Pentest Industriel OT/ICS 2026 : Méthodologie et Outils Spécialisés

Méthodologie pentest OT/ICS 2026 — reconnaissance passive, scanning non-intrusif, tests Modbus/DNP3, outils NMAP ICS, Redpoint, PLCscan et rapport ANSSI.

Le test d'intrusion (pentest) des systèmes industriels OT/ICS (Operational Technology / Industrial Control Systems) est une discipline à la croisée de la cybersécurité offensive et de l'ingénierie industrielle. Contrairement au pentest d'infrastructure IT classique — où les erreurs sont réversibles et les systèmes tolérants aux perturbations — un pentest OT mal conduit peut provoquer des arrêts de production, des dommages physiques sur des équipements de plusieurs millions d'euros, voire mettre en danger des vies humaines si des processus de sécurité physique sont affectés. Cette réalité impose une méthodologie radicalement différente, avec une priorité absolue accordée à la disponibilité des systèmes et à la sécurité physique des opérateurs. En 2026, la demande de pentests OT/ICS s'est fortement accrue, portée par les obligations NIS 2 pour les Opérateurs de Services Essentiels (OSE) et les Opérateurs d'Importance Vitale (OIV) français, ainsi que par les exigences de la norme IEC 62443 qui recommande des évaluations régulières de la sécurité. Ce guide présente la méthodologie complète d'un pentest OT/ICS en 2026 : préparation et coordination avec les équipes opérationnelles, phases de reconnaissance passive et active, outils spécialisés, tests des protocoles industriels, livrables et recommandations, ainsi que le cadre réglementaire français.

À RETENIR

À retenir — Pentest OT/ICS 2026

• La règle absolue du pentest OT : **passivité maximale** — aucune action intrusive sans validation opérateur

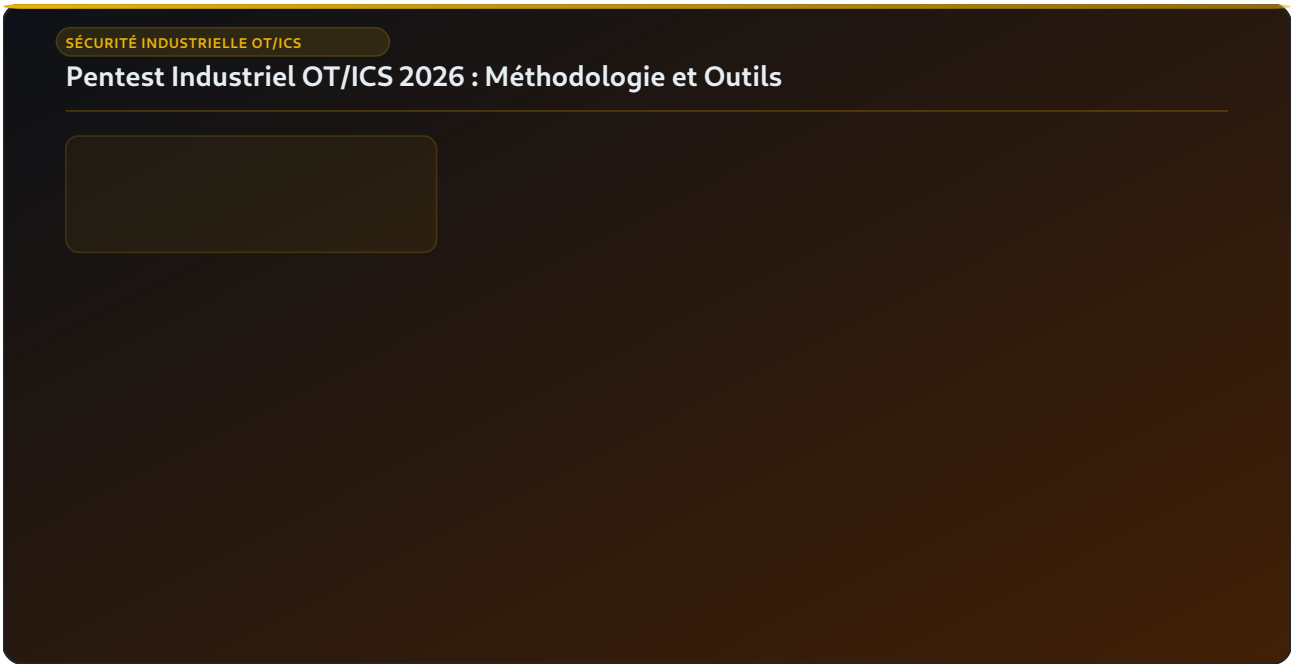
• Phase 1 obligatoire : reconnaissance passive via Wireshark/TAP, jamais de scan actif d'emblée

• Outils clés : **Nmap NSE ICS scripts**, Redpoint, PLCscan, Modbus-cli, DNP3 tools

• IEC 62443-2-4 définit les exigences pour les prestataires de services OT (dont pentest)

• Livrable obligatoire ANSSI : rapport avec classification CVSS adapté OT et plan de remédiation priorisé

• SLA 99.999% des systèmes industriels critiques interdit tout test pouvant provoquer un arrêt



