Sécurité OT/ICS SCADA 2026 : Guide Pentest et Protocoles Industriels

Sécurité OT/ICS SCADA 2026 : protocoles Modbus/DNP3/OPC UA, pentest industriel IEC 62443, segmentation Purdue, NIS2 OIV et outils Claroty/Dragos/Nozomi.

La sécurité des systèmes industriels — **OT (Operational Technology)**, **ICS (Industrial Control Systems)**, **SCADA (Supervisory Control and Data Acquisition)** — représente en 2026 l'un des enjeux les plus critiques de la cybersécurité française. Avec plus de 60 incidents cyber signalés à l'ANSSI en 2025 ciblant des infrastructures industrielles critiques (énergie, eau, transport, pétrochimie), et la convergence croissante des réseaux IT et OT qui expose des systèmes autrefois isolés à des menaces cyber sophistiquées, les équipes de sécurité industrielle font face à des défis sans précédent. Ce guide technique complet couvre les spécificités des protocoles industriels (Modbus TCP, DNP3, OPC UA, IEC 61850, Profinet), les méthodologies de pentest OT adaptées (approche passive, analyse de protocoles, tests sur équipements similaires), la cartographie des risques cyber-physiques (impacts sur la sécurité des travailleurs, l'environnement et la continuité de service), l'application de l'IEC 62443 comme référentiel de sécurité industrielle, les nouvelles obligations NIS2 pour les Opérateurs d'Importance Vitale (OIV) et Opérateurs de Services Essentiels (OSE) du secteur industriel, les architectures de segmentation OT/IT sécurisées (zones Purdue, DMZ industrielle, data diode), et les outils spécialisés pour l'analyse et le pentest des environnements OT/SCADA (Nmap ICS scripts, Shodan industrial, Claroty, Dragos, Nozomi Networks).

Convergence IT/OT : nouvelles surfaces d'attaque en 2026

La convergence des réseaux informatiques traditionnels (IT) et des systèmes opérationnels industriels (OT) est le phénomène qui a le plus transformé le paysage de la sécurité industrielle au cours de la dernière décennie. Cette convergence, motivée par des gains de productivité et la maintenance prédictive, expose désormais des systèmes de contrôle industriel conçus sans prise en compte de la cybersécurité à des menaces cyber sophistiquées.

Les vecteurs d'attaque exploitant la convergence IT/OT incluent : les interfaces HMI (Human-Machine Interface) connectées à Internet pour la supervision à distance, les réseaux de maintenance VPN permettant aux fournisseurs d'équipements d'accéder aux systèmes de contrôle, les équipements OT utilisant des systèmes d'exploitation Windows non patchés (Windows XP, Windows 7) encore très présents dans les environnements industriels, et les connexions entre les ERP (SAP, Oracle) et les systèmes MES (Manufacturing Execution System) qui créent des passerelles entre les réseaux IT et OT.

À RETENIR

À retenir : Contrairement aux systèmes IT où la disponibilité cible est de 99,9%, les systèmes industriels critiques (centrale nucléaire, réseau électrique, usine pétrochimique) ont des contraintes de disponibilité de 99,999% (5 minutes d'arrêt par an maximum). Un test de pénétration OT mal conduit peut provoquer un arrêt de production de plusieurs jours ou mettre en danger des vies humaines. Les tests de pénétration OT doivent impérativement suivre un protocole de sécurité strict et être réalisés par des experts certifiés.

Protocoles industriels : Modbus TCP, DNP3, OPC UA, IEC 61850

Les protocoles de communication industriels présentent des caractéristiques fondamentalement différentes des protocoles réseau IT en termes de sécurité. La plupart ont été conçus dans les années 1970-1990 pour des réseaux isolés, sans mécanismes d'authentification ni de chiffrement.

⚡ **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.

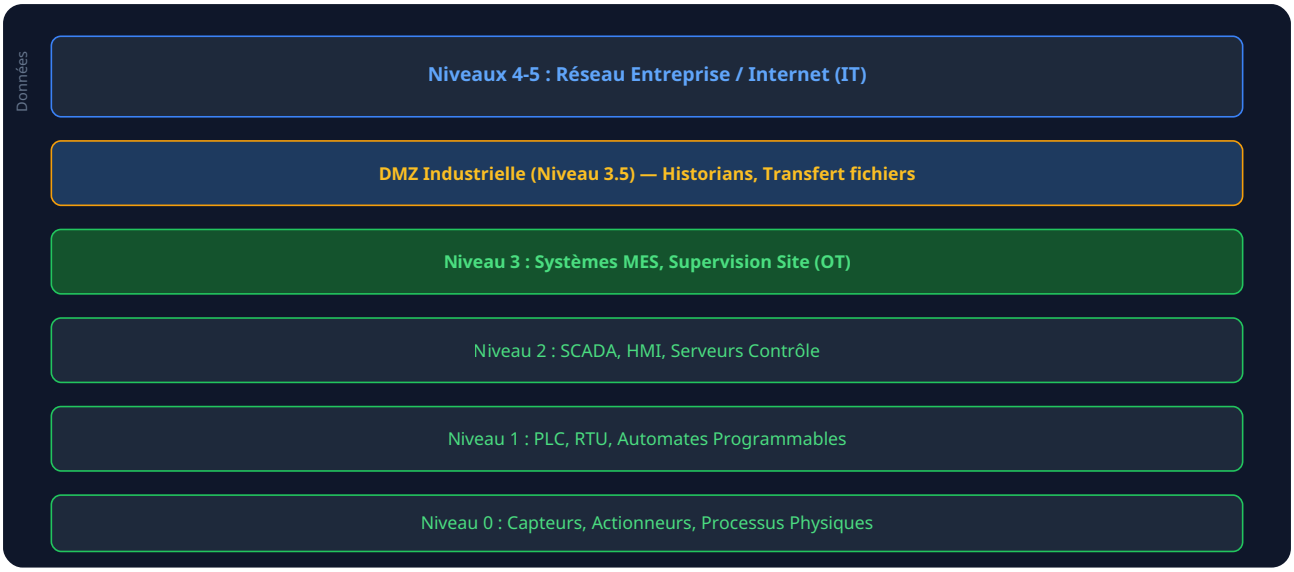
Protocole	Domaine	Port standard	Vulnérabilités principales
Modbus TCP	Automates (PLC), capteurs	502/TCP	Pas d'authentification, pas de chiffrement, commandes directes aux équipements
DNP3	Énergie, eau, transport	20000/TCP	Authentification optionnelle et souvent désactivée, spoofing possible
OPC UA	Industrie 4.0, IIoT	4840/TCP	Mauvaises configurations TLS, certificats auto-signés, Anonymous mode activé
IEC 61850	Protection réseau électrique	102/TCP (MMS)	Absence de chiffrement natif, exposition des GOOSE messages
Profinet	Automatisation industrielle	Multi-protocoles	Découverte passive (DCP), pas d'authentification
EtherNet/IP	Automatisation Allen-Bradley	44818/TCP	Commandes non authentifiées, messages broadcast exploitables

