



TECHNICAL LEARNING AND ASSESSMENT DOSSIER

OT / ICS / IIoT Cybersecurity Specialist

Course + certificate

On request

VAT excluded

Course code

OT-ICS-SEC

Minimum duration

480 min

Final pass score

75%

Dossier issue

13/10/2026

1. Course identity, purpose and scope

Specialist pathway to protect industrial, OT and control-system environments through an asset-driven, safe and process-compatible approach.

This extended technical dossier describes the pathway as published in CIWZ Academy on the issue date. It consolidates purpose, references, learning architecture, module contents, assessment system, passing criteria and certificate conditions. It does not replace the official texts of the standards, laws, guidelines or schemes referenced.

2. Normative, regulatory and technical references

IEC 62443 family; NIST SP 800-82 Rev.3; MITRE ATT&CK for ICS; industrial network security best practices

References are used as the learning and assessment framework within the limits of published content and available sources. For professional application, the official and current versions of the referenced documents always prevail.

3. Learning architecture and assessment system

- 8 structured learning modules
- minimum tracked time: 480 min
- intermediate-check bank: 256 questions
- active final-exam bank: 240 questions
- final exam: 30 questions selected from the bank
- passing threshold: 75%
- Access to the pathway through the personal Academy profile or a corporate assignment.
- Sequential study of the modules, with server-side recording of progress and required minimum time.
- Intermediate checks linked to modules to verify understanding, application capability and quality of reasoning.

- Final exam unlock only after the pathway requirements have been completed.
- Protected final exam assembled by the platform through selection from the active course question bank.
- Recording of the result and, where applicable, the option to request the final certificate.

4. Official catalogue technical information

Course technical sheet

Specialist CIWZ Academy pathway with original content, server-tracked lessons, 8 modules, randomized intermediate checks, protected final assessment and a scenario-based question bank. Indicative average market benchmark: EUR 2,790 (typical range EUR 1,890 – EUR 3,990). Free access; any fee applies only to certificate issuance after passing.

5. Detailed course syllabus

The following syllabus is derived from the active modules published on the platform. Each module shows its minimum study time and the size of its available intermediate-check bank.

01 OT/ICS context, safety and process

Minimum time: 60 min | Intermediate questions: 32

02 Purdue architectures, segmentation and remote access

Minimum time: 60 min | Intermediate questions: 32

03 Asset visibility, protocol awareness and passive monitoring

Minimum time: 60 min | Intermediate questions: 32

04 Hardening PLCs, HMIs, workstations and OT servers

Minimum time: 60 min | Intermediate questions: 32

05 Identity, privileged access and OT change control

Minimum time: 60 min | Intermediate questions: 32

06 Detection, incident response and recovery in OT

Minimum time: 60 min | Intermediate questions: 32

07 IIoT, edge and IT/OT integration

Minimum time: 60 min | Intermediate questions: 32

08 Governance, 62443 program and operational maturity

Minimum time: 60 min | Intermediate questions: 32

6. Developed module-by-module contents

The following pages analytically describe the content actually associated with each platform module. The structure is designed so that learners, companies, HR, Quality, HSE or CISO functions can understand precisely what is studied and assessed.

MODULE 01**OT/ICS context, safety and process**

- Minimum required time: 60 min
- Available intermediate-check bank: 32 questions

Executive briefing

Understand the difference between IT and OT, safety/availability priorities and the specifics of industrial systems.

Expected specialist competencies

The module is designed for operators who must turn the topic into designs, configurations, procedures and defensible technical decisions. Focus: Map process, assets, zones, conduits and impacts on physical safety and continuity.

Operational method

Apply the following pattern: define objective and risk, design the measure, implement it in a controlled way, collect evidence, measure effectiveness and review it. In this module: Map process, assets, zones, conduits and impacts on physical safety and continuity.

Configurations, proof and evidence

Mature adoption requires technical, operational and decision evidence. Key evidence: Asset inventories, process maps, zone/conduit models and criticality matrices.

Professional scenario

A plant modernizes lines but does not know all OT assets: start safe discovery. The analysis must distinguish urgency, residual risk, ownership, compensating measures and acceptance criteria.

KPIs, KRIs and weak signals

Measure not only implementation but also effectiveness. Minimum indicators: Coverage of OT assets and zones with defined owners.

Pitfalls to avoid

Specialist programs often fail due to technical superficiality or weak governance. Avoid: OT treated like IT, no process view, invisible assets.

Decision laboratory

Exercise: a change, anomaly or business request forces a rapid choice. Describe the decision, criteria, evidence to collect and the effectiveness test. Apply it to the theme "OT/ICS context, safety and process".

