



Cybersécurité des Systèmes SCADA & ICS (OT Security) dans l'Industrie Pétrolière, Gazière & Minière

Lien :

<https://afrique-formation.com/formation/cybersecurite-des-systemes-scada-ics-ot-security-dans-l-industrie-petroliere-gaziere-miniere>

 DURÉE
5 jours (35h)

 RÉFÉRENCE
PGM662

 CATÉGORIE
Digitalisation & Intelligence Artificielle

🎯 OBJECTIFS DE LA FORMATION

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

- ✓ Comprendre les architectures SCADA, ICS, DCS et PLC des installations industrielles.
- ✓ Identifier les principales cybermenaces pesant sur les infrastructures critiques.
- ✓ Réaliser une analyse de risques adaptée aux environnements OT.
- ✓ Appliquer les normes internationales de cybersécurité industrielle (IEC 62443, NIST, ISO 27001).
- ✓ Concevoir une architecture réseau OT sécurisée.
- ✓ Mettre en œuvre des dispositifs de contrôle d'accès, de surveillance et de détection des intrusions.
- ✓ Élaborer des plans de réponse aux incidents, de continuité et de reprise d'activité.
- ✓ Sécuriser les environnements IIoT, Cloud industriel et maintenance connectée.
- ✓ Réaliser des audits de cybersécurité des systèmes industriels.
- ✓ Développer une expertise opérationnelle en protection des infrastructures critiques des secteurs pétrolier, gazier et minier.

👥 POUR QUI ?

- ✓ Ingénieurs automatisme et contrôle-commande
- ✓ Ingénieurs SCADA, DCS et ICS
- ✓ Ingénieurs cybersécurité OT/IT
- ✓ Responsables des systèmes industriels
- ✓ Responsables des infrastructures critiques
- ✓ Responsables informatique industrielle
- ✓ Ingénieurs réseaux industriels
- ✓ Responsables HSE et gestion des risques
- ✓ Responsables de la continuité d'activité et de la résilience
- ✓ Chefs de projets en transformation numérique industrielle
- ✓ Toute personne impliquée dans la conception, l'exploitation, la maintenance, la sécurisation ou l'audit des systèmes SCADA, ICS et des réseaux industriels dans les secteurs pétrolier, gazier et minier.



Programme détaillé

1 / FONDAMENTAUX DE LA CYBERSÉCURITÉ INDUSTRIELLE (OT SECURITY)

- Différences entre IT (Information Technology) et OT (Operational Technology)
- Architecture des systèmes SCADA, ICS, DCS et PLC
- Enjeux de cybersécurité dans les industries pétrolière, gazière et minière

2 / ARCHITECTURE DES SYSTÈMES INDUSTRIELS ET CARTOGRAPHIE DES ACTIFS

- Identification des équipements critiques (SCADA, PLC, RTU, HMI, DCS)
- Cartographie des réseaux industriels et des flux de données
- Inventaire des actifs et classification des niveaux de criticité

3 / MENACES, VULNÉRABILITÉS ET ANALYSE DES RISQUES

- Typologie des cyberattaques ciblant les infrastructures industrielles
- Malwares industriels (Stuxnet, Triton, Industroyer, BlackEnergy...)
- Analyse de risques OT et scénarios d'attaque

4 / STANDARDS, NORMES ET CADRES DE RÉFÉRENCE

- IEC 62443, NIST Cybersecurity Framework, NIST SP 800-82
- ISO 27001 appliquée aux environnements industriels
- Recommandations de l'API, ISA et bonnes pratiques sectorielles

5 / SÉCURISATION DES RÉSEAUX INDUSTRIELS

- Segmentation IT/OT et architecture en zones et conduits
- Pare-feux industriels, DMZ, VPN et contrôle des accès
- Sécurisation des protocoles industriels (Modbus, DNP3, OPC, Profinet, Ethernet/IP)

6 / GESTION DES IDENTITÉS, DES ACCÈS ET DES ÉQUIPEMENTS

- Authentification forte et gestion des privilèges (PAM)
- Contrôle des accès distants et des prestataires
- Gestion des correctifs, des configurations et des actifs

7 / DÉTECTION, SURVEILLANCE ET RÉPONSE AUX INCIDENTS

- Supervision de sécurité (SOC OT)
- IDS/IPS industriels, SIEM et surveillance en temps réel
- Élaboration et mise en œuvre d'un plan de réponse aux incidents

8 / RÉSILIENCE, CONTINUITÉ D'ACTIVITÉ ET REPRISE APRÈS INCIDENT

- Sauvegarde et restauration des systèmes industriels
- Plan de continuité d'activité (PCA) et plan de reprise (PRA)
- Exercices de simulation, tests d'intrusion et gestion de crise cyber

9 / DIGITALISATION, IIOT ET NOUVELLES MENACES

- Cybersécurité des objets connectés industriels (IIoT)
- Cloud industriel, Edge Computing et maintenance à distance
- Intelligence artificielle appliquée à la détection des cybermenaces

10 / ATELIER PRATIQUE : AUDIT ET SÉCURISATION D'UNE ARCHITECTURE SCADA/ICS

- Analyse d'une architecture industrielle réelle
- Identification des vulnérabilités et élaboration d'un plan de remédiation

- Mise en place d'une stratégie de défense en profondeur adaptée aux installations pétrolières, gazières et minières

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

Réservation & Renseignements

 **Téléphone** : +212 522 247 210

 **Email** : contact@afrique-formation.com

 **Web** : <https://www.afrique-formation.com>