Un pentesteur IT expérimenté qui aborde son premier pentest OT sans préparation spécifique représente un risque opérationnel sérieux. Les différences entre les deux disciplines sont fondamentales. En termes de **priorités** : le pentest IT tolère des indisponibilités temporaires (crash d'un serveur web, redémarrage forcé) car la récupération est rapide ; le pentest OT doit

garantir la continuité de production à tout instant, car un arrêt de processus peut coûter des millions d'euros à l'heure. En termes de **protocoles** : les protocoles IT (HTTP, SSH, SMB) sont robustes aux scans et aux requêtes malformées ; les protocoles OT (Modbus, DNP3, PROFINET) peuvent crasher des automates avec une seule requête mal formée. En termes de **systèmes d'exploitation** : les postes de supervision OT tournent souvent sur Windows XP ou Windows 7 non patchés, embarqués dans des équipements dont le firmware est figé par le fabricant ; la moindre interaction active peut les déstabiliser. En termes de **cycle de vie** : un équipement OT peut rester en production 20-30 ans, accumulant des vulnérabilités jamais corrigées ; le patch management est contraint par les fenêtres de maintenance planifiées. En termes de **conséquences** : une exploitation réussie en OT peut provoquer des dommages physiques, des pollutions environnementales ou des accidents industriels — une responsabilité légale et morale incomparablement supérieure au pentest IT.

Cadre légal et contractuel du pentest OT en France

Avant de démarrer tout pentest OT, le cadre juridique doit être rigoureusement établi. La loi française (article 323-1 du Code pénal) punit sévèrement les accès non autorisés aux systèmes informatiques — un pentest doit impérativement reposer sur une **autorisation écrite explicite** du propriétaire des systèmes testés. Pour les systèmes OT des OIV, les systèmes d'information à protéger au titre de la SAIV (Sécurité des Activités d'Importance Vitale) font l'objet d'une réglementation spécifique — le prestataire de pentest doit être qualifié **PASSI (Prestataire d'Audit de la Sécurité des Systèmes d'Information)** par l'ANSSI pour les prestations sur ces systèmes. Le contrat de pentest doit couvrir : le périmètre précis des systèmes autorisés, les méthodes autorisées et interdites, les plages horaires des tests, la procédure d'arrêt d'urgence en cas d'incident inattendu, la confidentialité des résultats, et la responsabilité en cas de dommage accidentel. La définition contractuelle des **règles d'engagement** (Rules of Engagement, RoE) spécifiques à l'OT est indispensable et ne peut pas être un copier-coller du template IT habituel.

⚡ **Retour terrain**

Pour un groupe industriel agroalimentaire, l'audit OT a révélé que le réseau de supervision des lignes de production était connecté directement au réseau IT bureautique via un switch non managé — 'pour que les ingénieurs puissent accéder depuis leur PC'. La ségrégation via une DMZ industrielle avec des règles de flux explicites a été la première mesure. La seconde : supprimer les 4 accès directs Internet depuis les automates programmables, configurés 'temporairement' il y a 5 ans.

Phase 0 : préparation et coordination avec les équipes opérationnelles

La **phase de préparation** est la plus longue et la plus critique d'un pentest OT. Elle débute idéalement 4 à 6 semaines avant les premiers tests. La première étape est la **constitution du comité de pilotage** réunissant le RSSI, le responsable de production, le responsable maintenance, et le représentant sécurité du fabricant des équipements OT si disponible. Ce comité valide le périmètre, approuve les méthodologies et sera l'interlocuteur lors de chaque phase sensible. La deuxième étape est la **collecte de documentation** : schémas réseau OT, inventaire des équipements avec versions firmware, architecture des zones et conduits, synoptiques de processus. Cette documentation préalable évite les mauvaises surprises pendant les tests et permet de prioriser les zones à fort enjeu de sécurité physique. La troisième étape est la **identification des systèmes hors-scope absolus** : les équipements gérant des sécurités physiques (Safety Instrumented Systems, SIS), des processus irréversibles ou des systèmes avec SLA 99.999% sont typiquement exclus des tests actifs. La quatrième étape est la définition du **protocole d'escalade** : qui appeler, dans quel ordre, si un incident survient pendant les tests.

Phase 1 : reconnaissance passive et cartographie réseau

La **reconnaissance passive** est la phase initiale obligatoire de tout pentest OT sérieux. Elle se conduit exclusivement par écoute du trafic réseau, sans envoi de la moindre sonde active. La mise en place d'un **TAP (Test Access Point)** ou de ports mirror sur les switches des zones OT permet de capturer l'intégralité du trafic sans impact sur les équipements. **Wireshark** avec les dissecteurs de protocoles industriels (modules officiels ou ICS dissectors community) permet de décoder et analyser Modbus, DNP3, IEC 61850, PROFINET, EtherNet/IP, Siemens S7. Une période d'observation de 48 à 72 heures permet de constituer une cartographie complète des communications : quels équipements communiquent entre eux, sur quels protocoles, avec quels codes de fonction, à quelle fréquence. L'analyse de ce trafic révèle souvent des communications inattendues (équipements non documentés, communications inter-zones non autorisées, protocoles non sécurisés exposés) sans aucune interaction active. Des outils comme **Zeek (anciennement Bro)** avec des scripts ICS permettent d'analyser les flux à grande échelle et de générer des rapports automatiques sur les anomalies détectées.

