IEC 62443 : Maîtriser la Cybersécurité des Systèmes Industriels selon la Norme IEC 62443

Lien : https://innov-systems.com/formation/iec-62443-matriser-la-cybersecurite-des-systemes-industriels-selon-la-norme-iec-62443

DURÉE	RÉFÉRENCE	CATÉGORIE
5 jours (35h)	**SEC278**	**PECB, IEC 62443**

OBJECTIFS DE LA FORMATION

À l'issue de cette formation, vous serez capable de :

- Comprendre l’architecture et la philosophie de la norme IEC 62443 dans un contexte industriel
- Identifier les menaces et vulnérabilités propres aux environnements OT et aux systèmes IACS
- Concevoir et mettre en œuvre un programme de cybersécurité industrielle conforme à la norme
- Réaliser une évaluation de maturité et de conformité des systèmes et processus industriels
- Définir une stratégie de défense en profondeur intégrant les meilleures pratiques « secure by design »
- Intégrer les fournisseurs et prestataires dans une démarche globale de cybersécurité industrielle

POUR QUI ?

- Responsables d’exploitation ou de production industrielle
- Responsables techniques ou responsables maintenance d’installations industrielles
- Chefs de projet ou responsables d’intégration OT/IT
- Responsables sécurité des systèmes d’information (RSSI) secteur industriel
- Ingénieurs ou responsables qualité et conformité dans le domaine industriel

Programme détaillé

1 / FONDAMENTAUX DE LA CYBERSÉCURITÉ INDUSTRIELLE

- Comprendre la différence entre IT et OT
- Identifier les spécificités des environnements industriels
- Panorama des menaces et typologies d’attaques sur les systèmes industriels
- Enjeux économiques, opérationnels et réglementaires

2 / INTRODUCTION À LA NORME IEC 62443

- Historique et objectifs de la norme
- Structure de la série IEC 62443
- Terminologie et définitions essentielles
- Acteurs, rôles et responsabilités au sein d’un environnement IACS

3 / CADRE RÉGLEMENTAIRE ET INTERACTIONS AVEC D’AUTRES RÉFÉRENTIELS

- Lien entre IEC 62443, ISO 27001, NIS2 et DORA
- Exigences légales et conformité
- Articulation entre gouvernance cybersécurité et conformité réglementaire

4 / APPROCHE RISQUE ET MATURITÉ

- Méthodologie d’analyse des risques adaptée aux systèmes industriels
- Identification des actifs critiques et cartographie OT
- Évaluation du niveau de maturité en cybersécurité (modèles et outils)
- Atelier pratique : établir une matrice de risques OT

5 / MISE EN PLACE DU CSMS SELON IEC 62443-2-1

- Les principes et phases du CSMS

- Politique de cybersécurité industrielle et gouvernance
- Processus organisationnels et responsabilités
- Définir les indicateurs de performance et de suivi

6 / LES ZONES ET CONDUITS DE SÉCURITÉ

- Segmentation et défense en profondeur
- Méthodologie de définition des zones de sécurité
- Identification et gestion des conduits (communications interzones)
- Atelier pratique : construction d’une architecture zonée

7 / LES 7 EXIGENCES FONDAMENTALES DE LA NORME IEC 62443

- Contrôle d’accès
- Intégrité des données
- Confidentialité et disponibilité
- Réponse aux incidents
- Restriction des flux de données
- Gestion du changement
- Usage sécurisé des ressources

8 / STRATÉGIES DE DÉFENSE EN PROFONDEUR

- Modèles de protection multicouche
- Sécurisation des réseaux industriels (pare-feux, DMZ, segmentation)
- Gestion des correctifs et des vulnérabilités
- Journalisation et supervision des événements OT

9 / ÉLABORATION D’UNE ARCHITECTURE SÉCURISÉE

- Bonnes pratiques de conception « Secure by Design »
- Sécurisation des automates, SCADA et HMI
- Exemple d’architecture sécurisée conforme à IEC 62443

- Atelier : audit simplifié d’une architecture existante

10 / IEC 62443-2-4 ET LES FOURNISSEURS DE SERVICES IACS

- Exigences pour les intégrateurs et prestataires
- Relations contractuelles et clauses de cybersécurité
- Gestion de la conformité des sous-traitants
- Exemple de grille d’évaluation fournisseur

11 / DÉVELOPPEMENT ET MAINTENANCE DES PRODUITS SÉCURISÉS

- Application de la norme IEC 62443-4-1
- Processus de développement sécurisé
- Vérification, validation et gestion des écarts
- Maintenance, correctifs et mises à jour sécurisées

12 / CONTRÔLE ET SURVEILLANCE DU NIVEAU DE SÉCURITÉ

- Mise en place d’indicateurs de sécurité (KPI)
- Supervision des incidents et gestion des alertes
- Évaluation de la conformité et audit interne
- Outils de suivi et de reporting

13 / ÉVALUATION DU NIVEAU DE SÉCURITÉ ET DE MATURITÉ

- Évaluer les processus et systèmes selon IEC 62443-3-3
- Définir un plan d’amélioration continue
- Méthodes d’auto-évaluation et d’audit croisé
- Atelier : grille d’évaluation de maturité

14 / CERTIFICATION ET DÉMARCHE D’AMÉLIORATION CONTINUE

- Les certifications existantes : produits, systèmes, organisations

- Étapes et prérequis pour la certification IEC 62443
- Retour d’expérience sur des projets certifiés
- Élaboration d’un plan de mise en conformité

15 / MISE EN ŒUVRE D’UNE FEUILLE DE ROUTE CYBERSÉCURITÉ INDUSTRIELLE

- Définir les priorités et jalons de mise en œuvre
- Planifier les ressources et budgets
- Intégrer la culture cybersécurité dans les équipes industrielles
- Atelier final : conception d’un plan d’action opérationnel

Approche pédagogique

- Support Ecrit et Projection
- Exposés Interactifs, Podcasts et Vidéos
- Brainstorming et Jeux de Rôle
- Cas Pratiques et Labs inclus pour leur impact opérationnel
- Test de Validation des Acquis des Connaissances

Prochaines dates programmées

13 au 17 Juil. 2026	Présentiel - Casablanca
07 au 11 Sep. 2026	Distanciel
02 au 06 Nov. 2026	Distanciel

Autres dates possibles sur demande. Contactez-nous pour organiser une session intra-entreprise.

Réservation & Renseignements

Téléphone : +212 522 247 210
Email : contact@innov-systems.com
Web : https//www.innov-systems.com