Email: info@gatewayconsulting.com | Phone: +96522968641
https://gatewayconsulting.com

SCADA ENGINEER: SCADA ARCHITECTURE & CYBERSECURITY BEST PRACTICES

Start Date:	21/12/2025	**End Date:**	25/12/2025
Categories:	Cybersecurity	**Venues:**	Dubai
Formats:	In Person	**Instructors:**	

OVERVIEW

This technical course equips participants with comprehensive knowledge of SCADA (Supervisory Control and Data Acquisition) systems, focusing on architecture design, system integration, operations, and cybersecurity best practices. It covers both foundational and advanced topics to ensure the secure and efficient deployment and management of SCADA systems across industrial environments.

OBJECTIVES

By the end of this course, participants will be able to: – Understand SCADA system components, architecture, communication protocols, and integration principles. – Design and optimize SCADA systems to meet operational, monitoring, and control requirements. – Identify cybersecurity vulnerabilities within SCADA environments and apply defense mechanisms. – Implement SCADA security policies in compliance with industry standards and regulations. – Troubleshoot and maintain SCADA systems to ensure operational reliability and resilience against cyber threats.

COURSE OUTLINE

1- Fundamentals of SCADA Systems: Components, Architecture, and Protocols 2- Designing, Integrating, and Optimizing SCADA Architectures 3- Identifying SCADA Cybersecurity Threats and Vulnerabilities 4- Implementing SCADA Security Best Practices and Compliance Standards 5- SCADA System Troubleshooting, Maintenance, and Cyber-Resilience Strategies

TARGET AUDIENCE

SCADA Engineers, Automation Engineers, Control System Engineers, IT Security Professionals, Operations Managers, Plant Engineers, and technical personnel involved in the deployment, maintenance, or security of SCADA and industrial control systems.

METHODOLOGY

The course uses a combination of technical lectures, SCADA system modeling exercises, cybersecurity risk assessment workshops, real-world industrial case study reviews, group discussions, and troubleshooting simulations to provide a balance of theoretical knowledge and

practical skills.

CONCLUSION

Upon completing the course, participants will have the technical expertise to design robust SCADA architectures, secure SCADA environments against cyber threats, and ensure the reliable operation of industrial control systems in various sectors.

DAILY AGENDA

Day 1: Introduction to SCADA Systems: Architecture and Components

Explore SCADA system structures, hardware and software components, communication protocols (e.g., Modbus, DNP3), and their applications across industries.

Day 2: Designing and Integrating SCADA Architectures

Learn system design methodologies, network integration strategies, scalability considerations, and optimization techniques for SCADA networks.

Day 3: SCADA Cybersecurity Threat Landscape and Vulnerability Assessment

Identify common cybersecurity threats targeting SCADA systems, analyze vulnerabilities, and assess potential operational impacts.

Day 4: Implementing SCADA Security Policies and Defense-in-Depth Strategies

Apply security frameworks (such as ISA/IEC 62443), configure secure remote access, and implement monitoring, intrusion detection, and response protocols.

Day 5: SCADA System Maintenance, Troubleshooting, and Cyber-Resilience Building

Perform SCADA system troubleshooting, plan maintenance activities, recover from incidents, and strengthen cyber-resilience through continuous improvement practices.

For more information, please contact us:
Email: info@gatewayconsulting.com | Phone: +96522968641
https://gatewayconsulting.com