Modèle Purdue : architecture de référence pour la segmentation OT/IT

Le modèle **Purdue Enterprise Reference Architecture (PERA)**, développé dans les années 1990 et mis à jour pour les environnements IIoT, reste la référence pour la segmentation des réseaux OT/IT en niveaux (Levels 0 à 5) avec contrôles stricts des flux entre niveaux.

La sécurité du modèle Purdue repose sur la définition de zones avec des niveaux de confiance décroissants depuis le niveau 0 (processus physiques, capteurs, actionneurs) jusqu'au niveau 5 (réseau d'entreprise, Internet). Les flux entre zones doivent transiter par des équipements de sécurité (firewalls industriels, data diodes, DMZ) filtrant strictement les communications autorisées.

La *DMZ industrielle* (généralement aux niveaux 3.5-4) est la zone tampon entre les réseaux OT (niveaux 0-3) et les réseaux IT (niveaux 4-5). Elle héberge les serveurs de données historiques (historians), les serveurs de fichiers de transfert, et les serveurs de maintenance. Tous les flux entre OT et IT doivent obligatoirement transiter par la DMZ industrielle, jamais directement entre les deux réseaux.



Pentest OT/ICS : méthodologie adaptée aux environnements industriels

Le test de pénétration d'un environnement OT/ICS est fondamentalement différent d'un pentest IT classique. La priorité absolue est la **continuité des opérations industrielles** : aucune action ne doit perturber les processus de production ou mettre en danger des vies humaines. Cette contrainte impose une méthodologie très différente des pentests offensifs traditionnels.

La méthodologie de pentest OT recommandée par l'ANSSI et l'ICS-CERT comprend plusieurs phases :

Phase 1 — Reconnaissance passive : Collecte d'informations sans interaction directe avec les systèmes OT. Sources utilisées : documentation technique fournie par le client, cartographie réseau existante, analyse Shodan des équipements potentiellement exposés, et capture passive du trafic réseau sur des spans dédiés.

Phase 2 — Analyse de protocoles : Capture et analyse du trafic des protocoles industriels (Modbus, DNP3, OPC UA) pour comprendre les communications normales et identifier les équipements présents. Outils utilisés : Wireshark avec plugins ICS, Claroty Research, et des scripts Scapy personnalisés.

Phase 3 — Tests sur équipements similaires : Les tests destructifs ou potentiellement perturbateurs sont réalisés sur des équipements identiques à ceux du site industriel, dans un laboratoire OT reproduisant fidèlement l'environnement cible. Cette approche garantit la non-perturbation du site réel.

Phase 4 — Tests contrôlés en production : Uniquement les tests non perturbateurs (scans de découverte lents et contrôlés, analyse de vulnérabilités passive) sont réalisés sur les systèmes de production, avec fenêtres de maintenance préplanifiées et possibilité de rollback immédiat.

IEC 62443 : le standard de référence pour la cybersécurité industrielle

La norme **IEC 62443** (anciennement ISA-99) est le standard international de référence pour la cybersécurité des systèmes de contrôle et d'automatisation industrielle (IACS). Elle définit les exigences pour les quatre parties prenantes de l'écosystème OT : les propriétaires d'actifs (Asset Owner), les intégrateurs de systèmes, les fournisseurs de composants, et les organisations de maintenance.

IEC 62443 organise les exigences de sécurité en *Security Levels (SL)* de 0 à 4, reflétant la sophistication des attaquants potentiels et les conséquences d'une compromission :

SL 0 : Pas de mesure de sécurité spécifique (systèmes non connectés, sans risque d'attaque intentionnelle).

SL 1 : Protection contre les attaques opportunistes (erreurs humaines, erreurs logicielles accidentelles). Authentification basique, journalisation des accès.

SL 2 : Protection contre des attaquants ayant des ressources limitées. MFA, contrôle d'accès basé sur les rôles, segmentation réseau.

SL 3 : Protection contre des attaquants sophistiqués et motivés (hacktivistes, concurrents, cyber-terroristes). Chiffrement, détection des intrusions, tests de pénétration réguliers.