Assessment preparation

Before the final assessment, make sure you can explain why a technical choice is correct, identify at least two alternatives, state the necessary evidence and justify which configuration is truly sustainable.

MODULE 02**Purdue architectures, segmentation and remote access**

- Minimum required time: 60 min
- Available intermediate-check bank: 32 questions

Executive briefing

Design segmented industrial networks and secure remote access without compromising the process.

Expected specialist competencies

The module is designed for operators who must turn the topic into designs, configurations, procedures and defensible technical decisions. Focus: Apply zones/conduits, jump hosts, remote-vendor control, industrial firewalls and monitoring.

Operational method

Apply the following pattern: define objective and risk, design the measure, implement it in a controlled way, collect evidence, measure effectiveness and review it. In this module: Apply zones/conduits, jump hosts, remote-vendor control, industrial firewalls and monitoring.

Configurations, proof and evidence

Mature adoption requires technical, operational and decision evidence. Key evidence: Network architectures, remote-access procedures, firewall rules and vendor-access logs.

Professional scenario

A vendor maintains PLCs via permanent VPN: redesign access. The analysis must distinguish urgency, residual risk, ownership, compensating measures and acceptance criteria.

KPIs, KRIs and weak signals

Measure not only implementation but also effectiveness. Minimum indicators: Controlled remote sessions, segmentation implemented, open exceptions.

Pitfalls to avoid

Specialist programs often fail due to technical superficiality or weak governance. Avoid: Flat plant networks, permanent access, unmanaged dual-homed devices.

Decision laboratory

Exercise: a change, anomaly or business request forces a rapid choice. Describe the decision, criteria, evidence to collect and the effectiveness test. Apply it to the theme "Purdue architectures, segmentation and remote access".

Assessment preparation

Before the final assessment, make sure you can explain why a technical choice is correct, identify at least two alternatives, state the necessary evidence and justify which configuration is truly sustainable.

MODULE 03**Asset visibility, protocol awareness and passive monitoring**

- Minimum required time: 60 min
- Available intermediate-check bank: 32 questions

Executive briefing

Gain visibility on industrial protocols, baselines and anomalies without disrupting the process.

Expected specialist competencies

The module is designed for operators who must turn the topic into designs, configurations, procedures and defensible technical decisions. Focus: Use passive discovery, protocol decoders, asset fingerprinting and behavioural baselines.

Operational method

Apply the following pattern: define objective and risk, design the measure, implement it in a controlled way, collect evidence, measure effectiveness and review it. In this module: Use passive discovery, protocol decoders, asset fingerprinting and behavioural baselines.

Configurations, proof and evidence

Mature adoption requires technical, operational and decision evidence. Key evidence: Passive-monitor inventories, protocol maps, baseline anomalies and traffic reports.

Professional scenario

A cell uses undocumented legacy protocols: build the operational baseline. The analysis must distinguish urgency, residual risk, ownership, compensating measures and acceptance criteria.

KPIs, KRIs and weak signals

Measure not only implementation but also effectiveness. Minimum indicators: Discovered assets, decoded protocols, confirmed anomalies.

Pitfalls to avoid

Specialist programs often fail due to technical superficiality or weak governance. Avoid: Unauthorized active scans, unknown protocols, missing baselines.

Decision laboratory

Exercise: a change, anomaly or business request forces a rapid choice. Describe the decision, criteria, evidence to collect and the effectiveness test. Apply it to the theme "Asset visibility, protocol awareness and passive monitoring".

Assessment preparation

Before the final assessment, make sure you can explain why a technical choice is correct, identify at least two alternatives, state the necessary evidence and justify which configuration is truly sustainable.

MODULE 04**Hardening PLCs, HMIs, workstations and OT servers**

- Minimum required time: 60 min
- Available intermediate-check bank: 32 questions

Executive briefing

Apply hardening measures compatible with vendor support and plant availability.

Expected specialist competencies

The module is designed for operators who must turn the topic into designs, configurations, procedures and defensible technical decisions. Focus: Manage accounts, application control, controlled patching, removable media and service minimization.

Operational method

Apply the following pattern: define objective and risk, design the measure, implement it in a controlled way, collect evidence, measure effectiveness and review it. In this module: Manage accounts, application control, controlled patching, removable media and service minimization.

Configurations, proof and evidence

Mature adoption requires technical, operational and decision evidence. Key evidence: Hardening baselines, vendor matrices, patch approvals and workstation-control evidence.

Professional scenario

A critical HMI cannot be patched soon: define effective compensating controls. The analysis must distinguish urgency, residual risk, ownership, compensating measures and acceptance criteria.

