Sécurité des Protocoles OT 2026 : Modbus, DNP3, MQTT et IEC 61850

Sécurité protocoles OT 2026 — Modbus, DNP3, MQTT, IEC 61850 : vulnérabilités, chiffrement, monitoring Claroty/Nozomi et défenses pour infrastructures critiques.

Les protocoles de communication des systèmes industriels ont été conçus dans les années 1970-1990 pour un objectif unique : la fiabilité et la déterminisme temporel. La cybersécurité n'était alors pas une priorité — ces réseaux étaient physiquement isolés, les attaques informatiques n'existaient que dans les romans de science-fiction. En 2026, la réalité est radicalement différente : les environnements OT (Operational Technology) sont massivement connectés aux réseaux IT et à Internet, les protocoles Modbus, DNP3, MQTT et IEC 61850 sont exposés à des attaquants sophistiqués, et les incidents cyber sur des infrastructures industrielles critiques se comptent en dizaines par an en France. Stuxnet en 2010, Industroyer/CRASHOVERRIDE en 2016, Triton/TRISIS en 2017, les attaques sur Colonial Pipeline en 2021 et sur des collectivités locales françaises en 2022-2024 illustrent la réalité de cette menace. Ce guide technique présente l'état de la sécurité des principaux protocoles OT en 2026 : leurs vulnérabilités inhérentes, les extensions sécurité disponibles, les outils de monitoring spécialisés, les recommandations de l'ANSSI et les architectures de défense adaptées aux contraintes de disponibilité des systèmes industriels. La règle d'or des OT — "disponibilité avant confidentialité" — impose une approche de sécurisation fondamentalement différente de celle du monde IT.

À RETENIR

À retenir — Sécurité Protocoles OT 2026

• **Modbus TCP** : zéro authentification native — isolation réseau et application whitelist sont les seuls remèdes efficaces

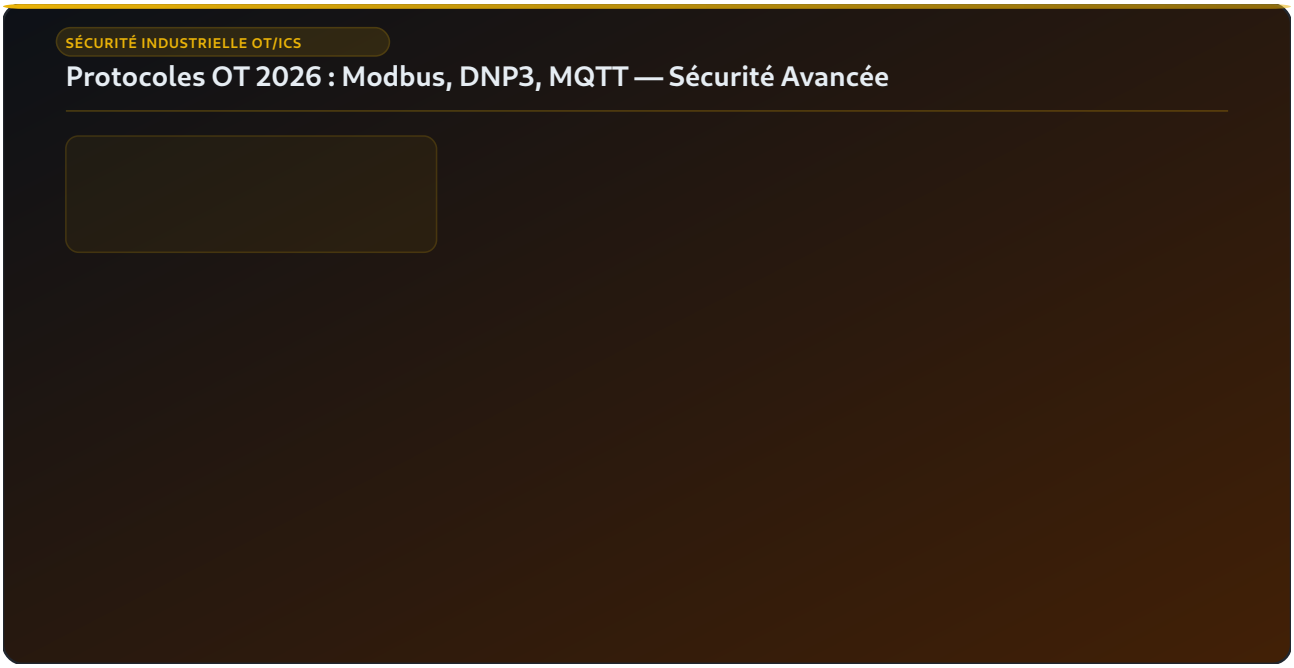
• **DNP3 Secure Authentication v5** (IEEE 1815-2012) : HMAC-SHA256 disponible mais peu déployé en France