Outils de reconnaissance OT : Nmap NSE ICS, PLCscan et Redpoint

Lorsque les tests actifs sont autorisés (après validation du comité de pilotage), des outils spécialisés permettent d'identifier les équipements OT avec un impact minimal. **Nmap** avec les scripts NSE (Nmap Scripting Engine) spécifiques ICS permet d'interroger les équipements industriels : le script `s7-info.nse` identifie les automates Siemens S7 et lit leurs informations de configuration (numéro de série, versions firmware, modules installés) ; `modbus-discover.nse` énumère les équipements Modbus ; `dnp3-info.nse` lit les informations DNP3. Ces scripts doivent être utilisés avec les options de lenteur maximale (`-T1`) et un seul port à la fois pour minimiser l'impact. **Redpoint**, un ensemble de scripts NSE ICS développé par Digital Bond (maintenant déprécié mais toujours fonctionnel), étend les capacités de découverte à de nombreux protocoles industriels. **PLCscan** est un scanner Python spécialisé pour la découverte d'automates programmables supportant Siemens S7, Modbus et quelques autres protocoles. Ces

outils doivent être utilisés sur des réseaux de test ou avec une autorisation explicite opérateur-par-opérateur pour chaque équipement ciblé.

Tests du protocole Modbus : lecture et écriture contrôlée

Les tests spécifiques au protocole **Modbus** visent à évaluer l'accessibilité non autorisée aux registres des automates. La première étape est la lecture des registres (`Read Holding Registers`, fonction 3) pour cartographier les données accessibles : consignes de process, états d'équipements, mesures de capteurs. Des outils comme **Modbus-cli** (Ruby) ou **pymodbus** (Python) permettent des interactions précises avec le protocole. La deuxième étape, si autorisée par les règles d'engagement, est le test d'écriture sur des registres non-critiques en dehors des heures de production : envoi d'une valeur nulle à un registre de holding non utilisé pour vérifier que l'écriture est possible sans authentification. La troisième étape est le test des **codes de fonction dangereux** : le code 0x08 (Diagnostic) et le code 0x11 (Report Slave ID) peuvent révéler des informations sensibles sur l'équipement. Le code 0x64 et au-delà (fonctions utilisateur) varie selon les fabricants et peut inclure des fonctionnalités d'administration non documentées. Ces tests doivent être conduits avec une extrême précaution, en commençant par la lecture seule et en n'effectuant des tests d'écriture que sur des équipements non-critiques clairement identifiés.

Tests DNP3 : authentification et vulnérabilités spécifiques

Les tests DNP3 évaluent l'absence ou la faiblesse de l'authentification et identifient les vulnérabilités spécifiques au protocole. La première vérification est l'identification de la présence ou non de **DNP3 Secure Authentication** (SA v5) : si absent, toute la communication est non authentifiée et vulnérable aux replay attacks et au spoofing. Des outils comme **Aegis** (Automatak) permettent de conduire des tests DNP3 avancés incluant des fuzzing contrôlés des messages. La vérification de la robustesse aux **messages malformés** consiste à envoyer des

trames DNP3 avec des longueurs incorrectes, des Application Layer Confirmation non sollicitées, ou des Objects mal formatés pour tester la robustesse de l'implémentation. Un équipement mal implémenté peut crasher ou entrer en état indéterminé face à ces entrées — une découverte à documenter immédiatement sans aller plus loin. Les **tunnels DNP3** utilisés pour les communications distantes (SCADA vers sous-stations sur réseaux MPLS ou radio) doivent être vérifiés pour s'assurer qu'ils ne sont pas accessibles depuis des réseaux non autorisés.

Tests réseau : segmentation IT/OT et lateral movement

La vérification de la **segmentation IT/OT** est l'un des tests les plus importants et les plus impactants d'un pentest OT. Les vecteurs de lateral movement IT vers OT les plus courants incluent : les historiens industriels mal configurés (AVEVA PI, Wonderware) exposant des interfaces sur les deux réseaux ; les postes de supervision Windows ayant des interfaces dans les deux réseaux ; les VPN de télémaintenance permettant un accès direct aux équipements OT depuis Internet ; et les partages réseau (SMB) accessibles depuis IT et OT simultanément. La méthodologie consiste à tenter un accès aux ressources OT depuis un poste positionné côté IT (avec autorisation), en utilisant des techniques de pivot et de mouvement latéral standard : scanner les adresses IP OT depuis un poste IT, tenter des connexions sur les ports de protocoles OT (502, 20000, 102), vérifier les règles de pare-feu par des tentatives de connexion sur des ports bloqués. Les faux positifs sont fréquents — une connexion TCP refusée ne signifie pas que le trafic atteint l'équipement OT si un pare-feu l'intercepte en amont. La corrélation avec les logs de pare-feu est indispensable pour distinguer les blocages effectifs des accès réellement ouverts.

Tests d'accès distant : VPN de télémaintenance et RDP

Les **accès distants** aux systèmes OT — VPN de télémaintenance pour les prestataires, RDP vers des postes de supervision, accès via Jump Server — sont historiquement le vecteur d'intrusion le plus exploité dans les incidents OT. Les tests spécifiques à ces vecteurs incluent : la vérification

de l'authentification (MFA obligatoire ou simple password ?), la durée de vie des sessions (expiration automatique ?), le périmètre d'accès autorisé (le prestataire peut-il accéder à des zones au-delà de ses équipements ?), et la journalisation des sessions (enregistrement vidéo des sessions distantes ?). La vérification des **accès prestataires abandonnés** — comptes VPN ou identifiants laissés actifs après la fin d'un contrat — est une découverte fréquente et impactante dans les audits OT. Un retour terrain : lors d'un pentest OT sur un site de traitement d'eau en 2025, nous avons découvert 7 comptes VPN actifs de prestataires n'ayant plus de contrat depuis 12 à 36 mois, dont 3 avec des mots de passe simples (prénom+année). Ces comptes auraient constitué un vecteur d'accès direct aux réseaux SCADA depuis Internet.