KPIs, KRIs and weak signals

Measure not only implementation but also effectiveness. Minimum indicators: Stations compliant with baseline, overdue patches, removable-media exceptions.

Pitfalls to avoid

Specialist programs often fail due to technical superficiality or weak governance. Avoid: Indiscriminate or absent patching, shared local accounts, uncontrolled USB use.

Decision laboratory

Exercise: a change, anomaly or business request forces a rapid choice. Describe the decision, criteria, evidence to collect and the effectiveness test. Apply it to the theme "Hardening PLCs, HMIs, workstations and OT servers".

Assessment preparation

Before the final assessment, make sure you can explain why a technical choice is correct, identify at least two alternatives, state the necessary evidence and justify which configuration is truly sustainable.

MODULE 05**Identity, privileged access and OT change control**

- Minimum required time: 60 min
- Available intermediate-check bank: 32 questions

Executive briefing

Bring access, changes and accountability under control in OT environments.

Expected specialist competencies

The module is designed for operators who must turn the topic into designs, configurations, procedures and defensible technical decisions. Focus: Separate roles, manage shared vendor credentials, change logging and approvals.

Operational method

Apply the following pattern: define objective and risk, design the measure, implement it in a controlled way, collect evidence, measure effectiveness and review it. In this module: Separate roles, manage shared vendor credentials, change logging and approvals.

Configurations, proof and evidence

Mature adoption requires technical, operational and decision evidence. Key evidence: Access registers, change tickets, configuration backups and approval evidence.

Professional scenario

An emergency PLC change is made without traceability: rebuild the process. The analysis must distinguish urgency, residual risk, ownership, compensating measures and acceptance criteria.

KPIs, KRIs and weak signals

Measure not only implementation but also effectiveness. Minimum indicators: Changes with approval, configuration backups, privileged accesses reviewed.

Pitfalls to avoid

Specialist programs often fail due to technical superficiality or weak governance. Avoid: Shared credentials seen as inevitable but unmanaged, change control bypassed.

Decision laboratory

Exercise: a change, anomaly or business request forces a rapid choice. Describe the decision, criteria, evidence to collect and the effectiveness test. Apply it to the theme "Identity, privileged access and OT change control".

Assessment preparation

Before the final assessment, make sure you can explain why a technical choice is correct, identify at least two alternatives, state the necessary evidence and justify which configuration is truly sustainable.

MODULE 06**Detection, incident response and recovery in OT**

- Minimum required time: 60 min
- Available intermediate-check bank: 32 questions

Executive briefing

Prepare response and recovery for OT events with safety and continuity impact.

Expected specialist competencies

The module is designed for operators who must turn the topic into designs, configurations, procedures and defensible technical decisions. Focus: Define triggers, roles, isolation decisions, evidence collection and safe recovery.

Operational method

Apply the following pattern: define objective and risk, design the measure, implement it in a controlled way, collect evidence, measure effectiveness and review it. In this module: Define triggers, roles, isolation decisions, evidence collection and safe recovery.

Configurations, proof and evidence

Mature adoption requires technical, operational and decision evidence. Key evidence: OT incident playbooks, escalation maps, recovery procedures and evidence checklists.

Professional scenario

An engineering workstation is suspicious but process shutdown is risky: decide the response. The analysis must distinguish urgency, residual risk, ownership, compensating measures and acceptance criteria.

KPIs, KRIs and weak signals

Measure not only implementation but also effectiveness. Minimum indicators: Detection time, incidents handled with adequate playbooks, recovery-test outcomes.

Pitfalls to avoid

Specialist programs often fail due to technical superficiality or weak governance. Avoid: IR only IT-centric, recovery untested, improvised decisions.

Decision laboratory

Exercise: a change, anomaly or business request forces a rapid choice. Describe the decision, criteria, evidence to collect and the effectiveness test. Apply it to the theme "Detection, incident response and recovery in OT".

Assessment preparation

Before the final assessment, make sure you can explain why a technical choice is correct, identify at least two alternatives, state the necessary evidence and justify which configuration is truly sustainable.

MODULE 07**IIoT, edge and IT/OT integration**

- Minimum required time: 60 min
- Available intermediate-check bank: 32 questions

Executive briefing

Manage sensors, gateways, edge platforms and interconnection between OT, cloud and analytics.

Expected specialist competencies

The module is designed for operators who must turn the topic into designs, configurations, procedures and defensible technical decisions. Focus: Assess trust boundaries, authentication, updates, remote management and data flow.

