# Formation « IEC 62443-2-1 – Cybersécurité des systèmes d'automatisation et de contrôle industriels (IACS) – Lead Implementer »

**Réf : IEC62LI**

Les systèmes d'automatisation et de contrôle industriels (IACS), appelés également systèmes OT (*Operational Technologie*), font l'objet d'un nombre croissant d'attaques. Les incidents récents montrent que la production, la sûreté des installations et la continuité des activités essentielles sont directement exposées à ces menaces. La série de normes IEC 62443 constitue le cadre de référence international pour la cybersécurité des systèmes OT (IACS).

La norme IEC 62443-2-1 décrit les exigences applicables à l'exploitant (*asset owner*) pour établir, mettre en œuvre, maintenir et améliorer un programme de cybersécurité IACS. Elle articule l'ensemble des autres parties de la série : analyse de risque (-3-2), exigences système (-3-3), exigences composants (-4-2), gestion des prestataires (-2-4), terminologie et niveaux de sécurité (-1-1 et -1-5).

La formation IEC 62443-2-1 Lead Implementer d'HS2 est dédiée à la mise en œuvre opérationnelle d'un programme de cybersécurité IACS conforme à cette norme. Son objectif est de permettre aux stagiaires d'implémenter et de piloter un tel programme dans un environnement d'exploitation, en intégrant les obligations réglementaires applicables (NIS2, LPM, CRA, exigences sectorielles). Elle s'appuie sur un scénario fil rouge industriel travaillé tout au long des quatre premiers jours.

## Objectifs

- Présenter la série IEC 62443 et le rôle pivot de la norme 2-1 du point de vue exploitant
- Présenter les exigences des normes IEC 62443-2-1, -3-2, -3-3, -2-4, ainsi que les éléments des -4-1 et -4-2 utiles à l'exploitant
- Présenter la méthodologie d'analyse de risque IACS selon la norme IEC 62443-3-2 et la définition des niveaux de sécurité cibles (SL-T)
- Présenter les différentes étapes d'implémentation et de pilotage d'un programme de cybersécurité IACS conforme à la norme IEC 62443-2-1
- Présenter l'articulation entre le programme de sécurité IACS et les obligations réglementaires (NIS2, LPM, CRA, exigences sectorielles)
- Mettre en pratique les concepts au travers d'un scénario fil rouge industriel

## Durée & horaires

- 5 jours soit 35 heures réparties en 31h30 de cours, 1h00 de travail individuel sur les exercices le soir et 2h30 d'examen.
- Du lundi au jeudi : de 9h30 à 12h00 et de 13h30 à 17h30/18h00.
- Le vendredi : de 09h30 à 12h00 et de 13h30/14h00 à 17h00/17h30.

## Nombre de participant

- Minimum 6 participants – Maximum 12 participants (pour préserver la qualité des exercices fil rouge en sous-groupes).

## Public visé

- RSSI / RSSI OT / Responsables cybersécurité industrielle
- Ingénieurs automatismes, ingénieurs méthodes, responsables d'exploitation
- Chefs de projet cybersécurité industrielle, architectes OT, consultants et intégrateurs
- Responsables conformité et gestionnaires de risques en charge des obligations réglementaires sur des périmètres industriels

- **Toute personne souhaitant implémenter un programme de cybersécurité IACS conforme à la norme IEC 62443-2-1 au sein de son entreprise.**

## Pré-requis

- **Connaître les concepts généraux des systèmes d'automatisation et de contrôle industriels (SCADA, automates, DCS, supervision) est indispensable (SECINDUS ??).**
- **Disposer de notions de base en cybersécurité (notions de risque, de mesure de sécurité, d'architecture réseau).**
- **Une connaissance préalable de la série IEC 62443 n'est pas exigée.**
- **Pour information, la formation et les supports sont en français. La connaissance de l'anglais technique est un plus pour la lecture des références normatives.**