Tests des postes de supervision SCADA : OS legacy et applications

Les postes de supervision — interfaces hommes-machines (IHM) et consoles SCADA — sont souvent les équipements OT les plus vulnérables du fait de leur exposition (connectés à Internet pour les mises à jour, équipés de navigateurs web, utilisés par des opérateurs pas toujours sensibilisés à la cybersécurité) et de leur ancienneté (Windows XP, Windows 7 end-of-life). Les tests spécifiques incluent : la vérification des versions OS et des niveaux de patch, l'identification des services réseau exposés (SMBv1, NetBIOS, Remote Registry activés ?), la vérification des comptes locaux et des mots de passe par défaut, l'analyse des applications installées (logiciels non nécessaires, connexions internet non contrôlées), et la vérification des interfaces USB désactivées ou non. L'application d'**exploits MS17-010 (EternalBlue)** ou d'autres vulnérabilités Windows connues est à considérer avec une extrême précaution — uniquement si la règle d'engagement l'autorise explicitement et sur des systèmes redondés, lors d'une fenêtre de maintenance. La vérification de la résistance au phishing (envoi d'un email de test à un opérateur) peut être incluse dans le scope avec l'accord de la direction.

IEC 62443 et pentests OT : exigences de la norme

La norme **IEC 62443**, cadre international de référence pour la cybersécurité industrielle, traite des évaluations de sécurité dans plusieurs de ses parties. IEC 62443-2-4 définit les exigences pour les prestataires de services de systèmes de contrôle industriel (dont les prestataires de pentest). IEC 62443-3-2 définit l'évaluation des risques de sécurité et la détermination des niveaux de sécurité (SL). IEC 62443-3-3 définit les exigences systèmes pour les différents niveaux de sécurité (SL1 à SL4), incluant les capacités de détection et de réponse aux intrusions. Dans le contexte d'un pentest OT, la norme IEC 62443 est utilisée à deux niveaux : comme référentiel de classification des vulnérabilités découvertes (en quels niveaux SL chaque vulnérabilité impacte-t-elle ?) et comme cadre de recommandations de remédiation (quelle mesure IEC 62443 permet de remédier à chaque vulnérabilité ?). Les **OIV et OSE français** soumis à NIS 2 sont encouragés par l'ANSSI à conduire des évaluations de sécurité IEC 62443 dans le cadre de leur gestion des risques cyber, créant un marché croissant pour les prestataires PASSI qualifiés OT.

Outils de fuzzing OT : tester la robustesse des implémentations

Le **fuzzing** — envoi de données aléatoires ou semi-structurées à un protocole pour identifier des comportements anormaux — est une technique de test puissante mais particulièrement risquée en OT. Un équipement industriel qui crashe sous fuzzing peut nécessiter une intervention physique (redémarrage par coupure de courant) et perturber le processus de production. Le fuzzing OT ne doit être conduit que dans des conditions très contrôlées : sur un environnement de test physiquement isolé, avec des équipements redondants, hors heures de production, et avec des opérateurs présents physiquement. Des outils de fuzzing OT incluent **Boofuzz** (successeur de Sulley, généraliste mais extensible aux protocoles industriels), **Aegis** (Automatak, spécialisé DNP3), et des fuzzers propriétaires développés par des équipes de recherche (Claroty Team82, Nozomi Networks Research). Les résultats de fuzzing les plus précieux sont les **crashs reproductibles** : ils confirment une vulnérabilité réelle et permettent d'en évaluer l'exploitabilité. Un fuzzing DNP3 conduit en 2025 sur un IED électrique a découvert une vulnérabilité de déni de

service permettant de bloquer l'équipement avec un seul paquet malformé — une découverte critique pour les réseaux de distribution électrique.

Rapport de pentest OT : format et contenu attendus

Le **rapport de pentest OT** diffère significativement du rapport de pentest IT standard dans sa structure et son contenu. Le résumé exécutif doit s'adresser simultanément au RSSI et au directeur industriel — deux audiences avec des préoccupations différentes. Pour le RSSI : les risques cyber et les recommandations de sécurité. Pour le directeur industriel : les risques de disponibilité et les impacts potentiels sur la production. Chaque vulnérabilité doit être documentée avec un **score CVSS adapté OT** (intégrant la dimension disponibilité avec un poids plus élevé qu'en IT) et une évaluation de l'impact opérationnel (arrêt de production potentiel, dommages physiques, risques de sécurité physique). Les recommandations doivent être classées en trois catégories : mesures immédiates (sans impact production, déployables dans les jours suivants), mesures à planifier en fenêtre de maintenance (nécessitant un arrêt ou une intervention sur équipements), et recommandations architecturales (projets moyen terme). Le plan de remédiation proposé doit être réaliste vis-à-vis des contraintes industrielles — une recommandation de mise à jour immédiate de firmware sur un automate gérant un processus continu n'est pas opérationnelle.

