OT-Knight
An RBJCS brand

OPLEIDINGSPORTFOLIO



OT/ICS-CYBERSECURITY · FUNCTIONELE VEILIGHEID · OPLEIDING

In OT en kritieke infrastructuur wordt cybersecurity een veiligheidsfunctie.

Kennis die terugkeert naar de installatie. Specialistische programma's in OT-cybersecurity en functionele veiligheid, van controlekamer tot directie, door een erkende ISA- en PECB-trainer met echte praktijkervaring.

Workshops op locatie	Meerdaagse opleidingen	Management-briefings	Eendaagse formats	Praktijk-oefeningen	Gecertificeerde leertrajecten

Erkende ISA- en PECB-opleidingen · IEC 62443 · IEC 61511 · ISO/IEC 27001 · ISO 31000

VOOR EXPLOITANTEN, EPC'S, INTEGRATOREN EN FABRIKANTEN IN

Kritieke infrastructuur · Olie en gas · Petrochemie · Hernieuwbare energie · BESS · Elektriciteitsproductie, -transmissie en -distributie

information@ot-knight.com
België · Europa · Midden-Oosten

Opleidingsportfolio

Kennis die terugkeert naar de installatie.

Acht specialistische programma's, afgestemd op uw team, assets en volwassenheid. Inhoud, diepgang en oefeningen kunnen worden afgestemd op uw team en de toepasselijke regelgeving: workshops op locatie, meerdaagse opleidingen en managementbriefings, in het Engels, Frans of Spaans.

EENDAAGS FORMAT T1 en T2 kunnen een eendaagse workshop ter plaatse worden, met een beknopte praktijkoefening. Duur is indicatief.

GECERTIFICEERDE LEERTRAJECTEN Erkende ISA- en PECB-opleidingen · via onze erkende opleidingspartner

- **IC32** Using the ISA/IEC 62443 Standards to Secure Your Control Systems
- **IC33** Assessing the Cybersecurity of New or Existing IACS Systems
- **IC34** IACS Cybersecurity Design & Implementation
- **IC37** IACS Cybersecurity Operations & Maintenance
- **IC49** ISASecure Automation and Control System Security Assurance (ACSSA) for Evaluators
- **PECB** Cursussen NIS 2, ISO/IEC 27001, ISO 31000

T1 Veiligheid en beveiliging vanaf het ontwerp

3 DAGEN · OPTIE 1 DAG

IEC 61511 · IEC 62443 · ISO/IEC 27001 · ISA-TR84.00.09-2024 · ISASecure ACSSA, voor asseteigenaren

- Waar beide levenscycli samenkomen: cyberrisicoanalyse IEC 61511 (8.2.4), cybereisen voor het SIS en impact op de SRS
- Gecombineerde governance: MoC, competentie, audits en proof testing naast securityverificatie
- Workshop: gecombineerde safety/security case voor één procesunit
- ISA-TR84.00.09-2024 in de praktijk: cyber als oorzaak van verlies van beschermingslagen, en SIS/BPCS-onafhankelijkheid in het zone-ontwerp
- Een draaiende site voorbereiden op ISASecure ACSSA

T2 Basiskennis IEC 62443: de taal van industriële cybersecurity

1 DAG

Basiskennis · Rollen · Normenoverzicht

- Opbouw van de reeks en wie welk deel bezit: asseteigenaren, dienstverlener, integrator, productleverancier
- De roadmap: 2-1 (programma), 3-2 (risico), 3-3 (systeem) en 4-1/4-2 (product)
- ISASecure-schema's (CSA, SSA, SDLA, ACSSA)
- Kernbegrippen: programma-elementen, zones en conduits, SL-T, SL-C en SL-A, Foundational Requirements FR 1–7, defence in depth
- Relatie met ISO/IEC 27001 en NIST CSF 2.0

T3 Uw IEC 62443-beveiligingsprogramma opbouwen

3 DAGEN

Voor asseteigenaren en exploitanten

- IEC 62443-2-1:2024 en de 8 SPE's: ORG, CM, NET, COMP, DATA, USER, EVENT, AVAIL
- Governance, rollen, beleid en procedures die operations echt gebruikt
- KPI's en continue verbetering
- Gap-analyse, maturiteitsniveaus en geprioriteerde roadmaps
- Dienstverleners beheren met IEC 62443-2-4