SL 4 : Protection contre des attaquants d'État disposant de ressources illimitées (groupes APT nationaux). Réservé aux infrastructures les plus critiques (nucléaire, défense).

NIS2 et OIV : nouvelles obligations pour les infrastructures critiques industrielles

La transposition française de NIS2 a introduit des changements significatifs pour les acteurs industriels. Les Opérateurs d'Importance Vitale (OIV) et les Opérateurs de Services Essentiels (OSE) des secteurs industriels critiques (énergie, eau, transport, alimentation) sont désormais classifiés comme **Entités Essentielles (EE)** sous NIS2, avec les obligations les plus strictes.

Pour les OIV industriels, les nouvelles obligations NIS2 incluent : la mise en œuvre des 18 mesures de sécurité obligatoires (gestion des risques, incidents, chaîne d'approvisionnement, chiffrement), la notification des incidents significatifs à l'ANSSI dans les 24 heures (72 heures pour les non-critiques), et la réalisation d'audits de sécurité par des prestataires qualifiés PASSI tous les 3 ans minimum.

Le secteur de l'énergie est particulièrement impacté : les gestionnaires de réseaux électriques (RTE), les opérateurs de distribution d'eau, et les exploitants de centrales thermiques et nucléaires doivent démontrer leur conformité NIS2/IEC 62443 via des audits réguliers. L'ANSSI a publié des guides sectoriels spécifiques à chaque secteur critique pour faciliter l'interprétation des exigences.

Outils spécialisés pour l'analyse OT/SCADA : Claroty, Dragos, Nozomi

L'écosystème des outils de sécurité OT/SCADA a considérablement mûri ces dernières années, avec l'émergence de solutions spécialisées capables d'analyser les protocoles industriels propriétaires et de détecter les anomalies comportementales dans les environnements de contrôle industriel.

Claroty : La plateforme Claroty offre une visibilité complète des actifs OT (découverte passive des équipements via analyse du trafic réseau), une détection des vulnérabilités des équipements industriels (base CVE OT propriétaire), et une surveillance comportementale pour détecter les

déviations par rapport aux communications normales. Claroty est particulièrement apprécié pour sa couverture des protocoles propriétaires Siemens, Schneider Electric, et Honeywell.

Dragos : Focalisée sur la détection des menaces OT avancées (APT ciblant les infrastructures critiques), la plateforme Dragos intègre des renseignements sur les groupes de menaces ICS documentés (Sandworm, TRITON/TRISIS, Industroyer/Crashoverride). Son intelligence spécialisée OT est reconnue comme l'une des plus complètes du marché.

Nozomi Networks : Solution populaire pour la visibilité OT/IoT combinée, Nozomi offre une analyse réseau passive, une gestion des vulnérabilités OT, et des intégrations avec les SIEM et SOC IT traditionnels. Son approche hybride OT/IT facilite la convergence des opérations de sécurité entre les équipes IT et OT.

Attaques notables sur les infrastructures OT/ICS : cas d'analyse

L'analyse des attaques réelles ayant ciblé des infrastructures OT/ICS fournit des enseignements précieux pour la conception de défenses adaptées. Plusieurs incidents emblématiques méritent une analyse détaillée :

Ukraine Power Grid (2015-2016) : La première cyberattaque documentée ayant provoqué une coupure d'électricité. Le malware BlackEnergy/Sandworm a compromis les systèmes IT des distributeurs d'électricité ukrainiens, puis pivoté vers les SCADA pour émettre des commandes d'ouverture de disjoncteurs, privant d'électricité environ 230 000 foyers pendant plusieurs heures. L'attaque a démontré la faisabilité d'attaques cyber sur les réseaux électriques.

TRITON/TRISIS (2017) : Cette attaque ciblant une pétrochimique au Moyen-Orient est la première à avoir visé spécifiquement les Safety Instrumented Systems (SIS), les systèmes de sécurité physique conçus pour éviter les accidents industriels. La compromission des SIS aurait pu provoquer une explosion de l'installation. L'attaque a été attribuée au groupe russe Sandworm.

Colonial Pipeline (2021) : Bien que l'attaque ransomware DarkSide ait ciblé principalement le réseau IT de Colonial Pipeline, les opérateurs ont eux-mêmes décidé d'arrêter les opérations OT par précaution, provoquant une pénurie de carburant sur la côte Est des États-Unis. Cet incident

illustre l'interdépendance IT/OT et l'impact potentiel des compromissions IT sur les opérations physiques.

FAQ — Questions fréquentes sur la sécurité OT/ICS SCADA

Comment réaliser un pentest OT sans interrompre la production ?

La règle fondamentale du pentest OT est "First, do no harm" (d'abord, ne pas nuire). Les approches permettant de tester la sécurité sans interrompre la production incluent : (1) Tests passifs uniquement (capture et analyse du trafic réseau sans interaction avec les équipements) ; (2) Tests sur des équipements hors ligne dans un laboratoire OT reproduisant l'environnement cible ; (3) Tests en heures creuses/arrêts programmés avec validation préalable des équipes de production ; (4) Utilisation d'équipements équivalents loués ou empruntés pour les tests destructifs ; (5) Tests uniquement sur les composants IT de l'infrastructure (interfaces de gestion, serveurs SCADA, HMI) en évitant les PLC et actionneurs. Le plan de test doit être validé par le Responsable de la Production avant toute exécution.

Quelle est la différence entre OT, ICS et SCADA ?

