PLC, DCS and SCADA Systems Training Course

5 – 9 July 2027
Kuala Lumpur (Malaysia)



PLC, DCS and SCADA Systems Training Course

Ref: 29_239590 **Date:** 5 – 9 July 2027 **Location:** Kuala Lumpur (Malaysia) **Fees:** 4900 GBP

Introduction:

PLC, DCS and SCADA Systems Training Course examines the operational architecture, programming interfaces, distributed process controls, and supervisory monitoring platforms essential to industrial plant automation. This one-week course prepares automation and process control professionals to develop and validate an Integrated Control and Safety Architecture Specification. Delivered at practitioner depth through a hands-on lab practical mode, delegates explore IEC 61131-3, ISA-101, and ANSI/ISA-18.2 alongside the IEC 62443 cybersecurity framework for industrial control systems. Engineering professionals attend the PLC, DCS and SCADA Systems Training Course with Blackbird Training Centre to build reliable, high-performance plant automation networks.

Course Objectives:

- Distinguish between programmable logic controllers, distributed control systems, and supervisory control and data acquisition architectures across plant operations.
- Apply IEC 61131-3 standardized programming languages to execute discrete sequences, analog measurement loops, and interlock logic.
- Select communication protocols and secure network topologies conforming to IEC 62443-3-3 industrial automation cybersecurity requirements.
- Compare ANSI/ISA-18.2 alarm management lifecycles against ISA-101 human-machine interface designs to mitigate operator alarm flooding.
- Interpret continuous closed-loop control dynamics and fieldbus communication diagnostics to resolve plant instrumentation faults.
- Justify safety instrumented system independence from basic process control systems under IEC 61511 functional safety standards.

Target Audience:

- Instrumentation and control engineers responsible for plant automation hardware who must select controller hardware configurations and field loop interfaces.
- Process control system specialists responsible for continuous distributed operations who must determine distributed control system loop tuning and controller redundancy.
- SCADA operations engineers responsible for central supervisory networks who must evaluate telemetry protocol efficiency and alarm rationalization metrics.
- Industrial IT and OT automation technicians responsible for control network maintenance who must decide cybersecurity segmentation boundaries and communication diagnostic tools.



Course Outline:

Day 1: Industrial Control Foundations and Hardware Architectures

- Programmable Logic Controllers vs Distributed Control Systems: Differentiating Architecture Scan Cycles and Operating Philosophies
- Field Instrumentation Wiring: Managing Discrete Signals Analog Loops and Remote IO Racks
- IEC 61131-3 Programming Fundamentals: Structuring Ladder Diagram and Function Block Diagram Logic
- Controller Redundancy Mechanisms: Implementing Hot Standby Processing and Fault Tolerant Power Supplies
- Fieldbus Networking Infrastructure: Configuring PROFIBUS DP and FOUNDATION Fieldbus Digital Signaling

Day 2: Industrial Communication Networks and Security Architecture

- Industrial Ethernet Protocols: Configuring PROFINET Modbus TCP and DNP3 Network Interfaces
- IEC 62443-3-3 System Security Requirements: Establishing Network Segmentation Zones and Conduits
- OPC Unified Architecture IEC 62541 Series: Enabling Secure Open Cross Platform Industrial Interoperability
- Demilitarized Zones vs Enterprise Networks: Securing SCADA Demilitarized Zones and Remote Jump Hosts
- Network Diagnostic Analysis: Troubleshooting Field Loop Noise Ground Loops and Packet Loss

Day 3: Supervisory Systems, HMI Engineering, and Alarm Management

- High Performance HMI ISA-101: Designing Visual Displays and Operational Situational Awareness Standards
- ANSI/ISA-18.2 Alarm Lifecycle: Implementing Rationalization Workflows Prioritization and Flood Suppression
- Real-Time Historian Integration: Setting Up Data Archiving High-Speed Logging and Operational Trending
- Client Server SCADA vs Web Interfaces: Managing Graphic Animation Runtime Tags and Database Links
- Batch Control and Sequence Execution: Implementing Procedural States and Automated Recipe Configurations