• **MQTT** : chiffrement TLS + authentification certificat + ACL fine-grained sont les trois piliers de sécurisation

• **IEC 62351** est le standard de sécurité pour IEC 61850 — encore largement ignoré sur le terrain

• Monitoring passif (Claroty, Nozomi) : ne perturbe pas les processus industriels — recommandé en premier déploiement

• ANSSI guide ICS : référence obligatoire pour les OIV/OSE français



Modbus, développé par Modicon en 1979, est probablement le protocole industriel le plus utilisé au monde — et le moins sécurisé. Sa conception repose sur un principe maître-esclave simple : un maître interroge des esclaves (automates, capteurs, actionneurs) en lisant ou en écrivant des registres. Dans sa version originale RS-485 (Modbus RTU), le protocole était limité à des liens

série point-à-point ou multi-drop. L'adaptation TCP/IP (**Modbus TCP**, RFC non officielle) a conservé intégralement l'absence de mécanismes de sécurité : aucune authentification, aucun chiffrement, aucune intégrité des données. N'importe quel équipement pouvant envoyer une trame TCP vers le port 502 peut lire et écrire tous les registres d'un automate Modbus, modifier des valeurs de consigne, forcer des sorties digitales ou déclencher des alarmes. En 2026, des scanners comme Shodan indexent régulièrement des centaines de milliers d'équipements Modbus exposés sur Internet — une réalité alarmante pour les infrastructures critiques. La solution à court terme n'est pas d'ajouter de la sécurité à Modbus (le protocole ne le supporte pas), mais d'appliquer rigoureusement l'isolation réseau via des pare-feu industriels, des VLAN dédiés et des passerelles de protocole contrôlées.

Vulnérabilités Modbus : replay attacks et spoofing

Les attaques contre les implémentations Modbus exploitent directement l'absence de mécanismes de sécurité natifs. Les **replay attacks** consistent à capturer des trames Modbus légitimes (une commande d'ouverture de vanne, une modification de consigne) et à les rejouer ultérieurement pour reproduire l'action sans autorisation. Sans numéro de séquence ni timestamp dans le protocole, aucun mécanisme Modbus ne peut détecter un replay. Le **spoofing** d'adresse IP maître — possible sur les réseaux sans authentification — permet à un attaquant de se faire passer pour le SCADA légitime et d'envoyer des commandes malveillantes aux automates. L'**énumération de registres** permet à un attaquant ayant accès réseau de lire l'intégralité de la configuration d'un automate (registres coils, discretes inputs, holding registers, input registers) sans aucune authentification. Des outils comme **modbuspal**, **mbtget** et les modules Metasploit Modbus permettent de conduire ces attaques en quelques minutes. Un incident réel documenté en France (secteur eau, 2023) a impliqué la modification à distance de consignes de dosage via une interface Modbus TCP accessible depuis Internet sans pare-feu.

⚡ **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.

Sécurisation Modbus : mesures compensatoires

Face aux limitations intrinsèques de Modbus, la sécurisation repose sur des **mesures compensatoires** au niveau réseau et applicatif. Au niveau réseau : isolation dans un VLAN dédié avec accès filtré par pare-feu industriel ; blocage de tout trafic entrant sur le port 502 depuis les réseaux IT ; mise en place d'une **whitelist d'adresses IP** maîtres autorisées ; journalisation de toutes les connexions Modbus TCP pour détection d'anomalies. Au niveau applicatif : déploiement d'un **proxy Modbus** (Deep Packet Inspection industriel) filtrant les commandes légitimes des commandes anormales — bloquer les writes si seules des reads sont attendues, limiter les plages de registres accessibles. Des solutions comme **Waterfall Security Unidirectional Gateway** permettent de rendre la communication Modbus physiquement unidirectionnelle (données uniquement vers l'IT, aucune commande possible depuis l'IT). Dans les architectures modernes, la **migration vers des protocoles plus sécurisés** (OPC-UA avec certificats) pour les nouvelles installations est fortement recommandée, Modbus étant maintenu uniquement pour la rétrocompatibilité avec les équipements legacy.