Livrables additionnels : cartographie OT et schémas réseau

En plus du rapport de vulnérabilités, un pentest OT produit typiquement plusieurs livrables complémentaires à forte valeur ajoutée. La **cartographie réseau OT découverte** — souvent plus complète que la documentation existante — liste tous les équipements identifiés avec leurs adresses IP, versions firmware et protocoles actifs. Cette cartographie peut révéler des équipements "fantômes" non référencés dans l'inventaire officiel. Le **schéma des flux de communication** (qui parle à qui, sur quel protocole, dans quel sens) permet de visualiser les

dépendances et d'identifier les communications non conformes aux politiques de sécurité. L'analyse des **protocoles non attendus** (Telnet sur un équipement supposément désactivé, SNMP v1 sur un switch industriel récent) complète le tableau de la surface d'attaque réelle. Enfin, une **roadmap de remédiation priorisée**, tenant compte des contraintes de fenêtres de maintenance et des budgets industriels, transforme les découvertes techniques en plan d'action opérationnel pour les équipes OT et IT.

Environnements de test et jumeaux numériques

Certaines organisations industrielles disposent d'**environnements de test** — répliques physiques ou virtuelles de leurs systèmes de production — permettant des tests plus poussés sans risque de perturbation. Ces environnements, quand ils existent, sont la voie royale pour le pentest OT avancé (fuzzing, exploitation de vulnérabilités, tests d'impact). Les **jumeaux numériques** (digital twins) — simulations logicielles des systèmes OT — émergent comme une alternative pour les tests de cybersécurité, permettant de simuler des attaques sans risque physique. Des plateformes comme **GE Predix Digital Twin**, **Siemens Digital Industries Simulation** ou des environnements open source (GNS3 avec émulation d'automates) permettent des tests avancés. Cependant, un jumeau numérique n'est jamais une copie parfaite du système physique — les comportements sous attaque peuvent différer significativement. Les découvertes sur jumeau numérique doivent être validées prudemment sur le système réel avant d'en tirer des conclusions définitives.

Prestataires PASSI qualifiés OT : comment choisir ?

La qualification **PASSI (Prestataire d'Audit de la Sécurité des Systèmes d'Information)** de l'ANSSI est la référence pour choisir un prestataire de pentest sérieux en France. En 2026, une vingtaine de prestataires PASSI sont qualifiés, dont plusieurs ont développé une spécialisation OT/ICS. Au-delà de la qualification PASSI, les critères de sélection spécifiques OT incluent :

l'expérience documentée sur des projets OT dans le même secteur (énergie, eau, industrie manufacturière, transport), la disponibilité d'équipements OT en laboratoire pour tester les outils sans risque, la formation des pentesteurs aux normes IEC 62443 et aux contraintes opérationnelles industrielles, et la capacité à coordonner avec les équipes d'exploitation industrielle. Une bonne pratique : demander des références clients et contacter directement les responsables OT de ces références pour évaluer la qualité de la coordination opérationnelle lors des tests — c'est souvent là que se joue la réussite d'un pentest OT, bien plus que dans la sophistication technique.

Coordination avec les opérateurs SCADA : protocoles de test en temps réel

La **coordination en temps réel avec les opérateurs SCADA** pendant les phases de tests actifs est une exigence non négociable du pentest OT professionnel. Un opérateur doit être présent physiquement à la console SCADA pendant tous les tests actifs ciblant des équipements OT, avec la capacité d'intervenir immédiatement si un comportement anormal est observé sur les processus. Le protocole de coordination typique inclut : un canal de communication direct entre l'équipe de pentest et l'opérateur (radio ou téléphone dédié, pas de messagerie internet potentiellement indisponible) ; un signal d'arrêt immédiat convenu — si l'opérateur envoie un signal "STOP", toute activité de test cesse instantanément sans discussion ; une procédure de log des actions de test avec horodatage pour corréler avec les événements observés sur le SCADA ; et un seuil d'alerte défini — si un paramètre de process dépasse X% de sa valeur normale pendant les tests, arrêt automatique. Cette coordination étroite transforme le pentest OT en un exercice collaboratif entre équipe sécurité et équipe opérationnelle, renforçant mutuellement leur compréhension des risques et des contraintes. Les meilleures missions de pentest OT que j'ai observées étaient celles où les opérateurs SCADA participaient activement à l'identification des comportements suspects — leur connaissance du "comportement normal" du système étant un outil de détection irremplaçable.

Malwares ICS : Triton, Industroyer 2 et leurs signatures

La compréhension des malwares ICS documentés est indispensable pour un pentesteur OT souhaitant simuler des scénarios d'attaque réalistes. **Stuxnet** (2010) reste la référence fondatrice : premier malware connu ciblant des équipements physiques (centrifugeuses d'enrichissement d'uranium iraniennes), exploitant des vulnérabilités Windows et des codes de commande Siemens S7-315 spécifiques. **Industroyer/CRASHOVERRIDE** (2016, Ukraine) ciblait les sous-stations électriques avec des modules spécialisés IEC 61850, IEC 104 et DNP3 — la première démonstration d'un malware avec des capacités de communication native sur des protocoles OT industriels. **Triton/TRISIS** (2017, pétrochimie Arabie Saoudite) a ciblé spécifiquement les SIS Schneider Electric Triconex, tentant de désactiver les sécurités physiques — un franchissement de ligne rarement vu, ciblant délibérément la barrière de sécurité physique ultime. **Industroyer 2** (2022, Ukraine) a démontré la capacité des attaquants à réutiliser et améliorer des techniques d'attaque IEC 61850 cinq ans après la première version. La connaissance de ces TTPs documentées — disponibles dans la base MITRE ATT&CK for ICS — permet aux pentesteurs OT de concevoir des scénarios d'attaque réalistes et de vérifier que les détections en place (règles SIEM, alertes Claroty/Nozomi) auraient détecté ces comportements. La simulation de la phase de discovery et de reconnaissance interne d'Industroyer 2 — sans exécution des charges malveillantes — est un exercice de red team OT particulièrement instructif.

