INDEX



CERTIFIED ISA/IEC 62443 LEAD IMPLEMENTER TRAINING COURSE

Table of contents

I. Detailed agenda of the training course 3
Day 1 3
Day 2 4
Day 3 5
Day 4 6
Day 5 7
II. Standards cited in this training course 8
III. Bibliography 10
IV. List of acronyms 11

I. Detailed agenda of the training course

Day 1 Foundations of ISA/IEC 62443 and IACS security

Section 1: Training course objectives and structure 4
- General information
- Educational approach
- Agenda of the training course
- Learning objectives
- Examination and certification
- About PECB

Section 2: Terms, definitions, and key technologies 17
- Key definitions
- Key attributes of information technology (IT) systems
- Key attributes of operational technology (OT) systems

Section 3: Purpose and scope 29
- The ISA/IEC 62443 family of standards
- What is in the standards?
- ISA/IEC 62443 family of standards and technical reports
- Purpose of the standards in the ISA/IEC 62443 series
- Scope of the standards
- Key drivers for ISA/IEC 62443
- History of ISA/IEC 62443
- Main differences between the old and new ISA/IEC 62443

Section 4: Key concepts 43
- Key aspects of IACS security
- IACS technology levels
- Basic operations of a typical OT system
- Components of IACS

Section 5: IACS networks 57
- Protocols and their importance for security
- Some basic networking concepts
- IACS network overview
- IACS networking technologies

Day 2 Security requirements, maturity models, and threat landscape

Section 6: System security requirements 3
- Key concepts in ISA/IEC 62443-3-3
- The risk management process of ISA/IEC 62443-3-3 and ISA/IEC 62443-1-1
- Security levels and zones
- Security functions
- Foundational requirements of ISA/IEC 62443

Section 7: Maturity models 15
- CMMI maturity levels
- ISA/IEC 62443 maturity levels
- ISO 9001 and ISA/IEC 62443
- Comparing CMMI and ISA/IEC 62443
- CMMI Levels 1 to 5
- The significance of the maturity levels

Section 8: Security levels and principles as defined in ISA/IEC 62443 30
- Security levels as defined by ISA/IEC 62443
- Purdue Enterprise Reference Architecture (PERA)
- The importance of security and maturity levels
- Key security principles in ISA/IEC 62443
- Zones and conduits

Section 9: Threat landscape and actors 42
- Threat agent and threat sources
- Threat landscape
- Threat actors
- Attack techniques
- Threat actors and examples

Section 10: Physical security 51
- Physical security in IACS
- Site planning, buildings, egress routes, health, and safety
- Points for consideration regarding physical security

Section 11: Access control 57
- Access control in IACS
- Recommended mechanisms for access control

Section 12: Supply chain management 62
- Supply chain management in IACS
- Points of consideration for supply chain management

Section 13: Audit and certifications 67
- Audit and certifications in IACS
- Possible audit actions

Section 14: Patching 72
- Patching in IACS
- Issues with patching in IACS
- Key issues for consideration regarding patching

Day 3 Establishing and managing an IACS security program

Section 15: Introduction to the IACS security program 3
- Specification of the requirements of ISA/IEC 62443
- Reasons for the IACS security program
- The stages in the IACS security program (ISA/IEC 62443-2-1)
- Activities of the ISA/IEC 62443 security program

Section 16: IACS security program establishment 11
- Scope of the implementation
- Systems in scope
- Key personnel
- Deliverables
- Project approval

Section 17: Risk assessment 32
- Two stages of ISA/IEC 62443 risk assessment
- The risk assessment method
- Perform the risk assessment
- Gap analysis
- Risk treatment project plan

Section 18: Policy development 55
- Identification of current policies
- Identification and development of missing policies
- Presenting to management
- Obtaining implementation approval

Section 19: IACS organization 82
- Areas of responsibility
- Risk assessment adjustment
- Reporting paths and contents

Day 4 Training, incident response, and sector-specific standards

Section 20: Training 3
- The importance of training
- Target groups
- Awareness training
- Topic specific training
- Training outcomes

