

# Convergence ITOT dans les Industries Électriques : Architecture Zero Trust et Segmentation

*Lien : https://innov-maroc.com/formation/convergence-itot-dans-les-industries-electriques-architecture-zero-trust-et-segmentation*

DURÉE
**10 jours (70h)**

RÉFÉRENCE
**II39**

CATÉGORIE
**Cybersécurité OT & Sécurité Réseau Industrielle**

INNOV MAROC

## OBJECTIFS DE LA FORMATION

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

- Comprendre les principes de la convergence entre les environnements IT et OT dans les industries électriques.
- Identifier les risques liés à l'interconnexion des systèmes industriels et informatiques.
- Concevoir une architecture réseau conforme au modèle Purdue et aux exigences des infrastructures critiques.
- Maîtriser les principes de l'architecture Zero Trust appliqués aux environnements industriels.
- Mettre en œuvre une segmentation efficace des réseaux OT à l'aide de zones, conduits, VLAN et DMZ industrielles.
- Sécuriser les protocoles de communication industrielle et les échanges entre systèmes IT, OT et Cloud.
- Déployer des mécanismes robustes de gestion des identités, des accès privilégiés et de l'authentification multifacteur.
- Détecter les cybermenaces, superviser les infrastructures industrielles et organiser une réponse efficace aux incidents.
- Garantir la conformité aux normes IEC 62443, IEC 61850, ISO/IEC 27001, ISO/IEC 27019, NIST SP 800-82 et aux exigences réglementaires des infrastructures critiques.
- Intégrer les technologies IIoT, Edge Computing, Smart Grids et Digital Twin dans une architecture sécurisée.
- Réaliser un audit de maturité cybersécurité IT/OT et définir une feuille de route de transformation.
- Développer une stratégie globale de gouvernance de la cybersécurité adaptée aux systèmes électriques industriels.
- Optimiser la résilience, la disponibilité et la sécurité des infrastructures électriques face aux cybermenaces.
- Acquérir les compétences nécessaires pour concevoir, exploiter et maintenir des architectures IT/OT modernes, résilientes et conformes aux meilleures pratiques internationales.

INNOV MAROC

## POUR QUI ?

- Ingénieurs en cybersécurité industrielle
- Ingénieurs en génie électrique
- Ingénieurs réseaux et télécommunications
- Ingénieurs automatisme et contrôle-commande
- Architectes IT/OT
- Responsables SCADA, DCS et EMS
- Responsables cybersécurité (CISO)
- Responsables infrastructures et réseaux industriels
- Responsables exploitation et maintenance des réseaux électriques
- Consultants en cybersécurité industrielle
- Auditeurs des systèmes d'information industriels
- Intégrateurs de systèmes industriels et Smart Grids
- Professionnels des producteurs et transporteurs d'électricité, gestionnaires de réseaux de distribution, industries de procédés, entreprises EPC, bureaux d'études, fabricants d'équipements électriques et sociétés d'ingénierie souhaitant développer une expertise avancée dans la convergence IT/OT, la cybersécurité industrielle et la protection des infrastructures électriques critiques.

INNOV MAROC



## Programme détaillé

### 1 / INTRODUCTION À LA CONVERGENCE IT/OT

- Différences entre les environnements IT et OT
- Enjeux de la convergence numérique
- Cas d'usage dans les industries électriques

### 2 / ARCHITECTURE DES SYSTÈMES INDUSTRIELS

- Architecture des réseaux SCADA, DCS, PLC et EMS
- Niveaux Purdue (Purdue Enterprise Reference Architecture)
- Intégration des systèmes IT et OT

### 3 / PRINCIPES DE L'ARCHITECTURE ZERO TRUST

- Fondamentaux du modèle Zero Trust
- Vérification continue des utilisateurs et équipements
- Principe du moindre privilège (Least Privilege)

### 4 / SEGMENTATION DES RÉSEAUX INDUSTRIELS

- Zones et conduits selon IEC 62443
- VLAN, DMZ industrielle et microsegmentation
- Isolation des systèmes critiques

INNOV MAROC

## 5 / PROTOCOLES DE COMMUNICATION INDUSTRIELLE

- IEC 61850, Modbus TCP, DNP3, OPC UA
- MQTT, PROFINET et Ethernet/IP
- Sécurisation des échanges de données

## 6 / GESTION DES IDENTITÉS ET DES ACCÈS

- IAM, PAM et contrôle des privilèges
- Authentification multifacteur (MFA)
- Gestion sécurisée des accès distants

## 7 / CYBERSÉCURITÉ DES SYSTÈMES OT

- Menaces spécifiques aux environnements industriels
- Analyse des vulnérabilités et gestion des risques
- Détection des intrusions (IDS/IPS) et surveillance OT

## 8 / INTÉGRATION DU CLOUD ET DE L'IIOT

- Architecture hybride IT/OT/Cloud
- Edge Computing et passerelles industrielles
- Sécurisation des objets connectés industriels

## 9 / SUPERVISION ET SOC INDUSTRIEL

- Centre opérationnel de sécurité (SOC)
- SIEM, SOAR et corrélation des événements
- Surveillance continue des infrastructures critiques

## 10 / GESTION DES INCIDENTS ET RÉPONSE AUX CYBERATTAQUES

- Plan de réponse aux incidents
- Continuité d'activité (PCA) et reprise après sinistre (PRA)

INOV MAROC

- Exercices de simulation et retour d'expérience (REX)

## 11 / CONFORMITÉ RÉGLEMENTAIRE ET GOUVERNANCE

- IEC 62443, ISO/IEC 27001, ISO/IEC 27019
- NIST Cybersecurity Framework et NIST SP 800-82
- Directive NIS2 et exigences applicables aux infrastructures critiques

## 12 / DIGITALISATION ET ÉVOLUTION DES RÉSEAUX ÉLECTRIQUES

- Smart Grids et postes électriques numériques
- Jumeaux numériques (Digital Twin)
- Intelligence artificielle appliquée à la cybersécurité

## 13 / AUDIT DE SÉCURITÉ ET ÉVALUATION DE LA MATURITÉ

- Audit d'architecture IT/OT
- Cartographie des actifs critiques
- Élaboration d'une feuille de route de sécurisation

## 14 / ATELIER PRATIQUE : CONCEPTION D'UNE ARCHITECTURE IT/OT SÉCURISÉE

- Conception d'une architecture Zero Trust pour un réseau électrique industriel
- Mise en œuvre d'une segmentation conforme à l'IEC 62443
- Élaboration d'une stratégie intégrant gouvernance, cybersécurité, supervision, gestion des risques, conformité réglementaire et amélioration continue

INNOV MAROC

## Approche pédagogique

- Support Ecrit et Projection
- Exposés Interactifs, Podcasts et Vidéos
- Brainstorming et Jeux de Rôle
- Mises en Situation pour faciliter l'assimilation
- Cas Pratiques et Labs inclus pour leur impact opérationnel
- Test de Validation des Acquis des Connaissances

## Prochaines dates programmées

| | |
|---|---|
| 08 au 19 Fév. 2027 | Présentiel - Casablanca |
| 05 au 16 Avr. 2027 | Présentiel - Casablanca |
| 31 Mai au 11 Juin 2027 | Présentiel - Casablanca |
| 26 Juil. au 06 Août 2027 | Présentiel - Casablanca |
| 20 Sep. au 01 Oct. 2027 | Présentiel - Casablanca |

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

## Réservation & Renseignements

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


INNOV MAROC — Tous droits réservés