



— OT/ICS CYBERSECURITY · FUNCTIONAL SAFETY · TRAINING

In OT and Critical Infrastructure, Cybersecurity becomes a **Safety Function.**

Specialised training that builds OT cybersecurity and functional safety competence, from the control room to the board. Standard or tailored programmes, delivered by an authorised ISA and PECB trainer with real plant-floor experience.

Onsite
workshops

Multi-day
courses

Executive
briefings

One-day formats

Hands-on labs

Certified courses



Authorised ISA and PECB trainer · IEC 62443 · IEC 61511 · ISO/IEC 27001 · ISO 31000

FOR OPERATORS, EPCS, INTEGRATORS AND
MANUFACTURERS IN

Critical infrastructure · Oil & gas · Petrochemicals · Renewables · BESS ·
Power generation, transmission and distribution

information@ot-knight.com

Belgium · Europe · Middle East



Training portfolio

Specialised OT cybersecurity and functional safety training, built around your needs.

OT-Knight develops and delivers specialised training around the needs and context of each customer or partner. Every programme is available as a standard course or adapted in depth, duration and exercises to your assets, maturity and regulatory context, as onsite workshops, multi-day courses or executive briefings.

ONE-DAY FORMAT

Programmes T1 and T2 can be tailored into a focused one-day onsite workshop with a condensed hands-on exercise. Durations shown are indicative.

CERTIFIED COURSES

Authorised ISA & PECB trainer · delivered via our authorised training provider

IC32 Using the ISA/IEC 62443 Standards to Secure Your Control Systems

IC34 IACS Cybersecurity Design & Implementation

IC49 ISASecure Automation and Control System Security Assurance (ACSSA) for Evaluators

IC33 Assessing the Cybersecurity of New or Existing IACS Systems

IC37 IACS Cybersecurity Operations & Maintenance

PECB NIS 2, ISO/IEC 27001 and ISO 31000 courses

T1 Safe & Secure by Design: Operationalising Functional Safety & OT Cybersecurity

3 DAYS

1-DAY OPTION

IEC 61511 · IEC 62443 · ISO/IEC 27001 · ISA-TR84.00.09-2024 · ISASecure ACSSA, for asset owners

- ◆ Where the safety and security lifecycles meet: the IEC 61511 clause 8.2.4 security risk assessment, the SIS security requirements, and the impact on the SRS
- ◆ One combined governance structure: management of change (MoC), competence, audits and proof testing alongside security verification
- ◆ Workshop: a combined safety/security case for one process unit
- ◆ ISA-TR84.00.09-2024 in practice: cyber as a cause of loss of protection layers, and how SIS/BPCS independence affects zone design
- ◆ Preparing an operational site for ISASecure ACSSA certification

T2 IEC 62443 Foundations: The Language of Industrial Cybersecurity

1 DAY

IEC 62443 fundamentals and overview

- ◆ How the series is structured, and who owns which part: asset owner, service provider, integrator, product supplier
- ◆ The roadmap from 2-1 (security program), through 3-2 (risk), 3-3 (system) and 4-1/4-2 (product)
- ◆ The ISASecure certification schemes (CSA, SSA, SDLA, ACSSA)
- ◆ Core concepts: Security Program elements, zones and conduits, Security Levels (SL-T, SL-C, SL-A), Foundational Requirements FR 1–7, defence in depth
- ◆ How the series relates to ISO/IEC 27001 and NIST CSF 2.0

T3 Building Your IEC 62443 Security Program for Asset Owner / Operators

3 DAYS

Security program implementation for asset owners

- ◆ IEC 62443-2-1:2024 structure across the 8 SPEs: ORG, CM, NET, COMP, DATA, USER, EVENT, AVAIL
- ◆ Governance, roles, policies and procedures that operations teams actually use
- ◆ KPIs and continuous improvement
- ◆ Gap assessment, maturity levels and prioritised roadmaps
- ◆ Managing service providers through IEC 62443-2-4