Ces trois termes sont souvent confondus mais désignent des périmètres différents. L'**OT (Operational Technology)** est le terme générique désignant tous les systèmes matériels et logiciels qui contrôlent, surveillent et gèrent des équipements physiques, des processus industriels et des infrastructures. L'**ICS (Industrial Control System)** est un type d'OT désignant les systèmes de contrôle industriels : il englobe les PLC, les DCS (Distributed Control System), les RTU (Remote Terminal Unit), et les systèmes de supervision associés. Le **SCADA (Supervisory Control and Data Acquisition)** est un type spécifique d'ICS permettant la supervision et le contrôle à distance d'infrastructures géographiquement dispersées (pipelines, réseaux électriques, systèmes d'eau). En résumé : SCADA ⊂ ICS ⊂ OT.

Les protocoles industriels anciens comme Modbus peuvent-ils être sécurisés ?

La sécurisation des protocoles industriels hérités sans mécanismes d'authentification ni de chiffrement natifs est possible via plusieurs approches : (1) **Encapsulation TLS** : des passerelles de sécurité encapsulent le trafic Modbus/DNP3 dans des tunnels TLS pour les segments réseau à risque ; (2) **Whitelisting des communications** : des firewalls industriels filtrant strictement les commandes autorisées (par exemple, autoriser uniquement les lectures Modbus et bloquer les commandes d'écriture depuis les segments non autorisés) ; (3) **Monitoring comportemental** : des solutions comme Claroty ou Nozomi détectent les commandes inhabituelles ou les fréquences d'interrogation anormales ; (4) **Segmentation réseau** : isolation des équipements utilisant ces protocoles dans des zones de confiance strictement contrôlées. La migration vers des protocoles sécurisés modernes (OPC UA avec sécurité activée) reste l'approche idéale mais nécessite des investissements et des arrêts de production conséquents.

Comment détecter une cyberattaque en cours sur un système SCADA ?

La détection d'attaques sur les systèmes SCADA nécessite des approches adaptées aux contraintes OT. Les indicateurs à surveiller incluent : modifications inattendues des paramètres de processus (setpoints, seuils d'alarme) qui pourraient indiquer une manipulation de PLC, communications réseau inhabituelles sur les ports de protocoles industriels (scans de ports, requêtes de lecture exhaustive des registres Modbus), accès aux HMI depuis des adresses IP non répertoriées ou à des heures inhabituelles, modifications des configurations des automates programmables, et alarmes de sécurité physique (détecteurs d'intrusion dans les salles de contrôle) simultanées avec des anomalies cyber. Un SOC hybride IT/OT avec des règles de détection adaptées aux protocoles industriels est indispensable pour une surveillance efficace.

Data diode et transfert unidirectionnel : protection des réseaux OT critiques

La **data diode** (ou passerelle unidirectionnelle) est le mécanisme de protection le plus robuste pour isoler les réseaux OT critiques tout en permettant la remontée de données vers les systèmes

IT. Contrairement aux firewalls (bidirectionnels), une data diode garantit physiquement qu'aucune donnée ne peut transiter du réseau IT vers le réseau OT.

Les data diodes sont utilisées dans les environnements les plus sensibles (nucléaire, défense, énergie critique) où la compromission du réseau IT ne doit en aucun cas affecter le réseau OT. Des constructeurs spécialisés comme Waterfall Security Solutions, Fox-IT (Owl) et VADO proposent des data diodes certifiées pour les environnements critiques.

L'implémentation d'une data diode impose des contraintes architecturales importantes : la supervision en temps réel des systèmes OT (statuts, alarmes, données de production) peut remonter vers le réseau IT, mais aucune commande de l'IT vers l'OT n'est possible via ce lien. La maintenance distante des équipements OT doit utiliser d'autres canaux sécurisés (accès physique local, connexion VPN dédiée avec contrôle strict).

En France, la mise en place de data diodes ou de mécanismes équivalents est obligatoire pour les OIV des secteurs les plus sensibles, conformément aux arrêtés sectoriels LPM (Loi de Programmation Militaire) et aux nouvelles exigences NIS2. L'ANSSI valide les solutions de passerelles unidirectionnelles dans le cadre de son processus de qualification. Des solutions comme les produits de sécurité qualifiés ANSSI incluent des passerelles unidirectionnelles pour les infrastructures critiques.

Pour aller plus loin sur les thématiques connexes, consultez notre guide sur la conformité NIS2 Phase 2, notre analyse du forensics cloud, notre article sur la certification SecNumCloud, et notre introduction à la conformité HDS 2026. La sécurité des infrastructures industrielles est aussi abordée dans notre référentiel ISO 27001.

Vulnerability management OT : spécificités et contraintes industrielles

La gestion des vulnérabilités dans les environnements OT présente des défis radicalement différents du monde IT. Les équipements industriels (PLC, RTU, HMI) ont des cycles de vie de 15 à 30 ans, leurs systèmes d'exploitation sont souvent obsolètes et non patchables sans interruption de service, et certains fabricants n'émettent plus de mises à jour de sécurité pour des équipements toujours en production.

L'inventaire des actifs OT est la première étape du vulnerability management industriel. Des outils comme **Claroty**, **Nozomi Networks**, et **Dragos** réalisent cette découverte passive (sans interaction active avec les équipements) en analysant le trafic réseau pour identifier chaque équipement, sa version firmware, et ses communications. Cet inventaire constitue la base du registre des risques OT.

La priorisation des vulnérabilités OT utilise des méthodes différentes du scoring CVSS standard. Le framework *CVSS ICS (Industrial Control System)* adapte le calcul du score aux spécificités OT : l'impact sur la sécurité physique (safety impact) est ajouté comme vecteur additionnel, et l'exploitabilité tient compte de la segmentation réseau typique des environnements OT.