Safety Instrumented Systems (SIS) : périmètre hors-scope absolu

Les **Safety Instrumented Systems (SIS)** — systèmes instrumentés de sécurité — sont les gardiens de la sécurité physique dans les environnements industriels dangereux. Ils surveillent les paramètres de processus critiques (température, pression, niveau) et déclenchent des actions d'arrêt d'urgence (Emergency Shutdown, ESD) si des limites de sécurité sont franchies. Les SIS sont soumis à des normes de fonctionnement sûr (IEC 61511, IEC 61508) avec des niveaux d'intégrité de sécurité (SIL) certifiés. Dans un pentest OT, les SIS sont **absolument hors-scope** pour tout test actif. Toute interaction, même passive (capture de trafic sur le réseau SIS), doit être

validée explicitement par l'ingénieur de sécurité fonctionnelle du site. La raison est simple : les SIS sont la dernière barrière entre un processus défaillant et un accident industriel majeur. Une interférence avec leur fonctionnement — même involontaire — peut désactiver cette barrière critique et créer un risque pour la sécurité des personnes. L'identification des SIS et leur exclusion formelle du périmètre de pentest doit être documentée dans les règles d'engagement, avec la liste des équipements SIS et leurs adresses réseau (si connectés en réseau, ce qui devrait être limité au maximum). La découverte d'une connexion réseau non documentée entre le réseau OT et le réseau SIS est en elle-même une finding critique à signaler immédiatement.

Rapport préliminaire et communication en cours de mission

La communication en cours de pentest OT est plus critique que dans le monde IT, du fait des risques opérationnels potentiels. Un **rapport préliminaire quotidien** — même sous forme d'un email ou d'un message sur un canal sécurisé — informant le comité de pilotage des activités du jour et des anomalies observées est une pratique recommandée. Si une découverte critique est faite — accès non authentifié à un équipement critique, connexion Internet directe vers le réseau OT, SIS connecté au réseau de supervision — elle doit être **signalée immédiatement** (en dehors du calendrier de rapport normal) pour permettre des mesures correctives immédiates. Cette communication en temps réel est d'autant plus importante que certaines vulnérabilités OT peuvent déjà être exploitées par des attaquants extérieurs — la découverte d'un Modbus TCP accessible depuis Internet n'est pas anodine et peut requérir une intervention de blocage dans l'heure. La gestion de la communication entre l'équipe de pentest, les équipes OT et les équipes IT (souvent des silos organisationnels distincts) est un facteur clé de succès du pentest OT que les prestataires expérimentés maîtrisent.

Threat modeling OT : STRIDE et ICS-specific frameworks

Avant de conduire un pentest OT, la réalisation d'un **threat modeling** spécifique aux systèmes industriels permet de prioriser les scénarios d'attaque les plus pertinents et d'orienter les tests vers les vecteurs à fort impact. Des frameworks adaptés aux environnements OT complètent l'approche STRIDE classique (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege). L'**ATT&CK for ICS** de MITRE est la référence en 2026 pour la modélisation des menaces OT : il catalogue les tactiques, techniques et procédures (TTPs) observées dans des attaques réelles sur des systèmes industriels (Stuxnet, Triton, Industroyer 2), organisées selon une kill chain ICS spécifique (Initial Access, Execution, Persistence, Privilege Escalation, Evasion, Discovery, Lateral Movement, Collection, Command and Control, Inhibit Response Function, Impair Process Control, Impact). L'utilisation d'ATT&CK for ICS dans le threat modeling permet d'identifier les TTPs les plus probables pour le secteur ciblé et d'orienter les tests de manière threat-driven plutôt que compliance-driven. Pour un site de distribution d'eau, les techniques d'Inhibit Response Function (désactivation des alarmes de sécurité physique) et d'Impair Process Control (modification des setpoints chimiques) seront priorisées. Pour une centrale électrique, les techniques ciblant les relais de protection IEC 61850 seront au premier plan.

Tests d'ingénierie sociale ciblés OT : le vecteur humain

Le vecteur d'accès initial le plus courant dans les incidents OT documentés n'est pas l'exploitation directe d'une vulnérabilité protocolaire, mais le **phishing ou l'ingénierie sociale** ciblant des employés ayant accès aux systèmes OT. Les tests d'ingénierie sociale dans le scope d'un pentest OT peuvent cibler plusieurs profils. Les **techniciens de maintenance** : envoi d'un email imitant un fournisseur d'équipements (Siemens, Schneider) avec une "mise à jour critique de firmware" malveillante ou une demande de connexion à une "plateforme de support" piégée. Les **opérateurs SCADA** : phishing imitant des notifications systèmes internes, demandant une connexion au portail de supervision. Les **responsables informatiques industriels** : usurpation d'une direction ou d'un prestataire pour obtenir des accès VPN ou des informations de

configuration. Si autorisés, ces tests révèlent souvent une vulnérabilité humaine significative — des opérateurs OT non sensibilisés au phishing car les formations sécurité se concentrent sur les équipes IT. Un test de phishing conduit lors d'un pentest OT d'une entreprise de transport en commun français en 2025 a obtenu les credentials d'un technicien SCADA avec un taux de clic de 40% sur un email imitant une notification de mise à jour de l'application de supervision — un résultat alarmant qui a conduit à l'implémentation d'un programme de sensibilisation spécifique OT.