DNP3 : le protocole des utilities avec authentification optionnelle

DNP3 (Distributed Network Protocol 3), développé en 1990 pour les utilities électriques et largement adopté en Amérique du Nord et dans certains pays européens, présente une architecture plus sophistiquée que Modbus. Il inclut des mécanismes de fragmentation de messages, d'acquittement, de timestamping et de niveaux de service différenciés. Cependant, la sécurité n'était pas davantage intégrée dans la conception originale. La version sécurisée, **DNP3 Secure Authentication v5 (SA v5)**, définie dans la norme IEEE 1815-2012, a été publiée en 2012 mais reste très peu déployée en France en 2026. SA v5 introduit un mécanisme de **challenge-response basé sur HMAC-SHA256** entre le maître et chaque esclave, permettant l'authentification des messages critiques (commandes, modifications de configuration). L'authentification n'est pas appliquée à tous les messages — une approche pragmatique pour maintenir les performances — mais couvre les opérations à fort enjeu de sécurité. L'implémentation de SA v5 nécessite une mise à jour firmware des équipements (RTU, IED) et une configuration soigneuse des clés partagées, ce qui explique en partie sa faible adoption face aux contraintes de maintenance industrielle.

DNP3 Secure Authentication v5 : mise en œuvre pratique

La mise en œuvre de **DNP3 SA v5** dans un environnement existant suit plusieurs étapes. La première est l'**inventaire de compatibilité** : vérifier que les RTU, IED et le logiciel SCADA supportent SA v5 (une mise à jour firmware peut être nécessaire). La deuxième est la **gestion des clés** : SA v5 utilise des Update Keys (UK) pour l'établissement des sessions et des Session Keys dérivées. La gestion sécurisée de ces clés — stockage hardware (HSM), rotation périodique — est la partie la plus complexe du déploiement. La troisième est la **configuration du niveau d'authentification** : SA v5 permet de définir quelles opérations nécessitent une authentification (DNP3 Critical Requests). La quatrième est le **test en environnement hors-production** : une erreur de configuration SA v5 peut bloquer la communication avec les équipements de terrain, avec des conséquences opérationnelles graves. La cinquième est le **déploiement progressif** : activer SA v5 sur les équipements les plus critiques en premier, en gardant la possibilité de

fallback en cas d'incident. Un retour terrain : le déploiement de SA v5 sur un réseau de distribution électrique de taille intermédiaire en France a nécessité 18 mois de travail, dont 12 mois consacrés aux tests et à la formation des opérateurs.

MQTT : sécurité du protocole IoT industriel

MQTT (Message Queuing Telemetry Transport), développé par IBM en 1999 et standardisé OASIS en 2014 (version 3.1.1) puis 2019 (version 5.0), est devenu un standard de facto pour la communication IoT industrielle et les architectures IIoT (Industrial IoT). Son modèle publish-subscribe via un broker central présente des avantages de scalabilité et de découplage, mais crée des vulnérabilités spécifiques si le broker n'est pas correctement configuré. Le vecteur d'attaque principal est le **broker MQTT mal configuré** : de nombreuses installations laissent le broker Mosquitto accessible sur le port 1883 sans authentification ni chiffrement, permettant à tout client de s'abonner à tous les topics (`#` wildcard) et de publier des messages arbitraires. Des scans réguliers révèlent des milliers de brokers MQTT industriels accessibles depuis Internet, exposant des données de capteurs, des états d'équipements et parfois des commandes de contrôle. La sécurisation MQTT repose sur trois piliers indissociables : **TLS 1.3** pour le transport (port 8883 au lieu de 1883) ; **authentification client** par certificat X.509 ou username/password ; et **ACL (Access Control Lists)** fine-grained définissant quel client peut publier ou s'abonner à quel topic.