T4 Cyberrisico's die ertoe doen: OT-cyberrisicomanagement

3 DAGEN

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

- ISO 31000 als overkoepelend kader, ISO/IEC 27005 voor informatierisico's en IEC 62443-3-2 voor het IACS
- Analyse vanuit gevolgen: koppeling met HAZOP en LOPA, kalibratie op de risicomatrix
- ZCR 1 tot ZCR 7: System under Consideration (SuC), initiële en gedetailleerde analyse, zones en conduits, SL-T en eisenspecificatie (CRS)
- Praktijkcase, van SuC tot CRS

T5 Eén ISMS, twee werelden: IEC 62443 en ISO/IEC 27001 samenbrengen

2 DAGEN

ISMS · Koppeling van beheersmaatregelen · Auditprogramma's

- Een ISMS uitbreiden van IT naar OT zonder iets te breken
- Scope, Verklaring van Toepasselijkheid (SoA) en risicobehandeling OT
- Annex A-maatregelen van ISO/IEC 27001 naast de eisen van IEC 62443-2-1 en de SR's van 62443-3-3
- Eén auditprogramma voor beide certificeringen

T6 Beveiligd van specificatie tot site

3 DAGEN

Voor EPC's, integratoren, leveranciers en projectteams van de asseteigenaren

- Capaciteiten van de dienstverlener volgens IEC 62443-2-4 voor integratie en onderhoud
- Veilige ontwikkeling IEC 62443-4-1 (SM, SR, SD, SI, SVV, DM, SUM, SG) en hoe componenteisen 4-2 doorwerken in systeemcapaciteiten 3-3
- Cybersecurity in elke fase: FEED, detailontwerp, FAT, SAT, overdracht, bedrijf en onderhoud
- Deliverables en contracteisen: CRS, zone- en conduittekeningen, hardening-baselines, gebruikersdocumentatie

T7 Vertrouw, maar verifieer: borging van OT-cybersecurity, van risicobeoordeling tot buitenbedrijfstelling

2-3 DAGEN

Audits · Verificatie · Veilige beveiligingstests

- Assuranceplan over de hele levenscyclus: wat, wanneer, hoe en met welke onafhankelijkheid verifiëren
- Veilig testen in OT: securitytests in FAT/SAT, kwetsbaarheidsanalyse, scope van pentesten in draaiende installaties
- OT-assets veilig uit dienst nemen: data wissen, credentials intrekken, wijziging beheren
- Securityprogramma's auditen volgens IEC 62443-2-1 en 2-4, en SL-A tegenover SL-T verifiëren (3-3)
- Bewijs, bevindingen en rapporten zoals ISASecure-evaluatoren werken

T8 Praktische hardening en tests voor ICS-omgevingen

2 DAGEN · PRAKTIJKOEFENINGEN

Samen verzorgd met een specialist in OT-penetratietests · beginner tot gevorderd

- Een praktisch, OS-onafhankelijk hardeningproces: waarom, wanneer, hoe en wat, en de link met IEC 62443
- Eigen hardeningscripts en systeembeleid, plus netwerk-, fysieke en gebruikershardening
- Hardening van Windows-HMI's en -servers, Linux, netwerkapparatuur en PLC's, standalone of in een domein, met afgeschermde operatoromgevingen
- Hardening verifiëren met gangbare tools, in labs gebaseerd op echte installaties

F

Opleiding functionele veiligheid

IEC 61511-competentie van controlekamer tot projectkantoor, afgestemd op uw installatie en procedures.

Alle opleidingen functionele veiligheid worden gegeven in het Engels, Frans en Spaans.

