Control Systems Engineer
SCADA & DCS Architecture & Cybersecurity

IPC022

Course Description

This course is designed for engineers and technical professionals involved in the design, implementation, and maintenance of SCADA (Supervisory Control and Data Acquisition) and DCS (Distributed Control Systems). Participants will gain a comprehensive understanding of the architecture and components of SCADA and DCS systems, with a particular focus on cybersecurity. The course covers the principles of system architecture, the integration of these control systems in various industries, and best practices for securing these systems against cyber threats. Emphasis is placed on real-world applications, security measures, and the ongoing management of SCADA/DCS systems to ensure operational continuity and safety.

Course Objectives

By the end of this course, participants will be able to:

- Understand the fundamental principles and architecture of SCADA and DCS systems.
- Identify the components and functions of SCADA and DCS systems, including field devices, communication protocols, and control loops.
- Understand the integration of SCADA/DCS with other industrial systems (e.g., PLCs, HMIs, and databases).
- Recognize the cybersecurity threats and vulnerabilities in SCADA and DCS systems.
- Implement best practices for securing SCADA/DCS systems against cyberattacks and unauthorized access.
- Develop strategies to monitor and protect critical infrastructure and data in control systems.
- Apply techniques for incident detection, response, and recovery in SCADA/DCS environments.
- Evaluate system performance and ensure high availability and redundancy in control system architectures.

Who Should Attend

- Control systems engineers and technicians working with SCADA and DCS systems.
- IT and cybersecurity professionals focusing on industrial control systems.
- Operations and maintenance personnel responsible for the performance and security of control systems.
- Engineers from other disciplines (e.g., electrical, mechanical, automation) involved in control system projects.
- Anyone seeking to understand the architecture and cybersecurity of SCADA and DCS systems.

Course Duration

5 Working Days

Course Outlines

1. Introduction to SCADA and DCS Systems
    - Overview of SCADA and DCS systems and their importance in industrial control.
    - Key differences between SCADA and DCS: architecture, applications, and functionalities.
    - Basic components of SCADA and DCS: field devices, controllers, and communication networks.
2. SCADA & DCS System Architecture
    - Understanding the architecture of SCADA and DCS systems: control layers and communication.
    - Field devices: sensors, actuators, PLCs, and RTUs (Remote Terminal Units).
    - Master control stations, SCADA servers, HMI (Human-Machine Interface), and database integration.
3. Communication Protocols in SCADA and DCS
    - Common communication protocols: Modbus, OPC, DNP3, and Ethernet/IP.
    - Data acquisition, transmission, and processing in control systems.
    - Ensuring reliability and real-time data processing in SCADA/DCS environments.
4. Cybersecurity for SCADA and DCS Systems
    - Understanding cybersecurity risks and vulnerabilities in control systems.
    - Common threats: malware, denial-of-service attacks, unauthorized access, and physical security risks.
    - Industry regulations and standards for cybersecurity in SCADA and DCS systems (e.g., NIST, IEC 62443).
5. Securing SCADA/DCS Networks and Devices
    - Implementing network security: firewalls, intrusion detection/prevention systems (IDS/IPS), and network segmentation.
    - Device hardening: securing control devices and communication equipment.
    - Secure remote access and monitoring strategies.

6. Incident Detection and Response in SCADA/DCS Systems
    - Techniques for detecting security incidents: monitoring, logging, and anomaly detection.
    - Developing incident response plans: preparation, containment, eradication, and recovery.
    - Forensics and data recovery in SCADA/DCS systems.
7. System Performance and High Availability
    - Ensuring high availability and fault tolerance in SCADA/DCS architecture.
    - Implementing redundancy: backup systems, disaster recovery plans, and failover mechanisms.
    - Performance monitoring and optimization strategies for SCADA/DCS systems.
8. Best Practices for SCADA/DCS Design, Operation, and Maintenance
    - Designing SCADA/DCS systems with security and performance in mind.
    - Best practices for regular system maintenance and updates.
    - Continuous monitoring and system diagnostics.
9. Case Studies and Real-World Applications
    - Review of case studies highlighting successful SCADA/DCS implementation and cybersecurity measures.
    - Lessons learned from cybersecurity incidents in SCADA/DCS environments.