Configuration sécurisée de Mosquitto : guide pratique

Mosquitto est le broker MQTT open source le plus déployé dans les environnements industriels. Sa configuration sécurisée passe par plusieurs paramètres essentiels dans le fichier `mosquitto.conf`. Le chiffrement TLS doit être activé avec les certificats appropriés. L'authentification par mot de passe ou par certificat client doit être obligatoire. Les ACL doivent

définir explicitement les topics autorisés par client. La journalisation complète doit être activée. Voici une configuration de base sécurisée :

```
 # /etc/mosquitto/mosquitto.conf — Configuration sécurisée

# Désactiver le listener non-chiffré
# listener 1883  # NE PAS activer

# Listener TLS uniquement
listener 8883
cafile /etc/mosquitto/certs/ca.crt
certfile /etc/mosquitto/certs/server.crt
keyfile /etc/mosquitto/certs/server.key
tls_version tlsv1.3

# Authentification obligatoire
allow_anonymous false
password_file /etc/mosquitto/passwd

# Authentification client par certificat (en plus du password)
require_certificate true
use_identity_as_username true

# ACL par fichier
acl_file /etc/mosquitto/acl

# Journalisation
log_type all
log_dest file /var/log/mosquitto/mosquitto.log

# Limite de taille des messages (protection DoS)
message_size_limit 65536
```

IEC 61850 et IEC 62351 : la sécurité pour les sous-stations électriques

IEC 61850 est le standard de communication pour les sous-stations électriques, définissant des modèles de données et des protocoles de communication (GOOSE, MMS, Sampled Values) adaptés aux contraintes de temps réel des équipements de protection électrique. Sa sécurité est

traitée dans la norme complémentaire **IEC 62351**, dont les différentes parties couvrent le chiffrement des communications (TLS pour MMS et XMPP, IEC 62351-3), l'authentification des échanges (IEC 62351-5 pour GOOSE et Sampled Values), la gestion des clés (IEC 62351-8), et le contrôle d'accès basé sur les rôles (IEC 62351-8). Le protocole **GOOSE (Generic Object Oriented Substation Event)** est particulièrement sensible car il véhicule les signaux de déclenchement des disjoncteurs en temps réel (délais de l'ordre de la milliseconde). Une attaque sur GOOSE peut provoquer le déclenchement intempestif de protections ou empêcher le déclenchement lors d'un défaut réel. IEC 62351-6 définit un mécanisme d'authentification GOOSE par HMAC, mais son déploiement reste limité en France, la plupart des sous-stations existantes n'ayant pas été mises à niveau.

Profinet et EtherNet/IP : sécurité des protocoles Ethernet industriels

Profinet (Siemens/PI) et **EtherNet/IP** (Allen-Bradley/ODVA) sont les deux protocoles Ethernet industriels dominants dans les environnements de fabrication en Europe et en Amérique du Nord respectivement. Contrairement à Modbus TCP, ces protocoles ont été conçus pour des communications temps réel avec des cycles de l'ordre de la milliseconde, mais partagent les mêmes lacunes de sécurité initiales. **Profinet Security** (IEC 61158-6-10) intègre désormais des mécanismes de sécurité via TLS pour les communications non-temps-réel et des mécanismes d'intégrité pour les données temps réel. **CIP Security** (extension d'EtherNet/IP) définie par ODVA ajoute TLS/DTLS pour les communications CIP, permettant l'authentification des équipements et le chiffrement. En pratique, ces extensions sécurité nécessitent des équipements récents et une infrastructure PKI industrielle — des prérequis souvent absents dans les installations existantes. La migration vers ces protocoles sécurisés s'inscrit dans les projets de modernisation pluriannuels, finançables via les dispositifs France Relance et les crédits NIS 2 pour les OSE.

OPC-UA : le protocole sécurisé pour l'interopérabilité IIoT

OPC-UA (Open Platform Communications Unified Architecture), développé par la OPC Foundation, est le protocole de référence pour l'interopérabilité industrielle moderne, incluant des mécanismes de sécurité natifs. OPC-UA intègre nativement le **chiffrement des communications** (AES-256), l'**authentification mutuelle** par certificats X.509, le **signing des messages** pour l'intégrité, et un modèle de sécurité configurable (None, Sign, Sign & Encrypt). L'architecture client-serveur et publish-subscribe d'OPC-UA permet des déploiements flexibles. Le **modèle de confiance PKI** d'OPC-UA est son principal avantage par rapport aux protocoles legacy : chaque équipement dispose d'un certificat, et la confiance est gérée via des listes de certificats approuvés/révoqués sur les serveurs. Sa principale limitation : les performances. OPC-UA est significativement plus gourmand en CPU et en mémoire que Modbus ou DNP3, le rendant inadapté aux microcontrôleurs industriels les plus contraints. Pour les architectures modernes avec des PLCs de génération récente, OPC-UA représente la trajectoire technologique naturelle pour remplacer les protocoles legacy.

