penetration readiness.
11. Enhance cyber resilience through Zero Trust principles.
12. Integrate business continuity with operational resilience.
13. Improve regulatory compliance and cybersecurity governance.

Organizational Benefits

- Strengthened airport cybersecurity posture.
- Reduced operational disruption risks.
- Enhanced resilience against ransomware attacks.
- Improved regulatory compliance.
- Better protection of critical infrastructure.
- Faster cyber incident detection and recovery.
- Increased operational continuity.
- Improved stakeholder confidence.
- Enhanced risk management capabilities.
- Greater organizational cyber maturity.

Target Audiences

- Airport Operations Managers

- Airport IT and OT Engineers
- Cybersecurity Professionals
- Air Navigation Service Personnel
- Infrastructure Maintenance Engineers
- Airport Safety and Security Officers
- Aviation Regulatory Authorities
- Airport Technology Consultants

Course Duration: 5 days

Course Modules

Module 1: Airport OT Security Fundamentals

- Understanding Operational Technology environments.
- Airport critical infrastructure overview.
- OT versus traditional IT security.
- Airport cyber threat landscape.
- Cybersecurity governance principles.
- Global Case Study: Cybersecurity transformation at Singapore Changi Airport.

Module 2: Airport OT Architecture and Risk Management

- Airport network architecture.
- Asset identification and classification.
- Cyber risk assessment methodologies.
- Threat modeling techniques.
- Risk mitigation planning.
- Global Case Study: Heathrow Airport cyber resilience initiatives.

Module 3: Industrial Control Systems and SCADA Security

- SCADA system fundamentals.
- Industrial Control System vulnerabilities.
- Secure communication protocols.
- Access control management.
- Industrial device hardening.
- Global Case Study: Industrial cybersecurity improvements at Schiphol Airport.

Module 4: OT Network Protection and Zero Trust

- Network segmentation strategies.
- Zero Trust implementation.

- Identity and access management.
- Secure remote connectivity.
- Continuous monitoring techniques.
- Global Case Study: Zero Trust deployment in Dubai International Airport.

Module 5: Threat Detection and Incident Response

- Cyber threat intelligence.
- Security monitoring tools.
- Incident response planning.
- Digital forensics basics.
- Business continuity integration.
- Global Case Study: Ransomware preparedness in major North American airports.

Module 6: Compliance, Standards and Governance

- NIST Cybersecurity Framework.
- IEC 62443 implementation.
- ISO 27001 integration.
- Aviation regulatory compliance.
- Security policy development.
- Global Case Study: European airport regulatory compliance program.

Module 7: Emerging Technologies and OT Security

- IIoT security controls.
- Artificial Intelligence in cybersecurity.
- Cloud-connected OT protection.
- Digital twin security.
- Predictive threat analytics.
- Global Case Study: Smart airport cybersecurity initiatives in Incheon International Airport.

Module 8: Building a Resilient Airport OT Security Program

- Cybersecurity maturity assessment.
- Security awareness programs.
- Vendor risk management.
- Operational resilience planning.
- Continuous improvement strategies.
- Global Case Study: Integrated OT security program at Hamad International Airport.

Training Methodology

- Interactive expert-led presentations.
- Practical airport OT security workshops.
- Real-world aviation cyber case studies.
- Group discussions and collaborative learning.
- Hands-on cyber risk assessment exercises.
- Incident response simulations.
- OT security framework implementation activities.
- Scenario-based problem-solving sessions.
- Knowledge assessments and feedback.
- Action planning for workplace implementation.

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

Start Date	End Date	Location	Price
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