Pour les vulnérabilités non corrigeables (équipements obsolètes, absence de patch fabricant), les **contrôles compensatoires** sont essentiels : segmentation réseau renforcée pour isoler les équipements vulnérables, monitoring comportemental pour détecter les tentatives d'exploitation, listes blanches de communications autorisées vers/depuis les équipements vulnérables, et planification de remplacement prioritaire dans la feuille de route d'investissement industriel.

Sécurité des automates programmables (PLC) : configuration et hardening

Les automates programmables (PLC — Programmable Logic Controllers) sont les composants les plus critiques d'un système de contrôle industriel. Un PLC compromis peut provoquer des arrêts de production, des dommages matériels, et dans les pires cas, des accidents industriels graves.

Le hardening des PLC commence par la sécurisation des accès : désactivation des protocoles de maintenance non utilisés (ports série, interfaces USB, protocoles de configuration non authentifiés), activation des mécanismes d'authentification disponibles (bien que limités sur les PLC anciens), et protection physique des ports de configuration locaux par des verrous ou des procédures d'accès strictes.

La **gestion des modifications des programmes automates** est un enjeu de sécurité majeur. Toute modification du programme PLC (ladder diagram, function block, structured text) doit suivre un processus de validation incluant : contrôle de version des programmes (SVN, Git

adapté OT), validation fonctionnelle en laboratoire avant déploiement en production, et signature cryptographique des programmes (disponible sur les PLC modernes Siemens S7-1500, Schneider Modicon M340+).

Les **accès de télémaintenance aux PLC** constituent un vecteur d'attaque majeur. Les connexions de maintenance des fournisseurs (Siemens, Schneider Electric, Rockwell Automation) doivent transiter par des VPN dédiés avec MFA, être limitées dans le temps (accès temporaire révoqué après intervention), et être supervisiées par du personnel interne. L'utilisation de solutions PAM (Privileged Access Management) adaptées OT, comme CyberArk ou Wallix, pour gérer ces accès tiers est une bonne pratique croissante.

IIoT et industrie 4.0 : nouveaux risques cyber pour les usines connectées

L'**IIoT (Industrial Internet of Things)** et la transformation digitale de l'industrie (Industrie 4.0) ont introduit une nouvelle catégorie de risques cyber dans les usines. Les capteurs IIoT, les robots collaboratifs (cobots), les systèmes de vision industrielle et les plateformes MES cloud créent de nouvelles surfaces d'attaque dans des environnements autrefois complètement isolés.

Les capteurs IIoT présentent des vulnérabilités spécifiques : firmware mis à jour rarement voire jamais, mots de passe par défaut souvent non changés, communications non chiffrées sur des protocoles comme MQTT sans TLS, et interfaces web d'administration accessibles sans authentification. La prolifération de milliers de capteurs IIoT dans une usine crée une surface d'attaque massive difficile à gérer avec les outils IT traditionnels.

Les plateformes **MES (Manufacturing Execution System)** cloud connectent en temps réel les données de production aux systèmes ERP et d'analyse. Cette connectivité cloud bidirectionnelle est un facteur de risque important : une compromission du compte cloud de la plateforme MES peut permettre à un attaquant d'accéder aux données de production ou, dans certaines architectures mal sécurisées, d'envoyer des commandes aux équipements de production via les APIs de la plateforme.

La sécurisation des environnements IIoT repose sur l'application des principes de *Zero Trust* à l'OT : vérification systématique de l'identité et de l'intégrité de chaque dispositif avant connexion

au réseau, segmentation micro-réseau par type d'équipement, chiffrement des communications même sur les réseaux internes, et surveillance comportementale continue des flux réseau OT/IIoT.

Réponse aux incidents OT/ICS : spécificités et procédures d'urgence

La réponse aux incidents de cybersécurité en environnement OT doit impérativement intégrer les contraintes de sécurité physique et de continuité des processus industriels. Un incident cyber OT peut avoir des conséquences bien au-delà de la perte de données : arrêt de production avec pertes financières importantes, dommages matériels aux équipements, accidents industriels, et dans les cas extrêmes, risques pour la vie humaine.

Le **plan de réponse aux incidents OT (ICS-IRP)** doit définir clairement les procédures de **mode dégradé** permettant de maintenir une production minimale en cas de compromission des systèmes de supervision. Dans de nombreuses industries, des procédures manuelles documentées permettent de maintenir la production de façon sécurisée pendant quelques heures sans SCADA, le temps de contenir l'incident et de restaurer les systèmes.

La collaboration entre les équipes IT (responsables de la réponse cyber) et les équipes OT (responsables de la sécurité physique et de la continuité de production) est critique lors d'un incident. Ces deux équipes ont souvent des cultures et des priorités différentes, et une formation et des exercices conjoints réguliers sont indispensables pour coordonner efficacement la réponse lors d'un vrai incident.

Les exercices de simulation d'incidents OT (*OT tabletop exercises*) devraient être réalisés annuellement, incluant des scénarios réalistes : compromission des serveurs SCADA, manipulation de setpoints de processus, ransomware ciblant les HMI, et perte de vision sur des équipements critiques. Ces exercices révèlent souvent des gaps dans les procédures et les compétences que seul un test en conditions quasi-réelles peut identifier. Références complémentaires : ENISA — Guide sécurité ICS.

Certification et formations en cybersécurité OT : GICSP, ICS-CERT, CSSA

La montée en compétences en cybersécurité OT/ICS requiert des formations spécialisées combinant expertise en systèmes de contrôle industriels et compétences en cybersécurité. L'offre de formation et de certification dans ce domaine s'est considérablement développée en réponse à la demande croissante.