Claroty et Nozomi Networks : monitoring passif des réseaux OT

Les outils de **monitoring passif des réseaux OT** constituent la première ligne de défense recommandée par l'ANSSI pour les environnements industriels. Leur principe est simple : écoute passive du trafic réseau par port mirroring ou TAP, sans aucune interaction avec les équipements de production. Cette approche non-intrusive préserve la disponibilité des systèmes tout en permettant une visibilité complète sur les communications. **Claroty** (acquis par Rockwell Automation en 2023) offre une découverte automatique des actifs OT (identification des équipements par analyse du trafic protocolaire), une détection d'anomalies comportementales (déviation par rapport aux baselines de communication), et une intégration avec les SIEM et les plateformes de gestion des vulnérabilités. **Nozomi Networks** propose des fonctionnalités similaires avec une forte capacité de décodage protocolaire (support de 200+ protocoles industriels) et une intégration native avec les SOC IT. **Dragos** (spécialisé sur les menaces ICS/OT et le threat intelligence associé) complète l'offre avec une orientation plus orientée threat

hunting. En France, ces trois solutions sont utilisées par plusieurs OIV dans leurs Security Operations Centers OT, souvent en complément d'une solution SIEM IT (Splunk, Elastic).

ANSSI et sécurité ICS : le guide de référence français

L'ANSSI a publié plusieurs référentiels de référence pour la sécurité des systèmes industriels. Le **guide "Maîtrise du risque numérique pour les systèmes industriels"** (ANSSI PA-073) définit une méthodologie d'analyse de risque et des recommandations de sécurisation adaptées aux contraintes OT. Les **recommandations pour la sécurité des architectures de contrôle de processus** (ANSSI DAT-NT-32) détaillent les architectures de référence avec zones et conduits selon IEC 62443. Le guide **"Sécurité des systèmes SCADA"** traite spécifiquement les systèmes de supervision. Ces documents, librement accessibles sur le site de l'ANSSI, constituent la référence obligatoire pour les Opérateurs d'Importance Vitale (OIV) et les Opérateurs de Services Essentiels (OSE) assujettis à NIS 2 en France. La norme **IEC 62443**, cadre international de référence pour la cybersécurité industrielle, est explicitement citée dans ces guides comme standard de mise en conformité. En 2026, plusieurs OIV du secteur énergie ont engagé des audits IEC 62443 dans le cadre de leurs obligations NIS 2, générant une demande importante de consultants spécialisés.

Architecture de référence : zones et conduits IEC 62443

L'architecture de sécurité ICS recommandée par l'ANSSI et IEC 62443 repose sur le concept de **zones et conduits**. Une **zone** est un groupement d'actifs partageant le même niveau de sécurité requis et les mêmes exigences de protection. Un **conduit** est le canal de communication contrôlé entre deux zones. La conception type pour un système industriel inclut la zone Level 5 (Enterprise), la zone Level 4 (Business Planning), la zone Level 3 (Operations Management — SCADA/DCS), les zones Level 2/1/0 (Control, Basic Control, Physical Process). Entre chaque paire de zones adjacentes, un conduit contrôlé (pare-feu industriel, DMZ OT, data diode) filtre

les communications selon le principe du moindre privilège. Cette architecture, souvent appelée **modèle Purdue étendu** ou modèle ISA-95/ISA-99, reste la référence en 2026 malgré les débats sur son adaptation aux architectures cloud et aux environnements IIoT. La mise en œuvre stricte des zones et conduits résout ou atténue la majorité des vulnérabilités protocolaires (Modbus, DNP3) par isolement des réseaux.

