

Course : ISO/IEC 62443: Understanding Cybersecurity for Industrial Systems

Practical course - 2d - 14h00 - Ref. SYI

Price : 1760 CHF E.T.

NEW

An immersive training course designed to help participants understand the fundamentals of the ISO/IEC 62443 standard, master its terminology and key concepts (zones and channels, Security Levels, Foundational Requirements), and learn how to apply the standard in practice to an industrial system through guided case studies

Teaching objectives

At the end of the training, the participant will be able to:

- ✓ Understanding the cybersecurity challenges of industrial systems (OT/ICS) and how they differ from IT systems
- ✓ Understand the structure of the ISO/IEC 62443 family of standards and the role of each of its documents
- ✓ Conduct a simplified risk analysis and a zone/conduit breakdown for a specific case
- ✓ Identify the responsibilities of the various stakeholders (asset owner, integrator, product supplier)
- ✓ Placing Standard 62443 within the Regulatory Landscape (NIS 2, ANSSI Guidelines)

Intended audience

Mixed IT and OT audience: SOC analysts, CISOs, industrial systems engineers, automation engineers, OT project managers, system integrators, auditors, and cybersecurity consultants.

Prerequisites

Basic knowledge of industrial control systems (PLCs, SCADA, sensors) or control systems in IT networks and systems, as well as cybersecurity (CIA, defense in depth).

Course schedule

PARTICIPANTS

Mixed IT and OT audience: SOC analysts, CISOs, industrial systems engineers, automation engineers, OT project managers, system integrators, auditors, and cybersecurity consultants.

PREREQUISITES

Basic knowledge of industrial control systems (PLCs, SCADA, sensors) or control systems in IT networks and systems, as well as cybersecurity (CIA, defense in depth).

TRAINER QUALIFICATIONS

The experts leading the training are specialists in the covered subjects. They have been approved by our instructional teams for both their professional knowledge and their teaching ability, for each course they teach. They have at least five to ten years of experience in their field and hold (or have held) decision-making positions in companies.

ASSESSMENT TERMS

The trainer evaluates each participant's academic progress throughout the training using multiple choice, scenarios, hands-on work and more. Participants also complete a placement test before and after the course to measure the skills they've developed.

1 industrial cybersecurity

- Fundamental Differences Between IT and OT: Priorities (CIA vs. AIC), Real-Time Constraints, Long Lifecycles, Operational Safety.
- Overview of Notable Incidents: Stuxnet, Triton/Trisis, Industroyer, Colonial Pipeline.
- Reference architecture: the Purdue model (levels 0 through 5).

2 Introduction to the ISO/IEC 62443 Family

- Source of the standard: ISA-99? IEC 62443.
- Structure divided into 4 categories: general, policies and procedures, system, and component.
- List of Key Documents: 62443-1-1, 2-1, 2-4, 3-2, 3-3, 4-1, 4-2.
- The three key roles: asset owner, system integrator, and product supplier.

Case study

Role Mapping — Using a diagram of a fictional factory, identify who does what and which 62443 document applies to each role.

3 Essential Vocabulary for the 62443

- IACS, SUC (System Under Consideration), essential function.
- Zones and Ducts: Definitions, Grouping Principles.
- Security Levels: SL-T (Target), SL-A (Achieved), SL-C (Capability), SL 1 through 4.
- Threat actors according to 62443: from script kiddies to nation-states.

4 The 7 Foundational Requirements (FR)

- FR1: Identification & Authentication Control (IAC).
- FR2: Use Control (UC).
- FR3: System Integrity (SI).
- FR4: Data Confidentiality (DC).
- FR5: Restricted Data Flow (RDF).
- FR6: Timely Response to Events (TRE).
- FR7: Resource Availability (RA).
- Relationship between FR, System Requirements (SR), and Component Requirements (CR).

Group discussion

Group analysis of a FR along with its associated SRs and Requirement Enhancements (RE) based on the target SL.

5 Risk Analysis in Accordance with 62443-3-2

- The 7-step ZCR (Zone and Conduit Requirements) process.
- Identification of the SUC and initial division into zones/ducts.
- Initial Risk Assessment and Determination of the SL-T.
- The concept of tolerable risk and iteration.

Case study

(In a small manufacturing plant equipped with MES, SCADA, PLCs, sensors, and remote supplier access), participants divide the system into zones and conduits on a paper layout, explain their choices, and assign an SL-T to each zone.

TEACHING AIDS AND TECHNICAL RESOURCES

- The main teaching aids and instructional methods used in the training are audiovisual aids, documentation and course material, hands-on application exercises and corrected exercises for practical training courses, case studies and coverage of real cases for training seminars.
- At the end of each course or seminar, ORSYS provides participants with a course evaluation questionnaire that is analysed by our instructional teams.
- A check-in sheet for each half-day of attendance is provided at the end of the training, along with a course completion certificate if the trainee attended the entire session.

TERMS AND DEADLINES

Registration must be completed 24 hours before the start of the training.

ACCESSIBILITY FOR PEOPLE WITH DISABILITIES

Do you need special accessibility accommodations? Contact Mrs. Fosse, Disability Manager, at psh-accueil@orsys.fr to review your request and its feasibility.

6 From the SL-T to Concrete Actions

- How to translate the target security level into technical and organizational requirements.
- A Practical Guide to 62443-3-3 (System Requirements).
- A Practical Guide to 62443-4-2 (Component Requirements) for Products.
- SL-T/SL-C/SL-A Consistency: What to Do When a Component Does Not Meet the Target SL? (Compensatory Measures)

Case study

For a given area, list the applicable safety requirements based on the selected SL-T and identify likely discrepancies compared to a typical industrial facility.

7 Organizational Aspects: 62443-2-1 and 2-4

- 62443-2-1: The CSMS (Cybersecurity Management System) from the asset owner's perspective.
- 62443-2-4: Requirements for integration and maintenance service providers.
- Link to an existing ISO 27001 ISMS: complementary, not redundant.
- Security lifecycle: design, integration, operation, decommissioning.

8 Product Section: 62443-4-1 and Certification

- 62443-4-1: Vendor-Side Secure Development Lifecycle (SDL).
- 62443-4-2: Technical requirements by component type (software, embedded, network, host).
- An Overview of Certifications: ISASecure, IECCE, and Their Value in a Request for Proposals.
- Regulatory Framework and Ecosystem: The Role of 62443 in NIS2 and the REC Directive.
- ANSSI Guides on Cybersecurity for Industrial Systems and Their Relationship to ISO 62443.
- Additional standards: NIST SP 800-82, IEC 62351.
- Community resources, feedback, organizations (ISA, CLUSIF, CESIN).

Case study

Analyze a technical data sheet for industrial equipment and identify the elements that demonstrate (or do not demonstrate) compliance with 62443-4-2.

This programme is an original creation, developed by the teaching teams at ORSYS Formation. Any reproduction, representation, adaptation or use, in whole or in part, without the prior written authorisation of ORSYS, is strictly prohibited. ORSYS reserves the right to take any action necessary to protect its intellectual property rights.

Dates and locations

REMOTE CLASS

2026 : 30 Nov.

2027 : 15 Mar., 14 June, 9 Sep., 6 Dec.