Le **GICSP (Global Industrial Cyber Security Professional)** de GIAC est la certification la plus reconnue dans le domaine de la cybersécurité OT. Elle couvre les protocoles industriels, les architectures ICS, la méthodologie de sécurisation des SCADA, et les pratiques de réponse aux incidents OT. Le cours préparatoire SANS ICS515 (ICS Active Defense and Incident Response) est particulièrement apprécié des praticiens.

L'**ICS-CERT (Industrial Control Systems Cyber Emergency Response Team)** américain propose des formations gratuites en ligne sur la cybersécurité OT via son Learning Management System (disponible sur training.cisa.gov). Ces formations couvrent les fondamentaux de la sécurité ICS, l'évaluation des risques cyber-physiques, et la réponse aux incidents OT.

En France, l'**ANSSI** a développé un référentiel de compétences pour les opérateurs OT des secteurs critiques et soutient plusieurs programmes de formation universitaires en cybersécurité industrielle (Master CISA à l'EPITA, formations IMT Atlantique sur la cybersécurité des systèmes industriels). Des certifications spécifiques aux équipementiers industriels (Siemens SITRAIN, Schneider Electric Learning) complètent l'offre pour les techniciens travaillant au quotidien sur les systèmes de contrôle.

Sécurité des réseaux électriques : normes NERC CIP et IEC 61850

Le secteur de l'énergie électrique est le plus réglementé en matière de cybersécurité OT. En Amérique du Nord, les normes **NERC CIP (North American Electric Reliability Corporation Critical Infrastructure Protection)** imposent des exigences strictes aux exploitants de réseaux électriques. En Europe, la directive NIS2 combinée aux standards IEC 61850 et IEC 62443 forme le cadre réglementaire applicable.

L'**IEC 61850** est le standard de référence pour les communications dans les postes de transformation électrique. Il définit les modèles de données, les protocoles de communication (GOOSE, SAMPLED VALUES, MMS), et les exigences de cybersécurité pour les Intelligent Electronic Devices (IED) utilisés pour la protection et le contrôle du réseau électrique.

Les vulnérabilités spécifiques aux protocoles IEC 61850 incluent : les messages GOOSE (Generic Object Oriented Substation Event) qui sont transmis en multicast non authentifié sur le réseau local — leur falsification peut provoquer l'ouverture de disjoncteurs, les communications MMS (Manufacturing Message Specification) sur le port 102/TCP qui transportent les commandes de contrôle sans chiffrement natif dans les versions antérieures, et les interfaces de configuration des IED souvent accessibles via des protocoles hérités non sécurisés.

La protection des réseaux électriques contre les cyberattaques est une priorité nationale pour l'ANSSI. RTE (Réseau de Transport d'Électricité) et Enedis (gestionnaire du réseau de distribution) sont classifiés comme OIV et soumis aux exigences les plus strictes en matière de cybersécurité OT, incluant des audits PASSI réguliers et des exercices de simulation d'attaques.

Sécurité des systèmes de traitement des eaux : enjeux OT spécifiques

Les systèmes de traitement des eaux (stations d'épuration, réseaux de distribution d'eau potable) sont parmi les infrastructures critiques les plus exposées aux cyberattaques OT, comme l'a démontré l'incident d'Oldsmar (Floride, 2021) où un attaquant a tenté d'augmenter le taux de soude caustique dans l'eau potable via un accès à distance non sécurisé au système SCADA.

Les *systèmes de contrôle du traitement de l'eau* présentent des vulnérabilités typiques : interfaces HMI accessibles via des logiciels de bureau à distance (TeamViewer, AnyDesk) sans MFA, mots de passe partagés entre plusieurs opérateurs, et accès Internet direct pour la supervision à distance sans VPN sécurisé.

Les recommandations de sécurité spécifiques aux réseaux d'eau incluent : isolation stricte des réseaux SCADA d'eau de l'Internet, MFA obligatoire pour tous les accès à distance (même locaux), surveillance des paramètres de traitement anormaux (dosage de chlore, pH, pression), et plans de continuité permettant un retour rapide aux contrôles manuels en cas de compromission

des systèmes automatisés. Les opérateurs de service d'eau français sont classifiés OIV et soumis aux obligations ANSSI/NIS2 correspondantes.

Gestion des tiers OT : prestataires de maintenance et sécurité de la chaîne d'approvisionnement

La sécurité de la chaîne d'approvisionnement OT est un enjeu critique souvent sous-estimé. Les attaquants sophistiqués ciblent fréquemment les prestataires de maintenance ayant un accès légitime aux systèmes industriels pour s'infiltrer dans leurs réseaux cibles via ces vecteurs de confiance.

L'incident NotPetya (2017) a rappelé l'importance de cette menace : le malware s'est propagé via le logiciel comptable ukrainien MeDoc, infectant des milliers d'entreprises mondiales ayant des connexions de confiance avec leurs partenaires ukrainiens. Dans le monde OT, les logiciels de maintenance des fabricants (Siemens TIA Portal, Schneider Electric EcoStruxure, Rockwell FactoryTalk) peuvent constituer des vecteurs similaires.

Les bonnes pratiques de gestion des tiers OT incluent : évaluation de la cybersécurité des prestataires avant contrat (questionnaire de sécurité OT, vérification des certifications), isolation des accès de maintenance sur des VLAN dédiés sans accès au réseau OT de production, supervision en temps réel de toutes les sessions de maintenance distante (PAM OT), et clause contractuelle imposant la notification immédiate en cas d'incident cyber chez le prestataire. La gestion des tiers OT est désormais explicitement couverte par les exigences IEC 62443-2-4 (exigences pour les prestataires de services OT) et les nouvelles obligations NIS2.

