

# Sécurité des systèmes de contrôle industriel (ICSSCADA) : cadre IEC 62443

*Lien : https://innov-maroc.com/formation/securite-des-systemes-de-controle-industriel-icsscada-cadre-iec-62443*

| DURÉE | RÉFÉRENCE | CATÉGORIE |
|---|---|---|
| **5 jours (35h)** | **SI119** | **PECB, IEC 62443** |

INNOV MAROC

## 🎯 OBJECTIFS DE LA FORMATION

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

- ✔ Comprendre les architectures ICS/SCADA et leurs vulnérabilités
- ✔ Maîtriser le cadre IEC 62443 et ses exigences
- ✔ Sécuriser les systèmes industriels critiques
- ✔ Mettre en œuvre une segmentation IT/OT efficace
- ✔ Détecter les menaces dans les environnements OT
- ✔ Protéger les PLC et équipements industriels
- ✔ Réduire les risques liés aux infrastructures critiques
- ✔ Déployer des solutions de monitoring OT
- ✔ Assurer la conformité aux normes industrielles
- ✔ Renforcer la résilience des systèmes de contrôle industriel
- ✔ Concevoir des architectures ICS sécurisées
- ✔ Étudier des cas concrets d’attaques et de défense ICS

## 👥 POUR QUI ?

- ✔ Ingénieurs cybersécurité OT/ICS
- ✔ Ingénieurs automatisme industriel
- ✔ Ingénieurs SCADA
- ✔ Architectes sécurité industrielle
- ✔ RSSI / CISO
- ✔ Responsables infrastructures critiques
- ✔ Ingénieurs réseaux industriels
- ✔ Techniciens maintenance industrielle
- ✔ Consultants cybersécurité industrielle
- ✔ Experts en systèmes embarqués industriels
- ✔ SOC analysts spécialisés OT
- ✔ Toute personne impliquée dans la sécurité des systèmes industriels et SCADA

INNOV MAROC



## Programme détaillé

### 1 / Introduction aux systèmes ICS/SCADA

- Définition des environnements industriels critiques
- Rôle des systèmes SCADA, DCS et PLC
- Enjeux de cybersécurité dans les environnements OT

### 2 / Architecture des systèmes industriels

- Segmentation IT/OT
- Composants industriels et flux de communication
- Protocoles industriels (Modbus, OPC UA, DNP3)

### 3 / Menaces et vulnérabilités ICS/SCADA

- Attaques ciblant les infrastructures critiques
- Malware industriel et APT (Stuxnet-like)
- Risques liés aux systèmes legacy

### 4 / Introduction au framework IEC 62443

- Présentation des normes IEC 62443
- Zones et conduits (zones & conduits model)
- Security levels (SL1 à SL4)

INNOV MAROC

### 5 / Gestion des accès et sécurité des actifs industriels

- IAM en environnement OT
- Contrôle des accès aux équipements industriels
- Gestion des comptes privilégiés

### 6 / Sécurisation des réseaux industriels

- Segmentation réseau OT
- Firewalls industriels et DMZ industrielle
- Surveillance du trafic industriel

### 7 / Détection des menaces en environnement OT

- IDS/IPS industriels
- Analyse comportementale des systèmes SCADA
- Détection d’anomalies sur protocoles industriels

### 8 / Sécurité des PLC et équipements embarqués

- Durcissement des automates programmables
- Sécurité du firmware et mises à jour
- Protection contre la reprogrammation malveillante

### 9 / Gouvernance et conformité industrielle

- Application de IEC 62443 en entreprise
- Gestion des risques industriels
- Audits et certification sécurité OT

### 10 / Cas pratiques et architecture sécurisée ICS

- Conception d’une architecture SCADA sécurisée
- Mise en œuvre de la segmentation OT/IT

INOV MAROC

- Retours d’expérience et bonnes pratiques

## 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

| | |
|---|---|
| 01 au 05 Fév. 2027 | Présentiel - Casablanca |
| 29 Mars au 02 Avr. 2027 | Présentiel - Casablanca |
| 24 au 28 Mai 2027 | Présentiel - Casablanca |
| 19 au 23 Juil. 2027 | Présentiel - Casablanca |
| 13 au 17 Sep. 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