Course Title:

ISA/IEC 62443 Cybersecurity Fundamentals Specialist
Duration: 5 Days

Course Overview

This course provides a comprehensive understanding of the ISA/IEC 62443 series of standards for securing Industrial Automation and Control Systems (IACS). Participants will learn the key concepts, terminologies, security principles, and implementation requirements necessary to protect industrial systems against cyber threats. The program covers the standard's structure, foundational security requirements, risk assessment methods, and compliance approaches, preparing learners for the Cybersecurity Fundamentals Specialist certification.

Prerequisites

- Basic knowledge of industrial automation and control systems (IACS) or operational technology (OT) environments
- Familiarity with general IT/OT cybersecurity concepts and terminology
- Understanding of networking fundamentals (TCP/IP, firewalls, segmentation)
- Recommended: Some experience in operations, engineering, cybersecurity, or system integration in an industrial setting

---

Day 1 – Introduction to Industrial Automation & Control Systems (IACS) Cybersecurity

1. **Course Introduction & Objectives**
2. **Overview of Industrial Automation and Control Systems**
    - Components of IACS
    - OT vs IT
    - Typical architectures & protocols
3. **Cybersecurity in the IACS Context**
    - Why cybersecurity is critical for IACS
    - Differences between IT security & OT security
4. **Introduction to ISA/IEC 62443 Standard Series**
    - Structure of the standard (Parts 1–4)
    - Key terminology & concepts

5. **Threat Landscape in Industrial Environments**
    - Common cyber threats to IACS
    - Case studies of notable ICS cyber incidents (e.g., Stuxnet, TRITON)

Day 2 – Security Concepts & Foundational Requirements

1. **Core Security Concepts**
    - CIA Triad & IIoT security considerations
    - Zones & conduits model
    - Defense-in-depth
2. **Risk-based Approach**
    - Threats, vulnerabilities & consequences in IACS
    - Introduction to risk assessment in the ISA/IEC 62443 context
3. **Foundational Requirements (FRs) Overview**
    - Identification & authentication control
    - Use control
    - System integrity
    - Data confidentiality
    - Restricted data flow
    - Timely response to events
    - Resource availability

Day 3 – Roles, Responsibilities & Security Levels

1. **IACS Stakeholders and Roles**
    - Asset owners
    - System integrators
    - Product suppliers
2. **Security Lifecycle Concept**
    - Secure design
    - Integration & operation
    - Maintenance & decommissioning
3. **Security Levels (SL 1–4)**
    - Understanding SL definitions and applicability
    - Mapping security requirements to SLs
4. **Security Program Requirements**
    - Security policies & governance
    - Procedures & documentation

Day 4 – Applying ISA/IEC 62443 Requirements

1. **Overview of ISA/IEC 62443 Parts**
    - Part 1: General concepts
    - Part 2: Policies & procedures for system security
    - Part 3: System security requirements & security levels
    - Part 4: Product development & component security
2. **Risk Assessment & Analysis Process**
    - Identifying critical assets & vulnerabilities
    - Threat modeling in ICS
3. **Security Requirements Specification (SRS)**
    - Developing SRS for IACS

Day 5 – Incident Response, Compliance & Certification

1. **Incident Response in IACS**
    - Preparation, detection, containment, eradication, recovery
    - Communication protocols during incidents
2. **Monitoring & Continuous Improvement**
    - Security monitoring in OT networks
    - Log management & anomaly detection
3. **Conformance & Certification**
    - ISA Secure Certification programs
    - Compliance process for ISA/IEC 62443
4. **Course Review & Exam Preparation**
    - Key concepts recap
    - Sample exam questions & practice discussion
5. **Final Assessment**
    - Mock exam & feedback