## Méthode pédagogique

**La méthode pédagogique se base sur les quatre points suivants :**

- **Cours magistral basé sur les normes IEC 62443-2-1, IEC 62443-1-1, IEC 62443-1-5, IEC 62443-2-4, IEC 62443-3-2, IEC 62443-3-3, IEC 62443-4-1 et IEC 62443-4-2.**
- **Exercices de contrôle des connaissances sur les concepts à connaître et sur les normes.**
- **Exercices pratiques individuels effectués par les stagiaires, articulés autour d'un scénario fil rouge industriel.**
- **Formation nécessitant quotidiennement 1 heure de travail personnel durant la session.**

## Supports

- **Support de cours au format papier en français**
- **Cahier d'exercices et corrections des exercices**
- **Tous les documents nécessaires à la formation en français ou anglais**
- **Certificat attestant de la participation à la formation**

## Modalité d'évaluation de la formation

- **Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration**

## Certification

- **Cette formation prépare à l'examen de certification HS2 IEC 62443-2-1 Lead Implementer. À l'issue de cette formation, le stagiaire passe l'examen d'une durée de 2h30 en français. L'examen est constitué d'une partie QCM sur les notions de cours et d'une partie rédactionnelle sous forme d'étude de cas.**

## Programme

### 1 - Introduction : Cybersécurité des IACS et série IEC 62443

- **1.1 - Spécificités des environnements OT vs IT :** sûreté, disponibilité, cycles de vie longs, systèmes hérités et contraintes d'arrêt.
- **1.2 - Panorama des menaces visant les IACS et retours d'expérience d'incidents marquants.**
- **1.3 - Histoire et structure de la série IEC 62443 : parties 1, 2, 3 et 4**
- **1.4 - Profils des acteurs des SI industriels :** exploitant (*asset owner*), intégrateur (*service provider*), fournisseur de produits (*product supplier*)
- **1.5 - Présentation générale de la norme IEC 62443-2-1 et de son rôle pivot**

### 2 - Cadre réglementaire applicable aux exploitants

- **2.1 - Directive NIS2 et sa transposition en loi française :** entités essentielles et entités importantes, secteurs concernés, obligations, etc.

- **2.2 - LPM / SAIV / OIV-OSE :** exigences applicables, articulation avec IEC 62443
- **2.3 - Cyber Resilience Act (CRA) :** cadre horizontal cybersécurité produits, obligations des fabricants, leviers contractuels pour l'exploitant, articulation avec IEC 62443-4-1 et -4-2
- **2.4 - Règlement Machines (UE) 2023/1230 :** intégration de la cybersécurité dans les exigences essentielles, notion de modification substantielle, bascule exploitant - fabricant
  - **Convergence réglementaire produit :** panorama CRA, RM 2023/1230, RED 3.3 (régime transitoire 2025-2027), AI Act et leur articulation.
- **2.5 - Réglementations sectorielles applicables** (énergie, eau, transport, santé, pharma)
- **2.6 - Articulation entre IEC 62443-2-1 et les obligations réglementaires**
- **Exercice fil rouge 1 :** présentation d'un dossier-site industriel, identification des fonctions essentielles et cartographie macro du SI.

**3 – Évaluation des risques IACS selon IEC 62443-3-2**

- **3.1 - Démarche ZCR (*Zone and Conduit Requirements*)** : principes, étapes, livrables
- **3.2 - Identification du système à étudier *(SuC - System under Consideration*) et de ses frontières (zones de confiance)**
- **3.3 - Appréciation des risques initiale (*high-level risk assessment*) et critères de tolérance**
- **3.4 - Appréciation des risques détaillée (*detailed risk assessment*) :** scénarios, conséquences, vraisemblance
- **3.5 - Articulation avec d'autres méthodes d'analyse de risques** (EBIOS RM, ISO 27005, HAZOP cyber)

**4 - Zones, conduits, niveaux de sécurité et architecture**

- **4.1 - Découpage en zones de sécurité** : critères, modèle Purdue revisité
- **4.2 - Les conduits** : définition, types (réseau, physique, sans-fil), exigences associées
- **4.3 - Niveaux de sécurité selon IEC 62443-1-5 :** SL-T (*target*), SL-A (*achieved*), SL-C (*capability*)
- **4.4 - Exigences fondamentales** *(Foundational Requirements - FR1 à FR7)*
- **4.5 - Lecture pratique de la norme IEC 62443-3-3 :** *System Requirements* par exigence et par niveau de sécurité
- **4.6 - Principes d'architecture sécurisée :** défense en profondeur, segmentation, cloisonnement IT/OT, DMZ industrielle, accès distants
- **Exercice fil rouge 2 :** analyse de risque ZCR, découpage en zones et conduits, fixation des SL-T

