+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Updated on 02/04/2026

Register

Introduction to Industrial Cybersecurity Training

1 day (7 hours)

Overview

The convergence of IT and OT and the entry into force of the Cyber Resilience Act (CRA) require a new level of rigor in the design of industrial systems. Security is no longer an option: it has become a condition for access to the European market (CE marking).

Our "Introduction to Industrial Cybersecurity" training course summarizes the key concepts of the IEC 62443 reference standard and the new CRA regulatory requirements in a single day. You will learn to identify the fundamental differences between IT and OT security, how to structure a secure architecture (Zones and Conduits), and what "Security by Design" means for your products or installations.

At the end of the training, you will have a clear vision of the actions to be taken to initiate your compliance process and communicate effectively with technical and legal experts.

Like all our training courses, this one is based on the latest ISA/IEC publications and favors a practical approach based on industrial feedback.

Objectives

- Understand the specific challenges of industrial cybersecurity (security vs. confidentiality).
- Master the vocabulary and concepts of IEC 62443 (Zones, Conduits, SL).
- Decipher the requirements of the Cyber Resilience Act (CRA) for manufacturers.
- Know how to define a "Security by Design" strategy.
- Identify vulnerabilities via SBOMs (Software Bill of Materials).

Target audience

- Industrial project managers & Product Owners

- IoT system and solution architects
- Quality/compliance managers
- IT/OT technical decision-makers

Prerequisites

- General IT and industrial knowledge.
- No prior knowledge of the IEC 62443 standard is required.

Hardware requirements

- A standard laptop is sufficient for viewing documents and participating in architecture workshops.

Our Industrial Cybersecurity Training Program

[Morning]

OT Fundamentals and IEC 62443 Architecture

- Context: IT/OT convergence and overview of threats (ransomware, sabotage)
- The AIC triad (Availability, Integrity, Confidentiality) in industry
- Introduction to the IEC 62443 standard: philosophy and structure
- Network segmentation: Zone and conduit concepts
- Understanding Security Levels (SL)
- The "Defense in Depth" model applied to the factory
- Hands-on workshop: Mapping an industrial system and defining Zones/Conduits (on paper/whiteboard).

[Afternoon]

CRA compliance and secure lifecycle

- Understanding the Cyber Resilience Act (CRA): scope and obligations
- The link between CRA and IEC 62443-4-1 (Secure Product Development Lifecycle)
- Essential requirements: Security by Design and Secure by Default
- Vulnerability management and SBOM (Software Bill of Materials)
- Maintenance and incident management (Notification within 24 hours)
- Roadmap: where to start with compliance?
- Hands-on workshop: Flash audit (gap analysis) of a fictitious product against CRA requirements.

Companies concerned

This training is intended for both individuals and companies, large or small, wishing to train their teams in new advanced IT technology or to acquire specific business knowledge or modern methods.

Positioning at the start of training

The positioning at the start of the training complies with Qualiopi quality criteria. Upon final registration, the learner receives a self-assessment questionnaire that allows us to assess their estimated level of proficiency in different types of technologies, as well as their expectations and personal objectives for the upcoming training, within the limits imposed by the selected format. This questionnaire also allows us to anticipate certain connection or internal security issues within the company (intra-company or virtual classroom) that could be problematic for the monitoring and smooth running of the training session.

Teaching methods

Practical training: 60% practical, 40% theory. Training materials distributed in digital format to all participants.

Organization

The course alternates between theoretical input from the trainer, supported by examples and discussion sessions, and group work.

Assessment

At the end of the session, a multiple-choice questionnaire is used to verify that the skills have been correctly acquired.

Certification

A certificate will be issued to each trainee who has completed the entire training course.