Section 21: Incident response 27
- Response capabilities
- Desired response level
- Response plan definition, development, and testing

Section 22: Testing IACS security 46
- IACS security
- Status of tests and readiness
- Feedback to risk assessment

Section 23: Monitoring 64
- Principles of monitoring under ISA/IEC 62443
- Periodic follow-ups
- Re-evaluation criteria

Section 24: Other relevant standards 76
- Maritime standards
- Medical sector
- Nuclear sector
- Energy and power; oil and gas
- Aerospace, defense, and automotive industry
- Chemical and process industry; water treatment
- Healthcare and railway

Section 25: Closing of the training course 95
- PECB certification scheme
- Attestation of course completion
- PECB certification process
- Other PECB services
- Other PECB training courses and certifications

Day 5 Certification exam

II. Standards cited in this training course

- IEC/TS 62443-1-1:2009, Terminology, concepts, and models
- IEC 62443-3-3:2013, System security requirements and security levels
- IEC TR 62443-2-3: 2015 (Ed. 1.0), Patch management in the IACS environment
- IEC 62443-4-1:2018, Secure product development lifecycle requirements
- IEC 62443-4-2:2019, Technical security requirements for IACS components
- IEC 62443-3-2:2020, Security risk assessment and system design
- IEC 62443-2-4:2023, Security program requirements for IACS service providers
- IEC 62443-2-1:2024, Security program requirements for IACS asset owners
- IEC 61162-460:2024, Digital interfaces — Ethernet interconnection — Safety and security
- Guidelines on Cyber Security Onboard Ships: 2024, Industry guidance by BIMCO/ICS/OCIMF
- IMO MSC-FAL.1/Circ.3/Rev.3:2025, Guidelines on Maritime Cyber Risk Management
- IACS UR E26/UR E27:2023, Cyber resilience requirements
- UK DfT/IET Cyber Security Code of Practice: 2023, Ship Security
- DNV Class Rules: 2025, “Cyber secure” rules / class notations
- AAMI TIR97:2019/(R)2023, Principles for medical device security — Postmarket risk management for device manufacturers
- ISO 14971:2019, Medical devices — Application of risk management to medical devices (+ Amd 1:2022)
- IEC 80001-1:2021, Application of risk management for IT-networks incorporating medical devices
- IEC 62304:2006, Medical device software — Software life-cycle processes
- NRC RG 5.71:2023 (Rev.1), Cyber Security Programs for Nuclear Power Reactors
- IAEA NSS No. 17-T (Rev.1):2021, Computer Security Techniques for Nuclear Facilities
- IEEE 1300:2011, Guide for Cable Connections for Gas-Insulated Substations
- IEC 61850:2025, Communication networks and systems for power utility automation
- API Std 1164:2021 (3rd Ed.), Pipeline Control Systems Cybersecurity
- API RP 754:2021 (3rd Ed.), Process Safety Performance Indicators for the Refining and Petrochemical Industries
- IEC 61508:2010 (Ed. 2), Functional safety of electrical/electronic/programmable electronic safety-related systems (+ TS 61508-3-2:2024 supplement)
- IEC 61511:2016 (Ed. 2 + Amd 1:2017), Functional safety — Process industry safety instrumented systems (61511:2025 SER for series packaging)
- AWWA G430:2024, Security Practices for Operation and Management
- NIST SP 800-82r3:2023, Guide to Operational Technology (OT) Security

- IEC 62279:2015 (Ed. 2.0), Software for railway control and protection systems
- CENELEC/CLC TS 50701:2023, Railway applications — Cybersecurity
- ISO/SAE 21434:2021, Road-vehicle cybersecurity engineering
- RTCA DO-326A/EUROCAE ED-202A: current, Airworthiness Security Process Specification
- RTCA DO-356A/EUROCAE ED-203A: current, Airworthiness Security Methods and Considerations
- ISO/IEC 27000:2018, Information technology — Security techniques — Information security management systems — Overview and vocabulary
- ISO 22301:2019, Security and resilience — Business continuity management systems — Requirements (+ Amd 1:2024)