Segmentation réseau OT : pare-feux industriels et DMZ

La **segmentation réseau** est la mesure de sécurité la plus impactante dans un environnement OT. Un pare-feu industriel adapté (Fortinet FortiGate, Cisco ASA avec module ICS, Tofino Xenon) doit comprendre les protocoles OT pour filtrer au niveau applicatif — filtrer Modbus au niveau TCP/IP (port 502) sans comprendre les codes de fonction ne protège pas contre les attaques sur les registres. La mise en place d'une **DMZ OT** entre les réseaux IT et OT permet d'héberger les serveurs de transit, les historians de données industrielles et les interfaces opérateurs dans une zone contrôlée. Les règles de pare-feu OT doivent suivre le principe du moindre privilège : seuls les flux strictement nécessaires sont autorisés, avec des plages horaires si les besoins sont périodiques. L'utilisation de **data diodes** (passerelles unidirectionnelles physiques) pour les flux de données des réseaux critiques vers le réseau de supervision est la mesure la plus robuste — une diode physique ne peut pas être contournée par un attaquant ayant compromis le réseau IT.

Vulnérabilités spécifiques des automates (PLC) : hardening

Les **automates programmables (PLC/API)** sont les équipements les plus critiques d'un système OT — leur compromission peut avoir des conséquences physiques directes. Leur hardening passe par plusieurs mesures. La désactivation des ports et services non utilisés (SNMP, Telnet, FTP, serveur web d'administration si non requis). La modification des **mots de passe par défaut** — une mesure basique souvent négligée dans les environnements OT. La mise à jour régulière du **firmware** — difficile car nécessitant une fenêtre de maintenance planifiée, mais

indispensable pour corriger les vulnérabilités connues. La protection des **projets automates** par mot de passe et chiffrement (fonctionnalité disponible sur les gammes récentes Siemens S7-1500, Allen-Bradley Logix 5000). La limitation des accès à l'environnement de programmation (TIA Portal, Studio 5000) aux seules machines autorisées, via whitelist d'adresses IP sur le port de programmation. Un incident marquant : lors d'un audit OT conduit en 2025 sur un site de production alimentaire français, nous avons trouvé 12 automates Siemens S7-300 avec le mot de passe par défaut "BELDEN" et accessibles depuis le réseau IT sans aucun filtrage.

Threat intelligence OT : ICS-CERT et CISA KEV

La veille sur les vulnérabilités spécifiques aux équipements OT est indispensable mais souvent négligée dans les équipes OT qui ne disposent pas d'expertise en cybersécurité. Plusieurs sources de threat intelligence sont spécifiques aux environnements industriels. L'**ICS-CERT (Industrial Control Systems Cyber Emergency Response Team)** américain publie des advisories réguliers sur les vulnérabilités des équipements OT (Siemens, Schneider Electric, Rockwell, ABB…). Le **Catalogue KEV (Known Exploited Vulnerabilities)** de la CISA inclut désormais de nombreuses CVE ICS, signalant les vulnérabilités activement exploitées dans des attaques. En France, le **CERT-FR** de l'ANSSI publie des alertes sur les vulnérabilités OT impactant les systèmes utilisés par les OIV français. Des services de threat intelligence spécialisés OT comme **Dragos WorldView**, **Claroty Team82** ou **Nozomi Threat Intelligence** fournissent des indicateurs de compromission (IOC) et des analyses de malwares ICS. L'intégration de ces flux dans les processus de patch management OT — adaptés aux contraintes de maintenance planifiée — est un enjeu organisationnel majeur.

NIS 2 et sécurité OT : nouvelles obligations pour les OSE

La transposition de la directive **NIS 2** en droit français (loi n°2024-884 du 1er octobre 2024) a étendu significativement le périmètre des entités soumises aux obligations de cybersécurité, incluant désormais de nombreux opérateurs industriels précédemment hors scope. Les **Entités Essentielles** (EE) et **Entités Importantes** (EI) dans les secteurs énergie, eau, transport et industrie manufacturière critique sont désormais soumises à des obligations de sécurité incluant des mesures spécifiques aux environnements OT. Les exigences NIS 2 pertinentes pour les OT incluent : la gestion des risques de la chaîne d'approvisionnement (sécurité des équipements OT acquis), la sécurité des réseaux et systèmes d'information (segmentation IT/OT), la détection et signalement des incidents (obligation de notification ANSSI dans les 24h), et les plans de continuité et de reprise d'activité. En 2026, l'ANSSI a commencé les contrôles de conformité NIS 2, avec des lettres d'information envoyées aux entités concernées. Les sanctions prévues — jusqu'à 10 M€ ou 2% du CA mondial pour les EE — constituent une incitation forte à investir dans la sécurité OT.

