Functional Safety and Industrial Cybersecurity Integration Training Course

28 June – 2 July 2027
Addis Ababa

AGILE LEADERS
Training Center

AGILE LEADERS
Training Center

Functional Safety and Industrial Cybersecurity Integration Training Course

Ref: 769_223987 **Date:** 28 June – 2 July 2027 **Location:** Addis Ababa **Fees:** 4500 Euro

Overview

Functional Safety and Industrial Cybersecurity Integration Training Course is a one-week intermediate course for control engineers, safety practitioners, OT security teams, automation engineers, risk managers, and assurance functions who leave with a Joint Safety-Cyber Assurance Case. Participants connect system boundaries, hazard and threat scenarios, coordinated requirements, risk treatment, change control, incident implications, and assurance evidence across industrial control environments. The course applies IEC TR 63069, IEC 61508, IEC 62443, and OT security guidance without offering certification. Agile Leaders Training Center develops safety-security integration practice.

Who Should Attend

- Control engineering functions responsible for industrial automation design and operation
- Functional safety functions responsible for hazards, requirements, and assurance evidence
- OT cybersecurity functions responsible for threats, zones, conduits, and controls
- Automation maintenance functions responsible for changes and system integrity
- Risk and assurance functions responsible for coordinated industrial decisions

The course assumes participants can interpret industrial control architectures and risk records, and leaves out detailed safety calculations, product certification, penetration testing, and generic enterprise security administration.

Departments and Industries

The course supports departments and industries operating safety-related industrial automation and control systems.

- Process manufacturing and chemical operations
- Energy, utilities, and pipeline control
- Industrial machinery and automated production
- Water and environmental process control
- Engineering assurance and asset maintenance

Learning Objectives

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

- Apply shared safety-security system boundaries
- Analyze linked hazard and cyber threat scenarios
- Build coordinated safety and cybersecurity requirements
- Evaluate controls for safety and security interactions
- Prioritize change and incident assurance evidence
- Build a Joint Safety-Cyber Assurance Case

Course Agenda

Day 1: Establish the Shared System Context

- IEC TR 63069 Integration Framework Map
- IEC 61508 Safety Lifecycle Context Diagram
- IEC 62443 Industrial Security Lifecycle Map
- Shared System Boundary and Asset Register
- Safety-Security Roles and Decision Matrix

Day 2: Connect Hazards and Threats

- Hazard and Cyber Threat Scenario Worksheet
- Unsafe Control Action and Attack Path Map
- Consequence, Likelihood, and Exposure Matrix
- Zone and Conduit Interaction Diagram
- Combined Risk Assumption Register

Day 3: Coordinate Requirements and Controls

- Safety and Security Requirement Traceability Matrix
- Defense-in-Depth and Safety Function Interaction Table
- Control Conflict and Dependency Analysis Method
- Risk Treatment Selection Record
- Verification Responsibility and Evidence Plan

Day 4: Manage Change and Incidents

- Safety-Security Change Impact Checklist
- Configuration Baseline and Approval Record
- Cyber Incident Safety Consequence Decision Tree
- Temporary Control and Compensating Measure Log
- Recovery Validation and Assurance Evidence Pack

Day 5: Practice Joint Assurance

- Exercise: Define Shared Industrial System Boundaries
- Exercise: Link Hazard and Threat Scenarios
- Exercise: Reconcile Conflicting Safety and Security Controls
- Exercise: Assess a Change and Incident Evidence Trail
- Capstone: Joint Safety-Cyber Assurance Case

Practical Exercises

The course uses suggested activities based on process plants, utilities, automated production, and water-control systems.

- Suggested activity: identify shared assets, boundaries, assumptions, and decision owners.
- Suggested activity: connect a cyber attack path with hazardous operational consequences.
- Suggested activity: compare control options for security benefit and safety interaction.
- Suggested activity: assemble requirements, treatment decisions, change records, and evidence into an assurance case.

FAQs

Who suits functional safety and industrial cybersecurity integration training, and what does it assume?

Control engineers, safety practitioners, OT security teams, automation engineers, risk managers, and assurance functions suit the training; it assumes they can interpret control architectures and risk records.

How does safety-security integration differ from generic SCADA security training?

Safety-security integration coordinates hazards, threats, safety functions, cyber controls, changes, incidents, and assurance evidence, while generic SCADA security training concentrates mainly on protecting control-system assets and communications.

Why must functional safety and cybersecurity requirements be coordinated?

Requirements must be coordinated because a security control can affect availability or response timing, while a safety design choice can create access, monitoring, maintenance, or recovery dependencies.

How should industrial teams assess a cybersecurity change for safety impact?

Industrial teams should trace the change to system boundaries, hazards, threats, safety functions, operational modes, dependencies, validation needs, approvals, and residual assumptions before implementation.

AGILE LEADERS
Training Center

What belongs in a joint safety-cyber assurance case?

A joint assurance case should contain scope, claims, assumptions, linked scenarios, coordinated requirements, treatment decisions, verification evidence, change records, incident implications, gaps, ownership, and review actions.

Conclusion

Participants take back a Joint Safety-Cyber Assurance Case linking boundaries, hazards, threats, requirements, controls, changes, incidents, and evidence. It changes separate safety and cybersecurity records into a coordinated industrial assurance workflow. The case supports traceable decisions across engineering, operations, maintenance, cybersecurity, risk, and assurance functions.