Architecture Zero Trust pour les réseaux OT industriels

L'approche **Zero Trust**, popularisée dans les environnements IT, est en cours d'adaptation pour les réseaux OT. Si les principes de Zero Trust (ne jamais faire confiance, toujours vérifier) sont

universellement pertinents, leur implémentation dans l'OT présente des défis spécifiques liés aux contraintes temps-réel des systèmes de contrôle industriel.

Les piliers Zero Trust adaptés à l'OT incluent : la microsegmentation des zones de contrôle industriel (remplacement des VLANs statiques par des règles de sécurité dynamiques basées sur l'identité des équipements), l'authentification basée sur des certificats pour les communications machine-à-machine dans les protocoles modernes (OPC UA, TLS mutualisé), la surveillance continue du comportement des équipements (baseline comportementale et détection d'anomalies), et la visibilité complète des actifs OT (inventaire automatisé en temps réel).

Des frameworks comme **NIST SP 800-82 Guide to ICS Security** et le guide ANSSI "Maîtriser la SSI pour les systèmes industriels" fournissent les architectures de référence pour l'implémentation d'une sécurité Zero Trust dans les environnements OT. Ces guides reconnaissent les contraintes temps-réel et les limitations des équipements hérités, et proposent des approches pragmatiques adaptées aux réalités opérationnelles industrielles.

La mise en œuvre progressive du Zero Trust OT suit généralement un parcours sur 3 à 5 ans : (1) Inventaire et classification des actifs OT ; (2) Segmentation réseau améliorée (zones et conduits IEC 62443) ; (3) Déploiement d'une solution NDR (Network Detection and Response) OT ; (4) Authentification forte pour les accès à distance ; (5) Microsegmentation et politiques de moindre privilège pour les communications machine-à-machine. Cette approche progressive permet de renforcer la sécurité sans perturber les opérations industrielles critiques.

Outils open source pour l'analyse des protocoles OT : Nmap ICS, Scapy, Redpoint

La communauté open source a développé plusieurs outils permettant l'analyse des protocoles industriels, utilisés principalement pour les audits de sécurité OT et la formation. Ces outils doivent être utilisés avec la plus grande prudence dans des environnements de production, car leur usage non contrôlé peut perturber des équipements industriels sensibles.

Nmap ICS NSE Scripts : Nmap dispose d'un ensemble de scripts NSE (Nmap Scripting Engine) spécialisés pour les protocoles industriels : `modbus-discover` (découverte d'équipements Modbus

et lecture des registres), `dnp3-info` (informations sur les stations DNP3), `s7-info` (identification des PLC Siemens S7), et `profinet-dcp-discover` (découverte d'équipements Profinet). Ces scripts doivent être utilisés avec des paramètres de timing très lents (`-T1`) pour ne pas saturer les équipements OT.

Scapy : Le framework de manipulation de paquets Python Scapy intègre des couches protocolaires pour Modbus, DNP3, EtherNet/IP, et d'autres protocoles industriels. Il permet de construire et d'envoyer des requêtes personnalisées pour tester des comportements spécifiques des équipements OT lors d'audits de sécurité contrôlés.

Redpoint : Développé par Digital Bond (maintenant SecurityMatters/Nozomi), le projet Redpoint fournit des scripts Nmap pour la découverte et l'interrogation d'équipements industriels. Bien que plus récents que les scripts NSE officiels, les scripts Redpoint couvrent un spectre plus large de protocoles propriétaires industriels.

Shodan Industrial : Le moteur de recherche Shodan dispose de filtres spéciaux pour identifier les équipements industriels exposés sur Internet : `port:502` (Modbus), `port:102` (Siemens S7/ ISO-TSAP), `port:47808` (BACnet), `port:4840` (OPC UA). L'utilisation de Shodan pour cartographier l'exposition OT d'une organisation est une étape de reconnaissance passive précieuse lors d'audits de sécurité.

Ces outils open source sont complétés par des plateformes commerciales comme **Tenable OT Security** (anciennement Indegy), **Claroty Platform**, et **Dragos Platform**, qui offrent une couverture protocolaire beaucoup plus large et des bases de vulnérabilités OT spécialisées. Le choix entre outils open source et solutions commerciales dépend de la taille de l'organisation, des budgets disponibles, et de la complexité de l'environnement OT à auditer. Pour les grands OIV industriels, l'investissement dans des plateformes commerciales spécialisées est généralement justifié par la richesse fonctionnelle et le support en cas d'incident.

Intégration OT dans le SOC : défis et architecture du SOC hybride IT/OT

L'intégration de la surveillance des réseaux OT dans un SOC (Security Operations Center) traditionnel IT représente un défi organisationnel et technique majeur. Les analystes SOC IT

n'ont généralement pas de formation en systèmes de contrôle industriels, et les alertes générées par les sondes OT (anomalies de protocoles industriels, déviations de comportement de PLC) nécessitent une interprétation spécialisée.

L'architecture d'un **SOC hybride IT/OT** efficace comprend généralement : des sondes de détection spécialisées OT (Claroty, Nozomi, Dragos) déployées dans les zones OT et remontant leurs alertes dans un SIEM commun (Splunk, QRadar, Elastic), des règles de corrélation IT/OT croisant les événements des deux domaines, des analystes spécialisés OT (souvent en astreinte) capables d'interpréter les alertes industrielles, et des procédures d'escalade définissant clairement qui contacter en cas d'alerte OT critique (équipe de production, RSSI, direction).

