Course Title:

ISA/IEC 62443 Cybersecurity Design Specialist
Duration: 5 Days

Course Overview

This course equips participants with the knowledge and skills to design secure Industrial Automation and Control Systems (IACS) that comply with ISA/IEC 62443 requirements. It covers secure architecture principles, applying security levels, implementing zones and conduits, selecting security controls, and integrating cybersecurity into the system design lifecycle. Participants will learn how to translate security requirements into technical and procedural measures while balancing operational constraints and safety requirements.

Prerequisites

- Understanding of IACS/OT environments and basic control system architecture
- Knowledge of general cybersecurity principles and risk assessment concepts
- Familiarity with ISA/IEC 62443 structure and terminology
- Recommended: Completion of ISA/IEC 62443 Cybersecurity Fundamentals Specialist and Cybersecurity Risk Assessment Specialist courses

---

Day 1 – Introduction to Secure IACS Design

1. **Course Introduction & Objectives**
2. **Role of Secure Design in the Cybersecurity Lifecycle**
    - Differences between IT and OT design considerations
    - Integration with ISA/IEC 62443 framework
3. **Security-by-Design Principles**
    - Defense-in-depth
    - Least privilege and segregation of duties
4. **Security Levels and Their Application in Design**
    - SL1–SL4 in system architecture
5. **Understanding Design Requirements from Risk Assessments**

Day 2 – IACS Secure Architecture & Network Segmentation

1. **IACS Reference Architectures**
    - Purdue Enterprise Reference Architecture
    - ISA/IEC 62443 architectural models
2. **Zones and Conduits Implementation**
    - Defining boundaries and trust levels
    - Secure data flow design
3. **Network Segmentation Strategies**
    - VLANs, firewalls, DMZs in OT environments
4. **Designing for Remote Access & Vendor Connections**

Day 3 – Selecting and Applying Security Controls

1. **Security Control Categories**
    - Technical, administrative, and physical controls
2. **Mapping Controls to Foundational Requirements**
    - Identification & authentication control
    - Use control
    - System integrity
    - Data confidentiality
    - Restricted data flow
    - Timely response to events
    - Resource availability
3. **Industrial Protocol Security Considerations**
    - Modbus, DNP3, OPC UA, Ethernet/IP security implications

---

Day 4 – Secure Component & System Integration

1. **Vendor and Product Security Requirements**
    - Compliance with ISA/IEC 62443-4-1 and 4-2
2. **Secure Configuration Management**
    - Hardening guidelines for devices and software
3. **Design for Resilience and Redundancy**
    - High availability and fault tolerance considerations
4. **Secure Integration of IIoT and Cloud-based Solutions**

Day 5 – Validation, Documentation & Lifecycle Maintenance

1. **Validation of Secure Design**
    - Verification & testing during commissioning
    - Security acceptance criteria
2. **Documentation of Security Design**
    - Security design package and as-built diagrams
3. **Lifecycle Considerations**
    - Change management, patching, and upgrade planning
4. **Course Review & Exam Preparation**
    - Key concepts recap
    - Sample exam questions and discussion
5. **Final Assessment**
    - Mock exam & feedback