
Industrial Control Systems Oversight: PLC, SCADA and Telemetry Training Course

4 – 8 July 2027
Zoom





Industrial Control Systems Oversight: PLC, SCADA and Telemetry Training Course

Ref: 463_26219 Date: 4 – 8 July 2027 Location: Zoom Fees: 1700 GBP

Programme Summary

Industrial control systems oversight is the subject of this one-week training course for operations, engineering and technology managers, ending in a control system governance pack for their own site or fleet. Many managers approve controller upgrades and vendor contracts without a shared view of how PLC and SCADA estates fail or are secured. The programme moves from architecture to diagnosis of communications and alarms, then to design of security and lifecycle choices, and then to application. Mars Training Centre UK delivers this programme on industrial control systems oversight for managers from mixed organisations.

The Business Case

Automated plants, pipelines and utilities depend on controllers and telemetry that few senior managers see directly, so weaknesses stay hidden until a stoppage or an incident. Managers who cannot read architecture diagrams and alarm records tend to approve changes without clear acceptance tests. A common framework lets operations, engineering and procurement leaders discuss risk, availability and supplier dependence together.

- Availability Management: Improves as single points of failure are found before they cause a stoppage.
- Cyber Exposure: Reduces as network zones and remote access routes are mapped and ranked.
- Lifecycle Cost Control: Strengthens as obsolescence and vendor commitments are planned ahead of failure.

Principles and Evidence Base

- IEC 62443 on the security of industrial automation and control systems: It frames the zone, conduit and security level work in Sessions 3 and 4.
- IEC 61131-3 on programming languages for programmable controllers: It guides the review of program documentation and change records in Session 2.
- Reliability analysis of series and redundant systems: It supports the single point of failure diagnosis in Session 2.

Intended Participants

- Managers who own the availability of automated plants, pipelines or utility networks.
- Engineering leaders who approve control system changes.
- Technology and security leaders who govern operational networks and remote access.
- Procurement and asset leaders who commit to controller, telemetry and software suppliers.



Typical participants come from oil and gas, water and power utilities and process manufacturing.

Learning Outcomes

1. Participants will be able to construct an architecture map of a PLC and SCADA estate from field device to control centre.
2. Participants will be able to diagnose weaknesses in telemetry communications and remote site links.
3. Participants will be able to evaluate alarm records for flooding, shelving and ownership gaps.
4. Participants will be able to prioritise cyber risk by zone, conduit and access route.
5. Participants will be able to compare upgrade and replacement options for ageing controllers.
6. Participants will be able to justify a control system governance pack to senior colleagues.

Programme Structure

Day 1: Reading Control System Architecture from Field to Control Centre

What does the estate consist of, and where does each layer depend on another?

- Field Device to Control Centre Layer Diagram
- PLC and RTU Role Comparison Table
- SCADA Server and Historian Dependency Map
- Telemetry Link Type Overview
- Asset Inventory Template

Day 2: Diagnosing Communications, Availability and Program Control

Where can the estate fail, and how would the failure show itself?

- Series and Redundant Path Failure Chart
- Communication Protocol and Latency Review Sheet
- Single Point of Failure Register
- Program Documentation and Change Record Audit
- Remote Site Outage Scenario Grid

Day 3: Evaluating Alarms and Cyber Exposure

Which alarms and network routes put operations at greatest risk?

- Alarm Flood and Ownership Review Table
- Alarm Philosophy Document Outline
- Network Zone and Conduit Diagram
- Remote Access Route Register
- Security Level Target Grid



Day 4: Designing Lifecycle, Vendor and Upgrade Decisions

How should replacement, support and supplier choices be planned?

- Controller Obsolescence Timeline
- Upgrade versus Replacement Decision Tree
- Vendor Support Dependency Matrix
- Acceptance Test Criteria Checklist
- Spares and Recovery Plan Outline

Day 5: Applying Industrial Control Systems Oversight to One Site

Is the governance pack ready to present to senior colleagues?

- Placing the Site on the Session 1 Architecture Map
- Testing Session 2 Failure Scenarios on Recent Incidents
- Ranking Session 3 Alarm and Cyber Findings
- Selecting Session 4 Lifecycle Options
- Completing the Control System Governance Pack

Methodology

The programme uses a structured exercise method built on anonymised architecture diagrams, alarm logs and incident summaries from pipeline, water and power operations. Participants review the material in small groups and defend each finding to peers who act as operations directors and security leads. Facilitators give feedback on every work product.

- Suggested activity: Tracing one pipeline control loop from sensor to control centre display.
- Suggested activity: Ranking ten alarms by consequence and stating who owns the response.
- Suggested activity: Comparing two controller upgrade routes under a short and a long outage window.

Capstone Output

Each participant completes a control system governance pack for their own site or fleet. It holds an architecture map, a failure register, an alarm and cyber exposure ranking and a lifecycle and vendor plan. The pack is used at work to brief senior colleagues, set upgrade priorities and agree acceptance tests.



Frequently Asked Questions

Is industrial control systems oversight suitable for managers who are not control engineers?

Yes. Industrial control systems oversight is taught at a managerial level and assumes responsibility for automated operations, not programming skill.

Which standards does industrial control systems oversight rest on in this programme?

Industrial control systems oversight rests on IEC 62443, IEC 61131-3 and reliability analysis of redundant systems.

How is the governance pack from industrial control systems oversight used at work?

You use the governance pack to brief senior colleagues, rank upgrade and security priorities and agree acceptance tests before the next change.

How does industrial control systems oversight differ from a programme on PLC programming?

Industrial control systems oversight centres on architecture, risk and supplier decisions for a manager, while PLC programming centres on writing and testing controller logic.