Day 4: Functional Safety, Critical Interlocks, and System Hardening

- IEC 61511 Safety Instrumented Systems: Enforcing Separation Between Basic Control and Safety Shutdown
- Safety Integrity Levels vs Basic Control: Evaluating Hazard Risks and Risk Reduction Factors
- Operational Technology Patching Strategies: Deploying Field Controller Updates Without Production Interruption
- Access Control Hardening: Enforcing Multi-Factor Authentication and Restricting Default Engineering Accounts
- Power Quality SEC Directives: Evaluating Redundant Uninterrupted Power Supply and Power Conditioning Rules

Day 5: Hands-on Lab Integration and Specification Delivery

- Multivariable Loop Tuning: Conducting Automated Feedback Parameter Tuning Across Simulation Workstations
- Network Boundary Verification: Auditing Firewalls and Disabled Ports Across Industrial Subnets
- Alarm Annunciation Benchmarking: Stress Testing Plant Screens During Simulated High Consequence Trips
- Root Cause Diagnostics vs Sensor Faults: Resolving Signal Drift and Communication Loss
- Final Deliverable Formulation: Delivering the Integrated Control and Safety Architecture Specification

Skills You Will Gain:

- IEC 61131-3 Programming
- DCS Loop Tuning
- SCADA Screen Development
- ISA-101 HMI Design
- ANSI/ISA-18.2 Alarm Rationalization
- IEC 62443 Network Hardening
- Industrial Protocol Diagnostics
- Safety Instrumented System Separation

Why Attend This Course:

- From relying on disparate automation systems to deploying a unified industrial control infrastructure across plant operations.
- From managing frequent nuisance alarm floods to implementing rigorous alarm rationalization conforming to ANSI/ISA-18.2 and ISA-101 standards.
- From uncertain operational network configurations to engineering secure industrial network segments aligned with IEC 62443 standards.
- From managing isolated field equipment to delivering a verified Integrated Control and Safety Architecture Specification.



Conclusion:

Industrial automation relies on the coordinated operation of programmable logic controllers, distributed control systems, and supervisory platforms to maintain plant productivity and safety. This course establishes essential technical distinctions between high-speed discrete interlocks, complex multivariable distributed control, and wide-area supervisory monitoring. Designed for instrumentation, automation, and control professionals working at practitioner depth, the curriculum equips delegates to configure robust controller architectures, build high-performance operator interfaces, and apply industrial cybersecurity safeguards.

Frequently Asked Questions FAQ:

What is the PLC, DCS and SCADA Systems Training Course?

PLC, DCS and SCADA Systems Training Course is an intensive engineering program examining the hardware, communication protocols, and software platforms that govern plant automation. Delegates learn how to design, program, configure, and secure controllers and supervisory interfaces across discrete, batch, and continuous industrial processing operations.

What is the difference between a PLC, DCS, and SCADA system in this training course?

PLCs excel at high-speed discrete logic, DCS platforms specialize in integrated, complex analog regulatory control for continuous operations, and SCADA systems provide supervisory monitoring, remote telemetry, and data visualization across distributed geographic networks.

Which international engineering standards guide this PLC, DCS and SCADA Systems Training Course?

This course follows IEC 61131-3 for controller programming, ISA-101 for human-machine interface design, ANSI/ISA-18.2 for alarm lifecycle management, IEC 62443 for industrial control systems cybersecurity, and IEC 61511 for process safety instrumented system independence.

Is this course appropriate for control systems engineers working at practitioner depth?

Yes, control systems engineers responsible for configuring controllers, fieldbus networks, and supervisory platforms will gain direct practical skills in loop tuning, network security, alarm rationalization, and system architecture specification design.

