BOOST
THE LEADING TRAINING PROVIDER

Instrumentation & Controls

Industrial Ethernet and Network Security for Control Systems

Course Introduction

This course provides an in-depth understanding of **Industrial Ethernet** and **network security** in control systems. Participants will explore the fundamentals of Ethernet-based communication in industrial automation, including protocols, network architectures, and best practices for securing critical infrastructure. The course also covers **cybersecurity threats, risk mitigation strategies, and industrial network hardening techniques** to ensure reliable and secure operations.

Target Audience

- Industrial automation and control engineers
- Network and IT professionals managing industrial networks
- Cybersecurity specialists securing control systems
- Maintenance and reliability engineers for industrial networks
- Process control specialists ensuring secure communication
- Operational Technology (OT) professionals handling ICS security

Learning Objectives

- Understand **Industrial Ethernet** and its role in process automation and control systems.
- Learn about **key communication protocols** such as **PROFINET, EtherNet/IP, Modbus TCP, and OPC UA**.
- Design and configure **Ethernet-based industrial networks**.
- Implement **redundancy and reliability** strategies for industrial networks.
- Identify **cybersecurity threats** to industrial control systems (ICS).

- Apply **network security best practices** to protect industrial systems from cyberattacks.
- Explore **firewalls, VLANs, VPNs, and intrusion detection systems (IDS)** for industrial environments.
- Conduct **network troubleshooting and diagnostics** to ensure uptime and efficiency.

Course Outline

- **01 Day One**

  Module 1: Introduction to Industrial Ethernet

  - Basics of **Ethernet technology** and its application in industrial automation
  - Comparison of **traditional fieldbus vs. Industrial Ethernet**
  - Overview of **Ethernet topologies** (star, ring, mesh) and network components

  Module 2: Industrial Ethernet Communication Protocols

  - **PROFINET, EtherNet/IP, Modbus TCP/IP, OPC UA** – features and use cases
  - Real-time communication and deterministic behavior in Ethernet networks
  - Network design considerations for **low-latency and high-availability**

- **02 Day Two**

  Module 3: Network Infrastructure and Redundancy

  - Network **switching, routing, and segmentation**
  - Redundancy protocols: **Rapid Spanning Tree Protocol (RSTP), Media Redundancy Protocol (MRP), Device Level Ring (DLR)**
  - Best practices for **high-availability industrial networks**

- **03 Day Three**

  Module 4: Cybersecurity in Industrial Control Systems (ICS)

  - **Cyber threats and vulnerabilities** in industrial networks
  - Differences between **IT and OT (Operational Technology) security**
  - Case studies on **real-world cyber incidents in industrial automation**

  Module 5: Industrial Network Security Strategies

  - **Network segmentation using VLANs** to isolate control networks
  - **Firewalls and Intrusion Detection/Prevention Systems (IDS/IPS)**

- **Secure remote access** using VPNs and encrypted communication

- **04 Day Four**

Module 6: Hardening Industrial Ethernet Networks

- Role of **zero-trust architecture** in industrial cybersecurity
- Secure device authentication and **role-based access control (RBAC)**
- Implementing **patch management and endpoint security**

- **05 Day Five**

Module 7: Network Monitoring, Troubleshooting, and Maintenance

- **SNMP (Simple Network Management Protocol)** and network monitoring tools
- Identifying and resolving **latency, jitter, and packet loss** issues
- Logging, auditing, and compliance with **IEC 62443 and NIST cybersecurity frameworks**

Confirmed Sessions

FROM	TO	DURATION	FEES	LOCATION
May 4, 2025	May 8, 2025	5 days	4250.00 $	KSA - Al Khobar
July 7, 2025	July 11, 2025	5 days	4950.00 $	Spain - Madrid
Feb. 11, 2025	Feb. 15, 2025	5 days	4250.00 $	Morocco - Casablanca
Jan. 13, 2025	Jan. 17, 2025	5 days	4250.00 $	UAE - Dubai