MQTT 5.0 : améliorations sécurité et fonctionnelles

MQTT 5.0, publié en 2019, apporte plusieurs améliorations significatives par rapport à la version 3.1.1, notamment sur le plan de la sécurité et de la gestion des erreurs. Le mécanisme d'**Enhanced Authentication** (propriété MQTT 5.0 AUTH) permet des mécanismes d'authentification challenge-response personnalisés, au-delà du simple username/password. Les **User Properties** permettent d'ajouter des métadonnées arbitraires aux messages, utiles pour les audits et le traçage. La gestion améliorée des erreurs avec des codes de raison détaillés facilite le debugging et le monitoring. Pour la sécurité industrielle, MQTT 5.0 offre le **Payload Format Indicator** et le **Content Type**, permettant une validation plus précise du type et du format des messages avant traitement. La migration de MQTT 3.1.1 vers MQTT 5.0 est recommandée pour les nouveaux déploiements industriels, mais nécessite une mise à jour du broker (Mosquitto 2.0+ supporte MQTT 5.0) et des clients. La rétrocompatibilité est assurée : un broker MQTT 5.0 peut servir simultanément des clients 3.1.1 et 5.0.

Gestion des identités dans les environnements OT

La gestion des identités (IAM) dans les environnements OT présente des défis spécifiques. Les équipements industriels (automates, capteurs, actionneurs) ont des identités machine qui doivent être gérées avec autant de rigueur que les identités humaines. Les **certificats X.509** pour l'authentification machine (OPC-UA, MQTT avec TLS client auth) doivent être issus d'une PKI industrielle avec des procédures de rotation et de révocation adaptées aux contraintes OT (temps de maintenance planifiée). Les **accès humains** aux systèmes OT — ingénieurs d'exploitation, techniciens de maintenance, prestataires externes — doivent être gérés via des solutions de Privileged Access Management (PAM) adaptées : comptes dédiés OT, sessions enregistrées, accès limités dans le temps. Le **MFA (Multi-Factor Authentication)** pour les accès aux consoles de supervision (SCADA, DCS) est désormais recommandé par l'ANSSI, même si son déploiement reste complexe sur des interfaces opérateurs conçues avant l'ère du MFA. Les solutions de PAM industriel comme CyberArk OT Security ou Wallix Bastion ICS proposent des intégrations adaptées aux environnements Siemens, Schneider et Rockwell.

FAQ — Sécurité Protocoles OT 2026

Peut-on chiffrer Modbus TCP sans remplacer les équipements existants ?

Modbus TCP ne supporte pas nativement le chiffrement. Deux approches permettent de l'ajouter sans remplacer les équipements : un tunnel VPN entre le maître et les esclaves (IPSec ou WireGuard sur des passerelles industrielles intercalées), ou un proxy Modbus SSL/TLS qui encapsule le trafic Modbus dans une couche TLS. Ces approches ajoutent de la latence — à évaluer au regard des exigences temps réel de l'application. Pour la grande majorité des usages Modbus (polling de registres à des intervalles de secondes), cette latence supplémentaire est acceptable.

Quelle est la différence entre DNP3 SA v2 et SA v5 ?

DNP3 Secure Authentication version 2 (SA v2), défini dans l'annexe V de la norme DNP3, utilisait des MACs MD5 ou SHA-1, désormais cryptographiquement insuffisants. SA v5 (IEEE 1815-2012) est la version actuelle recommandée, utilisant HMAC-SHA256 et introduisant le concept de "Update Key" pour la gestion des clés à long terme. SA v5 améliore également la résistance aux attaques de rejoue par des numéros de séquence et des timestamps. La migration de SA v2 vers SA v5 nécessite une mise à jour firmware des équipements et n'est pas toujours possible sur le matériel le plus ancien.