La **corrélation IT/OT** dans le SIEM est particulièrement précieuse pour détecter les phases de latéralisation IT vers OT caractéristiques des attaques sophistiquées. Un exemple de règle de corrélation : "Si un compte de service IT accède à un serveur SCADA dans les 10 minutes suivant une authentification réussie sur ce compte depuis une IP externe inconnue, générer une alerte critique". Ce type de règle aurait pu détecter les premières phases de l'attaque Colonial Pipeline avant le déploiement du ransomware.

La supervision 24/7 des systèmes OT critiques est une obligation pour les OIV. Certaines organisations mutualisent cette surveillance via des **SOC sectoriels** : le Centre de Réponse aux Incidents Cyber pour les Opérateurs d'Importance Vitale (CERT-OIV), les SOC de branche proposés par des associations sectorielles (GIFEN pour l'énergie, USF pour les services de l'eau), et les offres de SOC managé OT proposées par des intégrateurs spécialisés (Capgemini Cybersecurity, Thales CERT, Airbus CyberSecurity).

Retour d'expérience : mise en œuvre de la sécurité OT dans une PMI française

La sécurisation des systèmes industriels n'est pas réservée aux grands OIV. Les PMI (Petites et Moyennes Industries) françaises sont de plus en plus ciblées par les attaques ransomware, qui frappent sans discrimination tous les secteurs. Le retour d'expérience d'une PMI agroalimentaire de 200 salariés ayant entrepris sa transformation cyber OT illustre les défis concrets de ce type de projet.

Le diagnostic initial révèle une situation typique des PMI industrielles françaises : réseau OT et IT sur le même VLAN sans séparation, automates programmables accessibles directement depuis les postes bureautiques, logiciels SCADA tournant sur Windows 7 sans patch depuis 2020, et accès de télémaintenance par TeamViewer sans mot de passe robuste ni MFA.

La remédiation a été planifiée sur 18 mois avec un budget de 180 000 euros, réparti entre : la mise en place d'un réseau OT segmenté avec DMZ industrielle et firewall industriel Stormshield SNXr (certifié ANSSI), le remplacement des postes SCADA Windows 7 par des postes Windows Server 2022 LTSC supportés jusqu'en 2031, la mise en place d'un VPN industriel pour les accès de maintenance, et la formation des techniciens de maintenance aux risques cyber.

Les résultats 18 mois après : zéro incident de sécurité majeur, réduction de 80% de la surface d'attaque mesurée lors d'un audit de suivi, et accès à des contrats avec donneurs d'ordre grand compte ayant imposé des exigences de cybersécurité OT minimales. L'investissement en cybersécurité OT s'est avéré être un avantage concurrentiel au-delà de la simple réduction des risques.

Perspectives 2027 : cyber-résilience OT et souveraineté technologique industrielle

Les tendances qui façonneront la sécurité OT/ICS dans les prochaines années incluent des évolutions technologiques et réglementaires majeures. L'accélération de la convergence IT/OT avec l'adoption de l'IIoT et des architectures cloud-edge en milieu industriel va continuer à élargir la surface d'attaque, nécessitant des architectures de sécurité plus flexibles et adaptables.

La **souveraineté technologique industrielle** devient un enjeu géopolitique : la dépendance à des équipements et logiciels industriels d'origines étrangères (Siemens, Schneider Electric, Rockwell Automation, ABB) crée des risques de backdoors et de vulnérabilités non divulguées. Des initiatives européennes comme le programme Gaia-X et les politiques de préférence européenne dans les marchés publics industriels cherchent à réduire cette dépendance. En France, le Plan France 2030 finance des projets de développement de technologies OT souveraines.

La **cyber-résilience OT** — la capacité à maintenir un niveau minimal de production même lors d'une cyberattaque — devient l'objectif ultime au-delà de la simple cybersécurité. Les architectures résilientes OT combinent segmentation réseau robuste, redondance des systèmes critiques, procédures de mode dégradé documentées et testées, et capacités de détection/réponse rapides. Cette approche résilience-by-design est au cœur des recommandations de l'ANSSI pour les OIV français dans leurs nouvelles directives publiées en 2025.

Procurement OT sécurisé : intégrer la cybersécurité dans les achats industriels

L'intégration de critères de cybersécurité dans les processus d'achat d'équipements industriels est une approche préventive fondamentale. Trop souvent, les équipements OT sont sélectionnés uniquement sur des critères fonctionnels et de prix, sans évaluation des caractéristiques de sécurité, créant des vulnérabilités qui devront être gérées pendant 15 à 30 ans.

Un processus de *secure procurement OT* inclut : la vérification que le fabricant dispose d'une politique de divulgation des vulnérabilités (CVD — Coordinated Vulnerability Disclosure) et d'une roadmap de support de sécurité sur la durée de vie prévue de l'équipement, l'évaluation des mécanismes d'authentification, de chiffrement et de mise à jour du firmware disponibles, la demande d'un Software Bill of Materials (SBOM) listant tous les composants logiciels tiers inclus dans le firmware (permettant de vérifier l'absence de composants vulnérables connus), et la négociation de clauses contractuelles obligeant le fabricant à fournir des patches de sécurité dans des délais définis.

Le règlement européen **Cyber Resilience Act (CRA)**, adopté en 2024 et applicable progressivement jusqu'en 2027, imposera aux fabricants d'équipements connectés (y compris les équipements OT/IIoT) des obligations de sécurité by-design et de support de sécurité sur toute la durée de vie des produits. Cette évolution réglementaire va progressivement améliorer le niveau de sécurité intrinsèque des équipements industriels disponibles sur le marché européen, réduisant à terme la charge de sécurisation compensatoire actuellement nécessaire dans les environnements OT.