OT-Knight
An RBJCS brand

PORTFOLIO DE FORMATIONS



CYBERSÉCURITÉ OT/ICS · SÉCURITÉ FONCTIONNELLE · FORMATION

Dans l'OT et les infrastructures critiques, la cybersécurité devient une fonction de sécurité.

Des connaissances qui reviennent sur le terrain. Programmes spécialisés en cybersécurité OT et sécurité fonctionnelle, de la salle de contrôle à la direction, par un formateur autorisé ISA et PECB avec une réelle expérience industrielle.

Ateliers sur site	Formations sur plusieurs jours	Séances pour dirigeants	Formats d'un jour	Travaux pratiques	Parcours certifiants

Formations ISA et PECB autorisées · IEC 62443 · IEC 61511 · ISO/IEC 27001 · ISO 31000

POUR LES EXPLOITANTS, EPC, INTÉGRATEURS ET FABRICANTS DE

Infrastructures critiques · Pétrole et gaz · Pétrochimie · Renouvelables · BESS · Production, transport et distribution d'électricité

information@ot-knight.com
Belgique · Europe · Moyen-Orient

Portfolio de formations

Des connaissances qui reviennent sur le terrain.

Huit programmes spécialisés, adaptés à votre équipe, vos actifs et votre maturité. Le contenu, le niveau de détail et les exercices peuvent être adaptés à votre contexte réglementaire : ateliers sur site, formations sur plusieurs jours et séances pour dirigeants, en anglais, français ou espagnol.

FORMAT D'UN JOUR — T1 et T2 peuvent devenir un atelier d'une journée sur site avec un exercice pratique condensé. Durées indicatives.

PARCOURS CERTIFIANTS

Formations ISA et PECB autorisées · supports PECB en français

- **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** Cours NIS 2, ISO/IEC 27001, ISO 31000

T1 Sécurité fonctionnelle et cybersécurité dès la conception

3 JOURS · OPTION 1 JOUR

IEC 61511 · IEC 62443 · ISO/IEC 27001 · ISA-TR84.00.09-2024 · ISASecure ACSSA, pour les exploitants

- Là où les deux cycles de vie se croisent : analyse de risques cyber IEC 61511 (8.2.4), exigences cyber du SIS et impact sur la SRS
- Gouvernance combinée : MoC, compétences, audits et tests périodiques avec la vérification cyber
- Atelier : dossier sécurité fonctionnelle et cyber d'une unité
- ISA-TR84.00.09-2024 en pratique : le cyber comme cause de perte de couches de protection, et l'indépendance SIS/BPCS dans le zonage
- Préparer un site en exploitation à ISASecure ACSSA

T2 Fondamentaux d'IEC 62443 : le langage de la cybersécurité industrielle

1 JOUR

Fondamentaux · Rôles · Panorama des normes

- Structure de la série et rôle de chacun : propriétaire, prestataire, intégrateur, fournisseur de produits
- La feuille de route : 2-1 (programme), 3-2 (risque), 3-3 (système) et 4-1/4-2 (produit)
- Schémas ISASecure (CSA, SSA, SDLA, ACSSA)
- Concepts clés : éléments du programme, zones et conduits, niveaux SL-T, SL-C et SL-A, exigences FR 1–7, défense en profondeur
- Liens avec ISO/IEC 27001 et NIST CSF 2.0

T3 Construire votre programme de cybersécurité IEC 62443

3 JOURS

Pour les propriétaires d'actifs et les exploitants

- IEC 62443-2-1:2024 et ses 8 SPE : ORG, CM, NET, COMP, DATA, USER, EVENT, AVAIL
- Gouvernance, rôles, politiques et procédures réellement utilisés
- KPI et amélioration continue
- Analyse des écarts, niveaux de maturité et feuilles de route priorisées
- Gérer les prestataires avec IEC 62443-2-4

T4 Un cyberrisque qui a du sens : gestion des cyberrisques OT

3 JOURS

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

- ISO 31000 comme cadre général, ISO/IEC 27005 pour le risque informationnel et IEC 62443-3-2 pour l'IACS
- Analyse fondée sur les conséquences : lien avec HAZOP et LOPA, calibrage sur la matrice de risques
- ZCR 1 à ZCR 7 : système considéré (SuC), analyse initiale et détaillée, zones et conduits, SL-T et spécification des exigences (CRS)
- Étude de cas, du SuC à la CRS

T5 Un SMSI, deux mondes : unifier IEC 62443 et ISO/IEC 27001

2 JOURS

SMSI · Correspondance des mesures · Programmes d'audit

- Étendre un SMSI de l'IT à l'OT sans rien casser
- Périmètre, Déclaration d'applicabilité (SoA) et traitement des risques OT
- Mesures de l'Annexe A ISO/IEC 27001 face aux exigences IEC 62443-2-1 et aux SR 62443-3-3
- Un seul programme d'audit pour les deux certifications

T6 Sécuriser du cahier des charges au site

3 JOURS

Pour EPC, intégrateurs, fabricants et équipes projet de l'exploitant

- Capacités du prestataire selon IEC 62443-2-4 en intégration et maintenance
- Développement sécurisé IEC 62443-4-1 (SM, SR, SD, SI, SVV, DM, SUM, SG) et passage des exigences composant 4-2 aux capacités système 3-3
- Cybersécurité à chaque phase : FEED, ingénierie de détail, FAT, SAT, réception, exploitation et maintenance
- Livrables et exigences contractuelles : CRS, plans de zones et conduits, durcissement de référence, documentation

T7 Faire confiance, mais vérifier : assurance cybersécurité OT, de l'évaluation des risques au démantèlement

