



— OT/ICS CYBERSECURITY · FUNCTIONAL SAFETY

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

Services that keep your plant compliant, verified and resilient, from the first drawing to the last shift. People, process and technology, delivered by one accountable partner.

Concept & FEED

Detailed design

Build, FAT & SAT

Commissioning

Operations &
maintenance

Change &
renewal

 **OT Cybersecurity Management as a Service** · all along the lifecycle

FOR OPERATORS AND MANUFACTURERS IN

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

information@ot-knight.com

Belgium · Europe · Middle East

THE CHALLENGE

Your plant should run with safety, security, reliability and productivity.

Regulation is tightening: NIS 2 across Europe, UK NIS and the Cyber Security and Resilience Bill, and the EU Cyber Resilience Act for the products you buy and build. Control systems are more connected than ever. Yet most cybersecurity programmes are designed by IT teams for IT systems, and rarely fit a control room, a turnaround schedule or a safety case.

OUR ANSWER



Cybersecurity and safety, joined up

We work at the interface between OT cybersecurity and functional safety (IEC 62443 with IEC 61511 and ISA TR84.00.09), treating cybersecurity as a safety discipline.



OT-native governance

We implement IEC 62443 and ISO/IEC 27001 together for critical infrastructure. One management system that operators can actually run, not an IT framework stretched over a control room.



Proven, certified competence

Knowledge, skills and behaviour backed by ISA, ISASecure, PECB, TÜV SÜD and Risknowlogy certifications, and a seat on the ISASecure ACSSA Technical Committee.

80+

years of combined OT experience in the field

6

lifecycle stages covered, from FEED to renewal

5

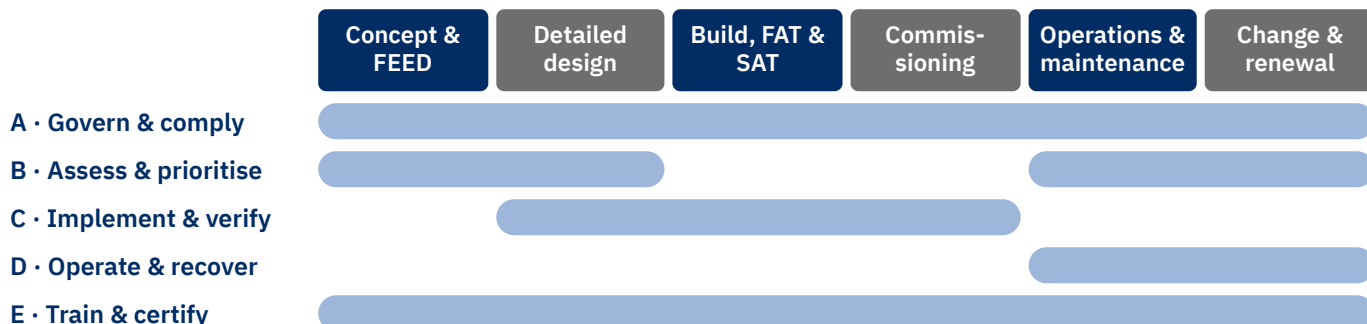
service families, one accountable partner

ML3

ACSSA certification, guided step by step

With you all along the plant lifecycle

Where each service family engages



People

Awareness, competence and clear roles, from operators to the board.

Process

Governance, risk management and procedures that work in a plant.

Technology

Secure architecture, controls and verification in live conditions.



Govern & comply

One management system for IT and OT, and one compliance approach across every jurisdiction you operate in.

A1

Unified Security Management System

IEC 62443 integrated with ISO/IEC 27001

One management system for corporate IT and plant OT, built from the OT side so the controls work in the control room.

YOU GET

- ◆ Combined Management system, Statement of Applicability (IEC 62443-2-1 SPEs + ISO/IEC 27001 Annex A)
- ◆ OT procedures written for operators and maintenance teams
- ◆ Readiness for ISO/IEC 27001 and ISASecure ACSSA

A2

NIS 2 and UK NIS / CSRB, plant-wide

Europe, EEA and the United Kingdom

Compliance for the whole site, OT included, mapped to each country's NIS 2 transposition (such as CyFun® in Belgium) or to UK NIS and the NCSC CAF.

