AYI NEDJIMI Consultants

Pentest SCADA/ICS : Sécurité des S

3 mai 2026 • Mis à jour le 17 mai 2026 • 44 min de lecture • 8917 mots •

Les systèmes SCADA (Supervisory Control and Data Acquisition) et ICS (In
dorsale des infrastructures critiques mondiales : centrales électriques, rés
naturel, usines chimiques et lignes de production manufacturière. Pendant

Les systèmes SCADA (*Supervisory Control and Data Acquisition*) et ICS (*Industria*
infrastructures critiques mondiales : centrales électriques, réseaux de distribution
lignes de production manufacturière. Pendant des décennies, ces systèmes ont fo
d'entreprise et d'Internet, ce qui a conduit leurs concepteurs à négliger la sécurité
sûreté fonctionnelle. L'avènement de l'Industrie 4.0, la convergence IT/OT et la nu
ont radicalement changé la donne : aujourd'hui, les automates programmables ind
standardisés, les IHM (Interfaces Homme-Machine) tournent sous Windows, et les
vers des systèmes ERP connectés à Internet. Cette évolution expose des système
adversaires de plus en plus sophistiqués, comme l'ont démontré Stuxnet en 2010,
2015-2016, TRITON/TRISIS ciblant les systèmes de sécurité instrumentée Schneid
frappant Colonial Pipeline en 2021. Ce guide techniq odologie co
protocoles industriels aux outils d'évaluation, en pas églementai

À RETENIR

Points clés : Un pentest ICS ne s'effectue jamais directement en production s
maintenance validée. Les protocoles industriels (Modbus, DNP3, OPC-UA) n'
segmentation réseau selon le modèle Purdue reste la défense fondamentale.
disponibilité (SLA 99,999%), ce qui influence profondément la méthodologie

1. Comprendre l'architecture des systèmes industriels

Avant d'aborder les techniques d'évaluation, il est impératif de maîtriser l'architect
permet d'identifier les vecteurs d'attaque pertinents et d'éviter toute interruption

2. Le modèle Purdue : hiérarchie des niveaux ICS

Le modèle de référence Purdue (Purdue Reference Model), également connu sous
Enterprise Reference Architecture), définit une hiérarchie en cinq niveaux pour les

Niveau 0 — Processus physique : capteurs, actionneurs, vannes, moteurs. C'e

Niveau 1 — Contrôle de base : PLC (Programmable Logic Controllers), RTU (Re
Systems). Ces équipements exécutent la logique de contrôle en temps réel.

Niveau 2 — Supervision : HMI (Human-Machine Interfaces), SCADA servers, in
commandent depuis ce niveau.

Niveau 3 — Opérations de site : historiens de données (OSIsoft PI, AspenTech)
gestion des alarmes.

Niveau 4 — Logistique d'entreprise : ERP (SAP, C e planificat

Réponse sous 24h

Devis gratuit →