2-3 JOURS

Audit · Vérification · Essais de cybersécurité sûrs

- Plan d'assurance sur tout le cycle de vie : quoi vérifier, quand, comment et avec quelle indépendance
- Tests sûrs en OT : tests FAT/SAT, analyse de vulnérabilités, cadrage de tests d'intrusion sur site en exploitation
- Démantèlement sécurisé : effacement des données, identifiants, gestion du changement
- Auditer les programmes selon IEC 62443-2-1 et 2-4, et vérifier SL-A face à SL-T (3-3)
- Preuves, constats et rapports à la manière des évaluateurs ISASecure

T8 Durcissement et essais pratiques pour les environnements ICS

2 JOURS TRAVAUX PRATIQUES

Avec un expert en tests d'intrusion OT · débutant à intermédiaire

- Un processus de durcissement pratique, indépendant de l'OS : pourquoi, quand, comment et quoi, et ses liens avec IEC 62443
- Vos propres scripts et politiques de durcissement, plus durcissement réseau, physique et utilisateurs
- Durcissement des IHM et serveurs Windows, Linux, équipements réseau et automates, autonomes ou en domaine, avec environnements opérateur restreints
- Vérifier le durcissement avec des outils courants, en labs inspirés de sites réels

F

Formation en sécurité fonctionnelle

Compétence IEC 61511 de la salle de contrôle au bureau de projet, construite autour de votre site et de vos procédures.

T9 Sensibilisation à la sécurité fonctionnelle : pourquoi le SIS compte

DEMI-JOURNÉE À 1 JOUR

Pour opérateurs, équipes de maintenance, sous-traitants et managers

- Ce que fait un système instrumenté de sécurité et en quoi il diffère du système de contrôle
- Pourquoi les inhibitions, les forçages et les modifications non revues mettent la protection en danger
- Le cycle de vie de sécurité IEC 61511 en termes simples, et qui est responsable de chaque étape
- Ce que chaque rôle doit faire, et ne doit jamais faire, autour d'une SIF

T10 IEC 61511 en pratique : de l'analyse des dangers à la SRS

3 JOURS

Pour ingénieurs, spécialistes de la sécurité des procédés et équipes projet

- Le cycle de vie de sécurité et l'enchaînement de ses phases : analyse des dangers et des risques, allocation, SRS, conception, validation, exploitation
- Rédiger la SRS : état sûr, seuils de déclenchement, temps de réponse, règles d'inhibition et de réarmement, exigences de tests périodiques
- Détermination du SIL cible avec HAZOP et LOPA, et calage sur la matrice de risque de l'entreprise
- Atelier : d'un scénario de danger à une SRS complète pour une SIF

T11 Vérification SIL : prouver que la conception atteint sa cible

2 JOURS

Pour ingénieurs de conception SIS, EPC et fournisseurs

- Calcul de la PFD pour des architectures types, et les données et hypothèses sous-jacentes
- Fixer l'intervalle de test périodique et documenter ce dont dépend le résultat
- Tolérance aux fautes matérielles, contraintes d'architecture et capacité systématique
- Atelier : vérifier une SIF et défendre le résultat lors d'une évaluation

T12 Exploiter le SIS : tests périodiques, inhibitions et gestion des modifications

2 JOURS

Pour les équipes d'exploitation, de maintenance et d'ingénierie

- Rédiger et exécuter les procédures de tests périodiques, et optimiser les intervalles
- Suivi des sollicitations et des défaillances, et usage des données pour revoir les hypothèses de conception
- Gestion des inhibitions et règles d'exploitation de la SRS
- Revue des modifications du SIS dans le cadre de la gestion des modifications

T13 Management de la sécurité fonctionnelle : piloter le système FSM

2 JOURS

Pour managers, responsables de sécurité fonctionnelle et maîtres d'ouvrage de projet

- Le plan de sécurité fonctionnelle, les plans de cycle de vie et de validation, et les rôles du propriétaire, des sous-traitants et des fournisseurs
- Évaluations et audits de sécurité fonctionnelle : ce que cherchent les évaluateurs, à chaque étape
- Gestion des compétences, activités de vérification et maîtrise documentaire
- Préparer votre système FSM à l'évaluation et à la certification du FSMS

Coaching sur projets réels

nous travaillons aux côtés de votre équipe sur vos propres projets

Nous aidons votre équipe à développer les compétences qu'exige IEC 61511, sur le travail qu'elle a devant elle. Aussi : T1, sécurité fonctionnelle et cybersécurité OT en un cours (3 jours ou 1 jour).

NOTRE MÉTHODE

Les compétences derrière chaque mesure

1 **Découvrir**
Votre équipe, votre site et vos objectifs

2 **Adapter**
Contenu, durée et exercices sur mesure

3 **Dispenser**
Sur site ou en inter, en EN, FR ou ES

4 **Pratiquer**
Études de cas, ateliers et labs

5 **Certifier**
Examens certifiants et suivi

QUI NOUS FORMONS

- Opérateurs
- Techniciens
- Ingénieurs
- Équipes projet
- EPC et intégrateurs
- Fabricants
- Managers
- Conseils d'administration

OÙ NOUS FORMONS

Sessions sur site et inter en **Europe et au Moyen-Orient**, dans vos locaux ou via notre organisme de formation autorisé. Basés à Bruxelles, Belgique.

Langues de travail : anglais, français, espagnol.

COMPÉTENCES CERTIFIÉES

Membre du Comité technique ISASecure ACSSA

Formons ensemble votre équipe.

Parlez-nous de votre équipe, de votre site et de vos objectifs. Nous vous proposerons un programme sur mesure et une première session concrète.

information@ot-knight.com

Bruxelles, Belgique · Europe et Moyen-Orient