OT-Knight
An RBJCS brand

PORTFOLIO DE SERVICES



CYBERSÉCURITÉ OT/ICS · SÉCURITÉ FONCTIONNELLE

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

Protéger ce qui fait fonctionner votre site. Les personnes, les processus et la technologie, de la première esquisse au dernier poste, avec un partenaire responsable.

Concept et FEED	Conception détaillée	Construction, FAT et SAT	Mise en service	Exploitation et maintenance	Modification et renouvellement

Gestion de la cybersécurité OT en tant que service · sur tout le cycle de vie

POUR LES EXPLOITANTS 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

LE DÉFI

Sécurité fonctionnelle, cybersécurité, fiabilité et productivité.

NIS 2 et le CRA durcissent la réglementation. Nous réunissons cybersécurité OT et sécurité fonctionnelle dans des programmes adaptés à la salle de contrôle, aux arrêts programmés et au dossier de sécurité.

NOTRE RÉPONSE

La sécurité comme point de départ

IEC 62443 rejoint IEC 61511 et ISA TR84.00.09 : les cybermenaces sur vos fonctions de sécurité se traitent avec les risques de procédé.

Une gouvernance adaptée à l'OT

IEC 62443 et ISO/IEC 27001 réunies dans un système de management, construit autour des personnes qui exploitent et entretiennent vos actifs.

L'expérience au service du conseil

Des compétences certifiées et une réelle expérience industrielle, avec une participation au comité technique ISASecure ACSSA.

80+
années cumulées d'expérience OT

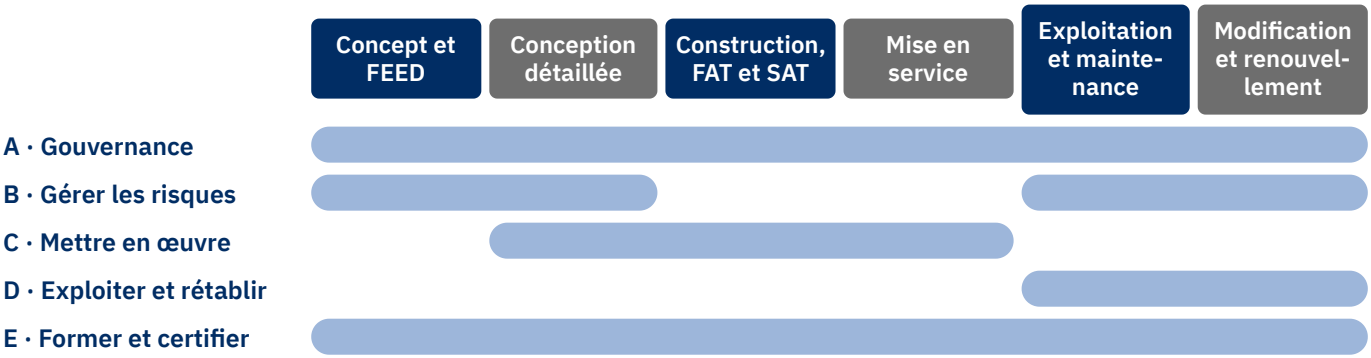
6
étapes, du FEED au renouvellement

5
familles, un partenaire responsable

ML1–3
parcours de certification ACSSA

Un partenaire responsable à chaque étape

Où intervient chaque famille de services



Personnes

Sensibilisation, compétences et rôles clairs, de l'opérateur au conseil.

Processus

Gouvernance, gestion des risques et procédures adaptées au terrain.

Technologie

Architecture sécurisée, mesures et vérification en conditions réelles.

F Sécurité fonctionnelle

Alignée sur le cycle de vie de sécurité IEC 61511 : sûre dès la conception, et sûre en exploitation.

F1 Management de la sécurité fonctionnelle et du cycle de vie

Nous mettons en place et pilotons le système de management qui garde votre SIS sûr toute sa vie, sur un site en exploitation ou dans un projet : prêt pour l'évaluation, avec une remise propre à l'exploitation.