III. Bibliography

Section 2: Terms, definitions, and key technologies

[1] Cisco. "How Do OT and IT Differ? OT vs. IT." *Cisco*. Accessed September 17, 2025. https://www.cisco.com/site/us/en/learn/topics/industrial-iot/what-is-ot-vs-it.html

Section 9: Threat landscape and actors

[1] Encyclopedia by Kaspersky. "Threat Landscape." Accessed March 13, 2023. https://encyclopedia.kaspersky.com/glossary/threat-landscape/#

[2] ENISA. "Hackers-for-Hire Drive the Evolution of the New ENISA Threat Landscape." Accessed June 15, 2023. https://www.enisa.europa.eu/news/enisa-news/hackers-for-hire-drive-the-evolution-of-the-new-enisa-threat-landscape

IV. List of acronyms

AC: Alternating current
AMF: Annual Maintenance Fee
AMQP: Advanced message queuing protocol
API: American Petroleum Institute
APT: Advanced persistent threat attacks
BCMS: Business continuity management system
BCP: Business continuity plans
BES: Bulk electric system
BIA: Business impact analysis
BLE: Bluetooth low energy
CA: Collision avoidance
CAN: Controller area network
CDMA: Collision detection multiple access
CIP: Critical Infrastructure Protection
CMMI: Capability Maturity Model Integration
CMU: Carnegie Mellon University
CoAP: Constrained application protocol
COAX: Coaxial cable
CPD: Continuing Professional Development
CUI: Controlled unclassified information
DC: Direct current
DCS: Distributed control system
DDS: Data distribution service
DIB: Defense Industrial Base
DMZ: Demilitarized zone
DRA: Detailed risk assessment
ECU: Electronic control units
GDPR: General Data Protection Regulation
GPS: Global Positioning System
GSM: Global System for Mobile Communications
HMI: Human-Machine Interface
HTTP/HTTPS: Hypertext transfer protocol / Hypertext transfer protocol secure
HVAC: Heating, Ventilation, and Air Conditioning
IACS: Industrial automation and control systems
IAEA: International Atomic Energy Agency
ICS: Industrial control system
ICS Attack: Attacks on industrial control systems
IDPS: Intrusion detection and prevention system
IDS: Intrusion detection system
IMO: International Maritime Organization
IoT: Internet of Things

IP: Internet Protocol
IRA: Initial risk assessment
ISDS: Integrated software dependent systems
ISMS: Information security management system
IT: Information technology
LA: Lead Auditor
LI: Lead Implementer
LoRaWAN: Long range wide area network
MMF: Multi-mode fiber
MQTT: Message queuing telemetry transport
MS/TP: Master-Slave/Token-Passing
NERC: North American Electric Reliability Corporation
NFC: Near Field Communication
NIST: National Institute of Standards and Technology
ODVA: Open DeviceNet Vendor Association
OT: Operational technology
PA: Process Automation
PDCA: Plan-do-check-act
PECB: Professional Evaluation and Certification Board
PERA: Purdue Enterprise Reference Architecture
PI: Profinet International
PLC: Programmable logic controller
QoS: Quality of Service
RAT: Remote Access Trojan
RBAC: Role-based access control
RG: Regulatory guide
RPO: Recovery point objectives
RTO: Recovery time objectives
RTU: Remote Terminal Unit
SCADA: Supervisory control and data acquisition
SEM: Security event management
SIM: Security information management
SIEM: Security information and event management
SL-A: Achieved Security Level
SL-C: Component Security Level
SL-T: Target Security Level
SMF: Single mode fiber
SOC: Service Organization Control
SP: Standard part
SPDL: Secure product development life cycle
SRs: System requirements
STP: Shielded twisted pair
TCP: Transmission Control Protocol
TIR: Technical information report

UDP: User datagram protocol
UR: Unified Requirements
USB: Universal Serial Bus
UTP: Unshielded twisted pair
VPN: Virtual private network