

# SCADA – Introduction à la sécurité des systèmes industriels

1 jour (7 heures)

Initiation

Présentiel ou classe à distance

à partir de

**885 € HT** par personne (TVA en vigueur) Repas inclus en présentiel

Contenu mis à jour le 25/09/2026. Document téléchargé le 07/10/2026.

## Objectifs

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

- Reconnaître le métier et les problématiques
- Dialoguer avec les automaticiens
- Identifier et décrire les normes et standards de sécurité propres au monde industriel
- Développer une politique de cybersécurité.

Les compétences visées par cette formation font l'objet d'une évaluation.

## À qui s'adresse cette formation ?

Auditeurs, responsables de sécurité, DSI, managers, automaticiens, consultants, architectes réseaux et systèmes ICS/SCADA, administrateurs réseaux et systèmes ICS/SCADA ou toute autre personne en contact avec ces systèmes.

### Prérequis

Avoir de bonnes connaissances générales en informatique.

## Programme

**1** Pendant votre formation

## SCADA – Introduction à la sécurité des systèmes industriels

### Les composants et les architectures des systèmes SCADA

- Les différents composants des systèmes industriels (systèmes de contrôle, bus, boucles de régulation...)
- Les composants hardwares et softwares des systèmes SCADA
- Les RTU (Unités Terminales Distantes)
- Les PLC (Contrôleurs Logiques Programmables)
- Les différents flux de communication entre tous les composants
- Les protocoles de communication temps réel

### Introduction aux systèmes de supervision et de contrôle industriel

- Les attentes des nouveaux systèmes industriels
- La convergence de l'OT et de l'IT
- L'architecture des environnements de supervision et des outils de contrôle
- Les protocoles et flux entre les automates et les systèmes de supervision modernes
- Les quatre générations de SCADA

### Les enjeux de la sécurité des systèmes SCADA

- Quelques chiffres
- Panorama de la cybersécurité
- Les spécificités de la cybersécurité industrielle
- Les profils des attaquants et leurs objectifs
- Les grandes familles d'attaques (spoofing, sniffing, forging...)
- Les référentiels sur la sécurité des systèmes d'information industriels
- Les normes de la sécurité industrielle (IEC 62443, ISO 270xx, IEC 61508 et 61511, NIST 800-82)
- Qu'est-ce que l'ANSSI et quel est son rôle ?
- Les secteurs d'activités cibles, typologies et populations cibles
- Le "Threat modeling" en fonction des générations et équipements des systèmes SCADA

### La sécurité des systèmes SCADA

- L'exposition publique des ICS (Shodan, Censys, Zoomeye...)
- L'exposition des ICS dans les réseaux privés
- Les méthodes de classification
- Les menaces et les vulnérabilités
- Les attaques APT (menaces persistantes avancées)
- Les attaques réelles sur les systèmes SCADA et retours d'expérience
  - Stuxnet, Duqu, Flame et Gauss
  - BlackEnergy
  - APT33
- Les techniques d'authentification et les méthodes de chiffrement :

- Leurs apports
- Leurs mises en place
- Protéger l'ensemble de la chaîne industrielle et les postes opérationnels
- Outils et technologies de sécurité (Firewall, IPS, IDS, SIEM...)
- Sécuriser les accès et les postes à distance (Sans-fil, VPN, 4G...)
- Garantir la disponibilité du réseau
- Gestion de crise et plan de continuité d'activité

#### *Exemples de travaux pratiques (à titre indicatif)*

- *Analyse du risque d'un environnement*
- *Proposition de mise en oeuvre d'équipements de sécurité sur un schéma d'infrastructure industrielle*

## Financement

Plusieurs dispositifs de financement sont accessibles via les OPCO (Opérateurs de Compétences), organismes agréés par le ministère du Travail dont le rôle est d'accompagner, collecter et gérer les contributions des entreprises au titre du financement de la formation professionnelle.

Pour plus d'information, une équipe de gestionnaires SKOLAE Formation spécialisée vous accompagne dans le choix de vos formations et la gestion administrative.

[Nous contacter pour en savoir plus →](#)

## Modalités pédagogiques

Formation délivrée en présentiel ou distanciel\* (blended-learning, e-learning, classe virtuelle, présentiel à distance).

Le formateur alterne entre apports théoriques et démonstrations concrètes.

Variables suivant les formations, les moyens pédagogiques mis en oeuvre sont :

- Ordinateurs Mac ou PC (sauf pour certains cours de l'offre Management), connexion internet fibre, tableau blanc ou paperboard, vidéoprojecteur ou écran tactile interactif (pour le distanciel)
- Environnements de formation installés sur les postes de travail ou en ligne
- Supports de cours

En cas de formation intra sur site externe à M2I, le client s'assure et s'engage également à avoir toutes les ressources matérielles pédagogiques nécessaires (équipements informatiques...) au bon déroulement de l'action de formation visée conformément aux prérequis indiqués dans le programme de formation communiqué.

*\* nous consulter pour la faisabilité en distanciel*

Accessibilité aux personnes en situation de handicap

## Détails de la session

Le 6 novembre 2026 (1 jour / 7 heures)

Nantes

Le 6 novembre 2026

Nantes

- 6 novembre 2026 ..... 9h00 – 17h00