Tests des interfaces HMI et SCADA web : vecteurs applicatifs

Les interfaces opérateurs SCADA modernes intègrent de plus en plus souvent des composants web — dashboards HTML5, APIs REST pour l'intégration IT/OT, portails de supervision à distance. Ces composants introduisent des vecteurs d'attaque applicatifs classiques du monde IT dans l'environnement OT. Les tests spécifiques aux interfaces HMI/SCADA web incluent : la vérification des versions des frameworks web utilisés (Ignition, iFIX, WinCC Web Navigator) pour l'identification de vulnérabilités connues ; le test des mécanismes d'authentification (politique de mots de passe, absence de MFA, sessions sans expiration) ; la recherche de vulnérabilités web standard — injection SQL dans les formulaires de recherche d'historique, XSS dans les champs de configuration, IDOR dans les APIs de lecture de données de process ; et la vérification des en-têtes HTTP de sécurité (CSP, HSTS, X-Frame-Options). Une découverte classique dans les audits OT : les portails web SCADA exposés sur Internet (pour la supervision à distance des dirigeants ou des astreintes) avec une authentification par simple password sans MFA, voire avec les credentials par défaut du logiciel. Ces vulnérabilités applicatives SCADA sont souvent plus exploitables que les vulnérabilités protocolaires OT car elles ne nécessitent pas d'accès réseau au segment OT proprement dit — un accès à l'interface web suffit. Des outils standard de pentest web (Burp Suite, OWASP ZAP) peuvent être utilisés sur ces interfaces avec les précautions habituelles (éviter le scanning intrusif, pas de SQLi en mode automatique sur des bases de données de production).

Gestion des clés et certificats dans les environnements OT

La **gestion des clés cryptographiques et des certificats** dans les environnements OT est un vecteur de vulnérabilité souvent négligé. Les problèmes les plus courants identifiés lors des pentests OT incluent : les certificats auto-signés acceptés sans vérification dans les configurations SCADA (permettant des attaques Man-in-the-Middle sur les communications chiffrées) ; les clés SSH ou certificats X.509 partagés entre plusieurs équipements (compromission d'un équipement = compromission de tous) ; les clés hardcodées dans les configurations d'équipements (extractibles avec un accès physique ou via backup) ; et l'absence de processus de rotation des clés (des clés jamais changées depuis la mise en service, parfois il y a 10-15 ans). Dans les systèmes DNP3 SA v5, les Update Keys utilisées pour les sessions d'authentification doivent être rotées périodiquement — une exigence souvent non respectée. La vérification de ces éléments durant un pentest OT passe par l'examen des configurations sauvegardées, l'analyse des exchanges SSL/TLS capturés durant la phase passive, et des questions directes aux équipes OT sur leurs procédures de gestion des clés. Les découvertes dans ce domaine génèrent souvent des recommandations à fort impact sécurité mais à faible coût de remédiation.

Tests de sécurité physique : accès non autorisés aux équipements

La **sécurité physique** des équipements OT est une composante indissociable d'un audit de sécurité industriel complet. Des tests de sécurité physique dans le scope d'un pentest OT peuvent inclure : la vérification des verrous des armoires électriques contenant les automates (combinaisons standards Siemens, ABB, Schneider facilement trouvables en ligne) ; la présence ou non de ports USB accessibles sur les automates et les postes de supervision ; la facilité d'accès physique aux racks réseau du LAN OT (switches industriels souvent non sécurisés physiquement dans les ateliers) ; et la possibilité de connecter un équipement non autorisé directement sur un port réseau OT disponible. Un acteur malveillant ayant accès physique à un automate Siemens S7-300 non sécurisé peut extraire la totalité du projet automate (code ladder, configurations, communications) avec Siemens SIMATIC Manager ou TIA Portal en quelques minutes. La

sécurité physique des équipements OT doit être intégrée dans la politique de sécurité globale et dans les évaluations régulières — une lacune souvent révélée lors des premiers pentests OT d'une organisation.

Intégration du pentest OT dans le programme de sécurité global

Un pentest OT ponctuel, même parfaitement conduit, n'a de valeur durable que s'il s'inscrit dans un **programme de sécurité OT continu**. La remédiation des vulnérabilités découvertes doit être suivie avec les mêmes outils de gestion que les vulnérabilités IT : un tableau de bord de remédiation avec propriétaires, délais et statuts de correction. Les vulnérabilités qui ne peuvent pas être corrigées immédiatement (équipements obsolètes, contraintes de production) doivent faire l'objet d'un **plan de traitement du risque** formalisé, avec des mesures compensatoires documentées. Un pentest de revérification (retest) après remédiation confirme que les corrections ont bien été appliquées. La **cadence des pentests OT** recommandée dépend de la criticité des systèmes : annuelle pour les systèmes OT critiques (OIV), bisannuelle pour les systèmes importants (OSE), et à chaque modification majeure de l'architecture OT (ajout d'une interface IT/OT, déploiement d'un nouveau SCADA). L'intégration des résultats de pentest OT dans le bilan annuel de sécurité présenté au comité de direction est une pratique de gouvernance saine qui permet d'allouer les budgets de remédiation avec une priorisation basée sur les risques réels.