YOU GET

- ◆ Entity classification and scope per site and country
- ◆ One group baseline mapped to every national regime
- ◆ Supervisor-ready evidence and incident reporting

A3

Security lifecycle programme

Focused on SEVESO or COMAH entities

A Cybersecurity Management Plan aligned with IEC 62443 and the functional safety lifecycle - IEC 61511, defining who does what at every gate.

YOU GET

- ◆ FS/CSMP with activities for every project phase and gate
- ◆ EPC-to-operations handover and acceptance criteria
- ◆ KPIs, management reporting and MOC integration

A4

ISASecure ACSSA certification

From ML1 all the way to ML3

ACSSA is the new ISA (ISASecure) certification for asset owners and operators implementing IEC 62443. We guide you along the full roadmap, with insight from our seat on the ACSSA Technical Committee.

YOU GET

- ◆ Eligibility, scoping and zone partition
- ◆ Gap assessment against IEC 62443-2-1, -3-2, -2-4 and -3-3 criteria
- ◆ Mock evaluation, then support through certification

A5

Supply-chain security

One standard for every supplier

EPCs, integrators, OEMs and service providers held to the same security requirements, from tender to handover.

YOU GET

- ◆ IEC 62443-2-4 requirements in tenders and contracts
- ◆ Third-party register and vendor assessments
- ◆ CRA conformity requirements for the products you buy

A6

EU Cyber Resilience Act (CRA)

For manufacturers and integrators

We combine EN 40000 horizontal, vertical and IEC 62443-4-1 / -4-2 standards, so one set of evidence covers them all.

YOU GET

- ◆ Product classification and conformity route
- ◆ Product risk assessment and secure development lifecycle
- ◆ Vulnerability handling, reporting readiness, technical file

B

Assess & prioritise

Know your risk before you spend: one risk language from management to the control room.

B1 Risk management framework

Built on ISO 31000, linking IEC 62443-2-1 organisational requirements, IEC 62443-3-2 OT risk assessment and ISO/IEC 27005, scored on your HSE risk matrix.

DELIVERABLES · methodology, risk criteria, register and treatment workflow

B2 IEC 62443-3-2 risk assessments

System under consideration, zones and conduits, high-level and detailed risk assessment, and a target security level for every zone.

DELIVERABLES · zones and conduits model, SL-T, risk report, Cybersecurity Requirements Specification

B3 Cyber-safety alignment

Cyber threats to your SIS and safety functions assessed as IEC 61511 requires, guided by ISA TR84.00.09 and fed into HAZOP and LOPA.

DELIVERABLES · SIS cybersecurity risk assessment, BPCS/SIS interface advice, SRS input

B4 Gap assessments

Your current state measured against IEC 62443-2-1, ISO/IEC 27001, NIS 2 or UK NIS, the CRA and, where relevant, ACSSA criteria.

DELIVERABLES · gap report, maturity scoring, roadmap planned around your turnarounds

C

Implement & verify

Close the gaps, then prove it, in live plant conditions.

C1 Requirements & specifications

IEC 62443-3-3 requirements at your target security level become the design basis that governs EPC and vendor delivery across the lifecycle.

DELIVERABLES · TRS (Technical Requirements Specification), segmentation and remote access specifications, recovery requirements

C2 OT Cybersecurity Management as a Service

We accompany you all along the lifecycle as your OT cybersecurity function, from objectives and projects to audits.

DELIVERABLES · named lead, project steering, tool selection, ToR, audit readiness, on-call advice

C3 Gap-closing projects

Segmentation, the IT/OT secure interface, secure remote access, hardening, accounts, backup and monitoring: scoped, managed and closed.

DELIVERABLES · scope of work, vendor selection, oversight, closure evidence

C4 Assurance & verification

Tested safely in live plants by people who know them: SL verification, cyber FAT and SAT, OT security assessments, OT penetration testing and audits.