T9 Bewustwording functionele veiligheid: waarom het SIS ertoe doet

HALVE DAG TOT 1 DAG

Voor operators, onderhoudsteams, aannemers en managers

- Wat een veiligheidsinstrumentsysteem doet en hoe het verschilt van het controlesysteem
- Waarom overbruggingen, overrides en niet-beoordeelde wijzigingen de beveiliging in gevaar brengen
- De IEC 61511-veiligheidslevenscyclus in gewone woorden, en wie elke stap beheert
- Wat elke rol moet doen, en nooit mag doen, rond een SIF

T10 IEC 61511 in de praktijk: van gevarenanalyse tot de SRS

3 DAGEN

Voor ingenieurs, procesveiligheidsspecialisten en projectteams

- De veiligheidslevenscyclus en hoe de fasen aansluiten: gevaren- en risicoanalyse, toewijzing, SRS, ontwerp, validatie, bedrijfsvoering
- De SRS opstellen: veilige toestand, trippunten, responstijden, overbruggings- en resetregels, proeftesteisen
- Het SIL-doel bepalen met HAZOP en LOPA, en afstemmen op de risicomatrix van het bedrijf
- Workshop: van een gevarenscenario tot een volledige SRS voor één SIF

T11 SIL-verificatie: aantonen dat het ontwerp zijn doel haalt

2 DAGEN

Voor SIS-ontwerpingenieurs, EPC's en leveranciers

- PFD-berekening voor typische architecturen, en de data en aannames erachter
- Het proeftestinterval bepalen en vastleggen waarvan het resultaat afhangt
- Hardwarefouttolerantie, architectuurbeperkingen en systematische capaciteit
- Workshop: één SIF verifiëren en het resultaat verdedigen in een beoordeling

T12 Het SIS in bedrijf houden: proeftesten, overbruggingen en management of change

2 DAGEN

Voor teams bedrijfsvoering, onderhoud en engineering

- Proeftestprocedures opstellen en uitvoeren, en testintervallen optimaliseren
- Demands en falen opvolgen, en de data gebruiken om de ontwerpaannames te toetsen
- Beheer van overbruggingen en de operationele regels in de SRS
- SIS-wijzigingen beoordelen binnen management of change

T13 Functional Safety Management: het FSM-systeem laten draaien

2 DAGEN

Voor managers, verantwoordelijken functionele veiligheid en projecteigenaren

- Het plan voor functionele veiligheid, de levenscyclus- en validatieplannen, en de rollen van eigenaar, aannemers en leveranciers
- Beoordelingen en audits functionele veiligheid: waar beoordelaars op letten, in elke fase
- Competentiebeheer, verificatieactiviteiten en documentbeheer
- Uw FSM-systeem voorbereiden op beoordeling en op FSMS-certificering

Coaching op echte projecten

wij werken samen met uw team aan uw eigen projecten

Wij helpen uw team de competentie op te bouwen die IEC 61511 vereist, op het werk dat voorligt. Ook: T1, functionele veiligheid en OT-cybersecurity in één cursus (3 dagen of een workshop van één dag).

ONZE AANPAK

De competentie achter elke maatregel

1 **Ontdekken**
Uw team, uw installatie en uw leerdoelen

2 **Afstemmen**
Inhoud, duur en oefeningen op maat

3 **Geven**
Ter plaatse of open sessies, in EN, FR of ES

4 **Oefenen**
Cases, workshops en praktijkoefeningen

5 **Certificeren**
Gecertificeerde examens en opvolging

WIE WIJ OPLEIDEN

- Operators
- Technici
- Engineers
- Projectteams
- EPC's en integratoren
- Fabrikanten
- Managers
- Directies

WAAR WIJ OPLEIDEN

Sessies ter plaatse en open sessies in **Europa en het Midden-Oosten**, bij u op de site of via onze erkende opleidingspartner. Gevestigd in Brussel, België.

Werktalen: Engels, Frans, Spaans.

GECERTIFICEERDE COMPETENTIE

Lid van het ISASecure ACSSA Technical Committee

ISA/IEC 62443 Cybersecurity Expert (ISA) · ISASecure ACSSA for Evaluators Specialist · ISA Qualified Instructor · PECB ISO/IEC 27001 Senior Lead Implementer · PECB ISO/IEC 27001 Senior Lead Auditor · PECB NIS 2 Directive Senior Lead Implementer · PECB ISO 31000 Senior Lead Risk Manager · TÜV SÜD · RISKNOWLOGY Certified Competency

Samen bouwen aan uw team.

Vertel ons over uw team, uw installatie en uw doelen. Wij komen terug met een programma op maat en een concrete eerste sessie.

information@ot-knight.com

Brussel, België · Europa en Midden-Oosten