Coûts d'un pentest OT/ICS : facteurs de dimensionnement

Le **coût d'un pentest OT/ICS** est significativement supérieur à un pentest IT équivalent, pour plusieurs raisons. La durée est plus longue (3-6 semaines vs 1-2 semaines pour un pentest IT équivalent). L'expertise OT requise est rare et plus coûteuse que l'expertise IT — un pentesteur senior spécialisé OT facture typiquement 1 200 à 1 800 €/jour HT en France en 2026. Les déplacements sur site sont obligatoires pour les phases critiques, ajoutant des coûts de transport et d'hébergement. La nécessité de prestataires qualifiés PASSI restreint la concurrence et

maintient les prix à des niveaux élevés. En pratique, un pentest OT sur un site industriel de taille intermédiaire (quelques dizaines d'équipements OT) coûte entre 40 000 et 100 000 euros HT selon le périmètre et la complexité. Pour les OIV avec des systèmes OT très étendus, des projets de 150 000 à 300 000 euros ne sont pas rares. Ces coûts doivent être mis en perspective avec le coût d'un incident OT majeur (arrêt de production, dommages physiques, sanctions réglementaires) qui peut atteindre plusieurs millions d'euros. Le ROI d'un pentest OT bien conduit et suivi de remédiation est généralement très positif sur un horizon de 3 à 5 ans.

FAQ — Pentest Industriel OT/ICS 2026

Combien de temps dure un pentest OT/ICS complet ?

Un pentest OT/ICS complet sur un site industriel de taille intermédiaire dure typiquement 3 à 6 semaines : 1 à 2 semaines de préparation et collecte de documentation, 1 à 2 semaines de reconnaissance passive (TAP, capture trafic, analyse), 3 à 5 jours de tests actifs limités (si autorisés), et 1 à 2 semaines de rédaction du rapport et de restitution. Ce calendrier est beaucoup plus long qu'un pentest IT équivalent, reflétant la nécessité de préparation approfondie et de coordination avec les équipes opérationnelles. Les tests actifs sont souvent planifiés lors de fenêtres de maintenance existantes (weekend, arrêt annuel).

Un pentest OT peut-il être conduit à distance ou faut-il une présence physique ?

La phase de reconnaissance passive nécessite une présence physique pour l'installation des TAP ou des ports mirror sur le réseau OT — ou l'accès à un système de monitoring existant (Claroty, Nozomi) qui peut fournir les captures. Les tests actifs sur les équipements OT nécessitent idéalement la présence d'un opérateur sur site prêt à intervenir physiquement en cas d'incident — une contrainte de sécurité incontournable. Certaines parties du pentest peuvent être conduites à distance (analyse des captures, tests sur des composants IT de la chaîne OT), mais les tests sur les équipements OT critiques requièrent une présence physique coordonnée.

NIS 2 impose-t-il des pentests OT réguliers pour les OSE ?

NIS 2 n'impose pas explicitement de pentests mais exige des mesures de gestion des risques cyber incluant des "tests et des audits de sécurité réguliers". La transposition française (décret d'application 2025) précise que les Entités Essentielles doivent conduire des évaluations de sécurité régulières, dont la fréquence et le périmètre doivent être proportionnels aux risques. Pour les systèmes OT des OSE dans les secteurs énergie, eau et transport, une évaluation annuelle ou biannuelle incluant des tests de pénétration est considérée comme une bonne pratique par l'ANSSI. Les résultats de ces évaluations peuvent être demandés par l'ANSSI dans le cadre de contrôles de conformité NIS 2.

Quelles certifications doit avoir un pentesteur OT ?

En 2026, les certifications pertinentes pour le pentest OT combinent des certifications cyber générales et des certifications OT spécifiques. Côté cyber : OSCP (Offensive Security Certified Professional), CEH (Certified Ethical Hacker), GPEN (GIAC Penetration Tester). Côté OT/ICS : GICSP (Global Industrial Cyber Security Professional, GIAC), GRID (GIAC Response and Industrial Defense), CSSA (Certified SCADA Security Architect). La certification constructeur — Siemens Certified OT Security Specialist, Rockwell Automation OT Security — est également valorisée. L'expérience pratique sur des équipements réels (automates, IED, SCADA) prime sur les certifications seules dans ce domaine où la connaissance opérationnelle des systèmes industriels est indispensable.

Phase	Durée	Outils principaux	Impact production
Phase 0 — Préparation	1-2 semaines	Documentation, réunions	Zéro
Phase 1 — Passive Recon	1-2 semaines	Wireshark, TAP, Zeek	Zéro
Phase 2 — Active Recon	2-3 jours	Nmap T1, PLCscan	Faible (hors production)
Phase 3 — Tests protocoles	2-3 jours	Modbus-cli, DNP3 tools	Modéré (avec opérateur)
Phase 4 — Tests réseau	1-2 jours	Pivot, lateral movement	Faible (réseau IT)
Phase 5 — Rapport	1-2 semaines	Documentation, restitution	Zéro

Pour approfondir, consultez notre guide sur les protocoles OT et leur sécurité, notre article sur la sécurité des passerelles ICS, notre comparatif outils SOC open source pour OT, et notre page méthodologie de pentest Active Directory pour les composantes IT du périmètre. Les ressources de l'ANSSI (publications ICS) et du CISA ICS constituent les références techniques incontournables pour les équipes conduisant ou commanditant des pentests OT en France.

© Ayi NEDJIMI Consultants — Tous droits réservés