Course Title:

ISA/IEC 62443 Cybersecurity Risk Assessment Specialist
Duration: 5 Days

Course Overview

This course provides participants with the knowledge and practical skills to conduct cybersecurity risk assessments in Industrial Automation and Control Systems (IACS) environments according to the ISA/IEC 62443 standards. It covers the risk assessment process, asset identification, threat and vulnerability analysis, determination of security levels, and developing risk treatment plans. Learners will gain the capability to align their risk assessments with organizational policies and industry best practices while supporting compliance with ISA/IEC 62443 requirements.

Prerequisites

- Understanding of industrial automation and control systems (IACS) or operational technology (OT)
- Basic knowledge of cybersecurity principles, risk management concepts, and ISA/IEC 62443 fundamentals
- Familiarity with networking concepts (firewalls, segmentation, TCP/IP)
- Recommended: Completion of the ISA/IEC 62443 Cybersecurity Fundamentals Specialist course

---

Day 1 – Introduction to Cybersecurity Risk Assessment in IACS

1. **Course Introduction & Objectives**
2. **Understanding Risk in the IACS Context**
    - Risk definitions & concepts (Likelihood, Consequence, Risk Value)
    - Differences between IT risk assessment and OT risk assessment
3. **ISA/IEC 62443 Risk Assessment Principles**
    - Role of risk assessment in the cybersecurity lifecycle
    - Standard references and alignment with other frameworks (ISO 27005, NIST)
4. **IACS Cyber Threat Landscape**
    - Common threats, attack vectors, and vulnerabilities in OT environments
    - Lessons from real-world ICS cyber incidents

Day 2 – Preparation & Asset Identification

1. **Risk Assessment Preparation**
    - Defining scope, boundaries, and objectives
    - Identifying stakeholders and their roles
2. **System Description & Architecture Review**
    - Network diagrams, control system topology, zones & conduits
3. **Asset Identification & Classification**
    - Critical asset determination
    - Categorizing assets based on business and operational impact
4. **Understanding Consequences**
    - Safety, environmental, financial, and reputational impacts

---

Day 3 – Threat & Vulnerability Analysis

1. **Threat Identification**
    - Threat actor types (insiders, outsiders, nation-states, hacktivists)
    - Motives and capabilities assessment
2. **Vulnerability Identification**
    - Technical vulnerabilities (hardware, software, network)
    - Human and process vulnerabilities
    - Reference sources (CVEs, vendor advisories, threat intelligence)
3. **Determining Likelihood of Threat Exploitation**
4. **Linking Threats, Vulnerabilities, and Consequences**

Day 4 – Risk Evaluation & Security Level Determination

1. **Risk Evaluation Methods**
    - Qualitative, quantitative, and semi-quantitative approaches
    - Risk matrices and scoring methods
2. **Risk Calculation in IACS Context**
    - Determining initial (unmitigated) risk
    - Determining residual (post-control) risk
3. **Security Level Target (SL-T) Determination**
    - Understanding SL1–SL4 in relation to risk reduction needs
4. **Prioritizing Risks for Treatment**

Day 5 – Risk Treatment, Reporting & Continuous Improvement

1. **Risk Treatment Planning**
    - Selecting appropriate controls from ISA/IEC 62443 Foundational Requirements
    - Technical and administrative controls
2. **Documenting and Reporting the Risk Assessment**
    - Report structure and communication to stakeholders
3. **Maintaining & Reviewing Risk Assessments**
    - Periodic review, incident-driven reassessment
4. **Course Review & Exam Preparation**
    - Key concepts recap
    - Sample exam questions and discussion
5. **Final Assessment**
    - Mock exam & feedback