DELIVERABLES · test protocols, witnessed reports, SL verification, findings register

OT Cybersecurity Management as a Service with you all along the lifecycle

- ◆ A named OT cybersecurity lead at your side
- ◆ Cybersecurity projects defined and steered
- ◆ OT security tools selected with you
- ◆ Internal and external audits prepared
- ◆ Core security objectives identified and tracked
- ◆ Gap-closing projects managed to closure
- ◆ Terms of reference and tender specifications
- ◆ On-call answers to ad-hoc questions

D Operate & recover

Ready for the day something goes wrong, and secure every day before it.

D1 Operational posture assessment

How secure is your site as it really runs today? We look beyond the documents: architecture, remote access, accounts, backups, media and daily practice.

DELIVERABLES · score per IEC 62443-2-1 SPE and IEC 62443-3-3 FR, top risks, 90-day action plan

D2 OT incident response

Plans and playbooks written for OT, aligned with your plant safety emergency response and your NIS 2 or UK NIS reporting duties.

DELIVERABLES · response plan, scenario playbooks, escalation matrix, tabletop exercises

D3 Continuity & disaster recovery

Recover your OT systems within defined objectives, combining IEC 62443 AVAIL requirements, ISO 22301, ISO/IEC 27031 and NIST practice.

DELIVERABLES · OT business impact analysis, RTO/RPO, restore procedures and tests

D4 OT monitoring, NDR, EDR & SOC

We define what your NDR, EDR, other monitoring tools and OT-SOC must deliver, select the right provider for your organisation and manage its performance, independent of any SOC vendor.

DELIVERABLES · OT-SOC scope of work, KPI framework, provider selection

E Train & certify

People are the first control: we build competence at every level of your organisation.

E1 Certified ISA and PECB training

Certifying ISA/IEC 62443 courses (IC32, IC33, IC34, IC37, IC49) and PECB courses (NIS 2, ISO/IEC 27001, ISO 31000), delivered by our ISA Qualified Instructor and PECB Certified Trainer through our authorised training provider, in-house or open.

E2 Awareness & competence

Tailored sessions for operators, technicians, engineers, contractors and management boards, including NIS 2 management-body training, built on real plant-floor experience.



“Functional safety and cybersecurity aren't analogous: they literally meet inside the same controller.”

That is why every OT-Knight engagement treats cybersecurity as part of your safety case.



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

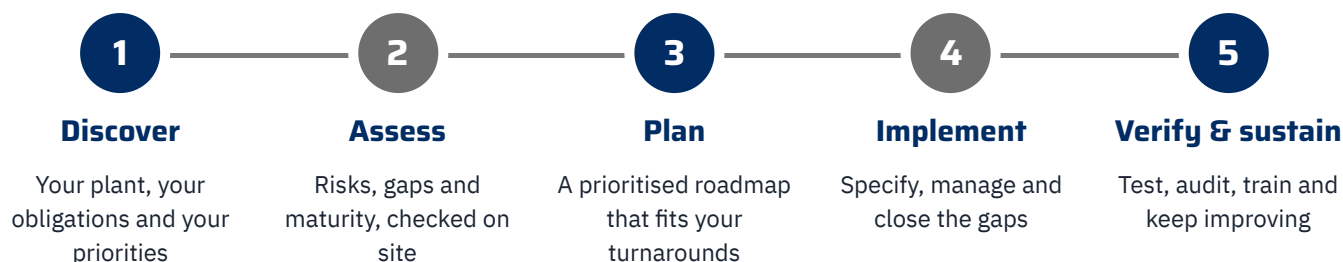
2 DAYS
HANDS-ON LABS

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

A clear path from obligation to secure operation



SECTORS WE KNOW

Critical infrastructure Oil & gas
 Petrochemicals Renewables BESS
 Power generation Transmission (TSO)
 Distribution (DSO/DNO)

WHERE WE WORK

Projects across **Europe and the Middle East**, including multi-country NIS 2 programmes and UK NIS. Based in Brussels, Belgium.

Working languages: English, French, Spanish.

CERTIFIED COMPETENCE

Member of the ISASecure ACSSA Technical Committee



Let's secure your plant together.

Tell us about your plant, your obligations and your next project. We will come back with a clear scope and a practical first step.

✉ information@ot-knight.com

Brussels, Belgium · Europe and the Middle East