**5 - Programme de cybersécurité IACS selon IEC 62443-2-1**

- **5.1 - Structure de la norme IEC 62443-2-1 et logique des *Security Program Elements* (SPE)**
- **5.2 - Articulation avec un SMSI ISO 27001 et avec les systèmes de management QHSE existants**
- **5.3 - Gouvernance, organisation et rôles :** engagement de la direction, RACI cyber industriel, politiques et procédures
- **5.4 - Gestion des actifs et des configurations :** inventaire, classification, gestion des changements
- **5.5 - Gestion des prestataires et de la chaîne d'approvisionnement**
  - **Lien avec IEC 62443-2-4** (exigences pour intégrateurs et prestataires)
  - **Périmètre exploitant des IEC 62443-4-1 et -4-2** (exigences à porter aux fournisseurs)
  - **Cas particulier de l'exploitant devenu fabricant au sens du Règlement Machines 2023/1230** (modification substantielle)
  - **Preuves de conformité à exiger des fournisseurs par type d'équipement** (CRA, RM, RED transitoire, certification 62443-4-2)
- **5.6 - Gestion des accès, des identités et des comptes à privilèges en environnement OT**
- **5.7 - Gestion des correctifs et des vulnérabilités OT :** analyse d'impact, fenêtres de maintenance, mesures compensatoires
- **5.8 - Sensibilisation, formation et culture cyber OT**
- **5.9 - Intelligence artificielle dans les IACS :** enjeux cyber, sûreté et réglementaires
- **Cas d'usage en environnement industriel** (maintenance prédictive, optimisation procédé, supervision augmentée, régulation adaptative, pilotage autonome)

- **Risques spécifiques à l'IA en OT (***data poisoning, adversarial inputs, drift*, opacité décisionnelle, dépendance fournisseur)
- **Cadre réglementaire** (AI Act, articulation avec RM 2023/1230 et CRA, statut provider et modification substantielle d'un système d'IA)
- **Intégration au programme 62443-2-1** (qualification des projets IA, exigences fournisseurs, supervision humaine, safe fallback, gouvernance)
- **Exercice fil rouge 3 :** rédaction d'éléments clés du programme de sécurité IACS (organisation, politiques, procédures, registre de risques, qualification d'une modification substantielle au regard du RM et de l'AI Act)

**6 - Exploitation, surveillance, réponse à incident et amélioration continue**

- **6.1 - Surveillance et détection en environnement IACS :** spécificités, sources de données, IDS industriels
- **6.2 - Articulation SOC IT / SOC OT et choix des scénarios de détection prioritaires**
- **6.3 - Préparation à la gestion des incidents IACS :** plan, équipes, outils, communication
- **6.4 - Conduite d'une réponse à incident en contexte OT :** détection, analyse, confinement, éradication, restauration
- **6.5 - Articulation avec la sûreté de fonctionnement, continuité d'activité et plan de reprise**
- **6.6 - Obligations de notification** (NIS2, ANSSI, CNIL si applicable)
- **6.7 - Audit interne du programme de sécurité IACS, indicateurs et trajectoire de maturité**
- **Exercice fil rouge 4 :** mise en situation de réponse à incident, notification réglementaire et plan d'amélioration

**7 - Actualité et préparation à l'examen**

- **7.1 - Évolutions récentes de la série IEC 62443 :** parties révisées, parties en cours d'élaboration
- **7.2 – Règlementations :** transposition NIS2, application du Règlement Machines 2023/1230 (janvier 2027), application complète du CRA (décembre 2027), abrogation du volet cybersécurité de la RED, AI Act (2 décembre 2027 pour les standalone high-risk, 2 août 2028 pour l'IA embarquée dans les produits régulés), évolutions sectorielles
- **7.3 - Articulation avec les autres référentiels** (ISO 27001, NIST CSF, certifications sectorielles)
- **7.4 - Révision générale et conseils méthodologiques pour l'examen**

**8 - Conclusion**