Operational method

Apply the following pattern: define objective and risk, design the measure, implement it in a controlled way, collect evidence, measure effectiveness and review it. In this module: Assess trust boundaries, authentication, updates, remote management and data flow.

Configurations, proof and evidence

Mature adoption requires technical, operational and decision evidence. Key evidence: IIoT architectures, data-flow maps, edge-security baselines and device inventories.

Professional scenario

New IIoT sensors are connected to the plant network without standards: introduce governance. The analysis must distinguish urgency, residual risk, ownership, compensating measures and acceptance criteria.

KPIs, KRIs and weak signals

Measure not only implementation but also effectiveness. Minimum indicators: Governed devices, secure updates, authorized data flows.

Pitfalls to avoid

Specialist programs often fail due to technical superficiality or weak governance. Avoid: Shadow IIoT, unmanaged gateways, confused trust boundaries.

Decision laboratory

Exercise: a change, anomaly or business request forces a rapid choice. Describe the decision, criteria, evidence to collect and the effectiveness test. Apply it to the theme "IIoT, edge and IT/OT integration".

Assessment preparation

Before the final assessment, make sure you can explain why a technical choice is correct, identify at least two alternatives, state the necessary evidence and justify which configuration is truly sustainable.

MODULE 08**Governance, 62443 program and operational maturity**

- Minimum required time: 60 min
- Available intermediate-check bank: 32 questions

Executive briefing

Elevate OT security to a continuous, measurable and sustainable program.

Expected specialist competencies

The module is designed for operators who must turn the topic into designs, configurations, procedures and defensible technical decisions. Focus: Translate 62443 into roadmaps, roles, minimum requirements and maturity metrics.

Operational method

Apply the following pattern: define objective and risk, design the measure, implement it in a controlled way, collect evidence, measure effectiveness and review it. In this module: Translate 62443 into roadmaps, roles, minimum requirements and maturity metrics.

Configurations, proof and evidence

Mature adoption requires technical, operational and decision evidence. Key evidence: OT roadmaps, maturity assessments, policy sets and governance minutes.

Professional scenario

Leadership invests only after incidents: build a credible program. The analysis must distinguish urgency, residual risk, ownership, compensating measures and acceptance criteria.

KPIs, KRIs and weak signals

Measure not only implementation but also effectiveness. Minimum indicators: Maturity trends, asset coverage, open risks and roadmap progress.

Pitfalls to avoid

Specialist programs often fail due to technical superficiality or weak governance. Avoid: Isolated initiatives, generic requirements copied from IT, intermittent governance.

Decision laboratory

Exercise: a change, anomaly or business request forces a rapid choice. Describe the decision, criteria, evidence to collect and the effectiveness test. Apply it to the theme "Governance, 62443 program and operational maturity".

Assessment preparation

Before the final assessment, make sure you can explain why a technical choice is correct, identify at least two alternatives, state the necessary evidence and justify which configuration is truly sustainable.

7. Assessment system, final exam and passing criteria

- Intermediate checks are linked to individual modules and provide progressive learning control before access to the final assessment.
- The final assessment consists of 30 questions selected from the active course bank. The platform applies an anti-repetition logic for new attempts when the bank size allows it.
- Final question-bank size detected at generation time: 240 active questions.
- Published passing threshold for the course: 75%.
- Questions are intended to assess not only recall but also interpretation, application, evidence selection, scenario assessment and quality of decision-making, depending on the subject matter.

8. Tracking, learning continuity and session integrity

- Path status, completed modules and recorded time are managed server-side when the course uses the Academy learning mode.
- The platform allows the pathway to resume from the recorded point and retains the results of required checks.
- Assessment sessions may be subject to the integrity and proctoring controls enabled by the platform and described in the applicable usage rules.
- Technical and integrity events support assessment and do not replace professional judgement where human review is required.

9. Certificate, use and limitations

The CIWZ certificate, where provided by the pathway and requested after passing, records the result achieved in the stated CIWZ pathway or assessment. It does not automatically replace personnel certification, professional registration, statutory licence, legal qualification or credentials issued by third-party bodies where such requirements are imposed by the applicable scheme.

10. Commercial and tax conditions

- Course + certificate: On request VAT excluded.
- UAE VAT is applied to UAE customers according to billing data and the applicable tax rules.
- Any specific commercial terms, agreements or corporate orders override the public price only when formally accepted by Certificato IWZ FZCO.

11. Dossier document control

- Document automatically generated by CIWZ Academy from the course data published at the time of the request.

- Course code: OT-ICS-SEC
- Document language: EN
- Generation date: 13/10/2026
- For normative and professional application, the current official sources and any applicable procedures/schemes prevail.