T4 Cyber Risk That Means Something: OT Cyber Risk Management

3 DAYS

IEC 62443-3-2 · ISO/IEC 27005 · ISO 31000

- ◆ ISO 31000 as the umbrella framework, ISO/IEC 27005 for information security risk, and IEC 62443-3-2 for the IACS
- ◆ Consequence-driven assessment: linking to HAZOP and LOPA, and calibrating against the corporate risk matrix
- ◆ Requirements ZCR 1 to ZCR 7: System under Consideration (SuC), initial and detailed risk assessment, zones and conduits, SL-T and the Cybersecurity Requirements Specification (CRS)
- ◆ Hands-on case study, from the SuC to the CRS

T5 One ISMS, Two Worlds: Unifying IEC 62443 and ISO/IEC 27001

2 DAYS

ISMS for process industry operators

- ◆ Extending an ISMS from IT to OT without breaking either one
- ◆ Scope, Statement of Applicability (SoA) and risk treatment for OT assets
- ◆ Mapping ISO/IEC 27001 Annex A controls to the IEC 62443-2-1 requirements and the 62443-3-3 System Requirements (SRs)
- ◆ Making one audit programme cover both certifications

T6 Secure from Spec to Site: The OT Cybersecurity Lifecycle for Automation Solutions

3 DAYS

For service providers: EPCs, integrators, vendors and asset-owner project teams

- ◆ Service provider capabilities under IEC 62443-2-4 for integration and maintenance
- ◆ IEC 62443-4-1 secure development practices (SM, SR, SD, SI, SVV, DM, SUM, SG), and how 4-2 component requirements roll up into 3-3 system capabilities
- ◆ Cybersecurity across the project phases: FEED, detailed design, FAT, SAT, handover, and operations & maintenance
- ◆ Cybersecurity deliverables and contract requirements: CRS, zone and conduit drawings, hardening baselines, user documentation

T7 Trust, but Verify: OT Cybersecurity Assurance from Risk Assessment to Decommissioning

2-3 DAYS

Auditing, evaluating and testing OT cybersecurity

- ◆ Assurance planning across the whole lifecycle: what to verify, when, how, and how independent the verifier must be
- ◆ Security testing that is safe in OT: FAT/SAT security tests, vulnerability assessment, scoping penetration tests for live plants
- ◆ Securely decommissioning OT assets: sanitising data, retiring credentials, managing the change
- ◆ Auditing security programs against IEC 62443-2-1 and 2-4, and verifying SL-A against SL-T for 3-3
- ◆ Writing up evidence, findings and reports the way ISASecure evaluators work

T8 Hands-On Hardening & Testing for ICS Environments

2 DAYS

HANDS-ON LABS

Co-delivered with an expert OT penetration tester · novice to intermediate

- ◆ A practical, OS-agnostic hardening process: the why, when, how and what, and its links to IEC 62443 requirements
- ◆ Building your own hardening scripts and system policies, plus network, physical and user hardening
- ◆ Hardening Windows HMIs and servers, Linux, network devices and PLCs, standalone or domain-joined, including operator jails
- ◆ Verifying hardening with common security tools, in scenario-based labs drawn from real plants

HOW WE WORK WITH YOU

From your needs to lasting competence**Discover**

Your team, your plant
and your learning
objectives

Tailor

Content, duration and
exercises adapted to
you

Deliver

Onsite or in open
sessions, in EN, FR or
ES

Practise

Case studies,
workshops and hands-
on labs

Certify & sustain

Certified exams where
available, and follow-up

WHO WE TRAIN

Operators

Technicians

Engineers

Project teams

EPCs & integrators

Manufacturers

Managers

Management boards

WHERE WE TRAIN

Onsite and open sessions across **Europe and the Middle East**, in-house at your site or through our authorised training provider. Based in Brussels, Belgium.

Working languages: English, French, Spanish.

CERTIFIED COMPETENCE

Member of the ISASecure ACSA Technical Committee



Let's build your team's competence.

Tell us about your team, your plant and your objectives. We will come back with a tailored programme and a practical first session.

✉ information@ot-knight.com

Brussels, Belgium · Europe and the Middle East