- Planification du cycle de vie
- Planification vérifications et FSA
- Rôles propriétaire et fournisseurs
- Gestion des modifications
- Gestion des compétences
- Maîtrise documentaire

F2 Évaluations de sécurité fonctionnelle

FSA indépendantes à chaque étape du cycle de vie, de l'analyse des dangers et des risques et de la SRS à la mise en service, l'exploitation et les modifications, ainsi que des audits qui vérifient l'application de vos procédures.

LIVRABLES · rapports FSA, audits de sécurité fonctionnelle, registre des constats

F3 Exigences de sécurité (SRS)

Nous rédigeons ou revoyons la SRS de chaque fonction instrumentée de sécurité : état sûr, seuils de déclenchement, temps de réponse, SIL cible, règles d'inhibition et de réarmement, exigences de tests périodiques.

LIVRABLES · SRS, liste des SIF, commentaires de revue

F4 Vérification SIL

PFD, tolérance aux fautes matérielles, contraintes d'architecture et capacité systématique vérifiées pour chaque SIL cible : un calcul indépendant, défendable lors d'une évaluation.

LIVRABLES · rapport de vérification SIL, recommandations

F5 Appui exploitation et maintenance

Procédures de tests périodiques et optimisation des intervalles, suivi des sollicitations et des défaillances, gestion des inhibitions et revue des modifications du SIS en exploitation.

LIVRABLES · procédures de tests périodiques, revues de performance du SIS, revues MoC

F6 Certifiez votre FSMS

Nous vous guidons dans le choix de l'organisme de certification et tout au long du processus. Nous avons mené un FSMS jusqu'à la certification exida : nous connaissons le parcours de l'intérieur.

+ Sécurité et cybersécurité réunies

Un SIS nécessite sa propre analyse des risques de cybersécurité selon IEC 61511. Nous la réalisons en même temps que nos travaux de sécurité fonctionnelle.

F7 Sensibilisation, formation et coaching

de la salle de contrôle au conseil

Sessions de sensibilisation

Sessions courtes pour opérateurs, maintenance, sous-traitants et managers : à quoi sert un SIS et pourquoi les inhibitions comptent.

Formation sur mesure

Le cycle de vie IEC 61511, la détermination du SIL, la SRS, la vérification SIL et les tests périodiques, construits autour de votre site et de vos procédures.

Coaching sur projets réels

Nous travaillons aux côtés de votre équipe sur vos propres projets et l'aidons à développer les compétences exigées par IEC 61511.

Aussi : **Safe & Secure by Design**, sécurité fonctionnelle et cybersécurité OT en un cours (3 jours ou 1 jour). Sur site, en EN, FR ou ES.

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

Un chemin clair. Une prochaine étape concrète.

1 — Découvrir
Votre site, vos obligations et vos priorités

2 — Évaluer
Risques, écarts et maturité, sur site

3 — Planifier
Feuille de route priorisée selon vos arrêts

4 — Mettre en œuvre
Spécifier, piloter et traiter les écarts

5 — Vérifier et pérenniser
Tester, auditer, former et améliorer en continu

CONÇU POUR LES OPÉRATIONS CRITIQUES

- Infrastructures critiques
- Pétrole et gaz
- Pétrochimie
- Énergies renouvelables
- BESS
- Production d'électricité
- Transport d'électricité
- Distribution

OÙ NOUS INTERVENONS

Projets en **Europe et au Moyen-Orient**, dont des programmes NIS 2 multi-pays. Basés à Bruxelles, Belgique.

Langues de travail : anglais, français, espagnol.

COMPÉTENCES CERTIFIÉES

Membre du Comité technique ISASecure ACSSA

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

Sécurisons ensemble votre site.

Parlez-nous de votre site, de vos obligations et de votre prochain projet. Nous vous proposerons un périmètre clair et une première étape concrète.

information@ot-knight.com

Bruxelles, Belgique · Europe et Moyen-Orient

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