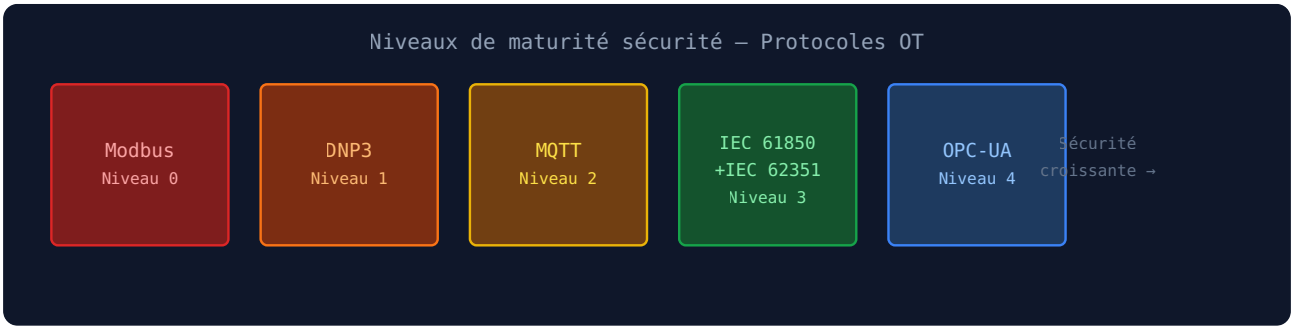
MQTT est-il adapté aux environnements industriels temps réel stricts ?

MQTT dans sa version standard n'est pas adapté aux contraintes de temps réel strict (délais de l'ordre de la milliseconde) car il repose sur TCP, qui ne garantit pas les délais de transmission. Pour les communications temps réel strict (GOOSE IEC 61850, Profinet IRT, EtherCAT), des protocoles industriels spécifiques restent nécessaires. MQTT est adapté aux échanges IIoT avec des contraintes temps réel souples (quelques secondes de latence acceptable) : télémétrie, reporting d'état, alertes. MQTT 5.0 améliore légèrement les performances mais ne résout pas la limitation fondamentale liée à TCP. Pour les usages temps réel strict sur IP, MQTT-SN (over UDP) ou DDS (Data Distribution Service) sont des alternatives à considérer.

Comment savoir si mes équipements OT sont exposés sur Internet ?

Plusieurs approches complémentaires permettent de vérifier l'exposition internet de vos équipements OT. La recherche sur Shodan (shodan.io) avec les mots-clés spécifiques à vos équipements (numéros de modèle, bannières protocolaires) ou vos plages d'adresses IP publiques révèle les équipements indexés. Le service ONYPHE (français, équivalent de Shodan) permet des recherches similaires avec une interface en français. L'ANSSI propose un service de notification aux OIV/OSE des vulnérabilités et expositions identifiées sur leurs systèmes. Un scan externe de vos adresses IP publiques avec des outils comme nmap ou masscan (dans un cadre légal, sur vos propres systèmes) complète la détection. La découverte d'équipements OT exposés sur Internet doit être traitée comme un incident de sécurité prioritaire.

Protocole	Authentification native	Chiffrement natif	Extension sécurité	Port standard
Modbus TCP	✗ Aucune	✗ Aucun	Tunnel VPN/TLS (externe)	502/TCP
DNP3	⚠ SA v5 (optionnel)	✗ Aucun	SA v5 HMAC-SHA256	20000/TCP
MQTT 3.1.1	⚠ User/Pass optionnel	⚠ TLS optionnel	TLS 1.3 + cert client	1883/8883
MQTT 5.0	√ Enhanced Auth	⚠ TLS optionnel	TLS 1.3 + SASL/ SCRAM	1883/8883
IEC 61850 MMS	⚠ IEC 62351-4	⚠ TLS (IEC 62351-3)	IEC 62351 complet	102/TCP
OPC-UA	√ Cert X.509 natif	√ AES-256 natif	Natif, sans extension	4840/TCP



Formation et sensibilisation des équipes OT à la cybersécurité

Le facteur humain est souvent le maillon faible dans la sécurité OT. Les techniciens et ingénieurs OT, formés à la fiabilité des processus industriels, n'ont pas nécessairement de culture cybersécurité. Des comportements à risque courants incluent : l'utilisation de clés USB personnelles sur des postes de supervision pour transférer des fichiers de configuration, la connexion de postes de programmation au réseau OT et au Wifi personnel simultanément, la réutilisation de mots de passe simples ou par défaut sur les équipements, ou l'acceptation d'accès distants non planifiés de prestataires sans vérification formelle. La **sensibilisation spécifique OT** doit couvrir ces comportements à risque concrets, différenciée des formations cybersécurité IT

génériques qui ne parlent pas aux opérateurs. Des exercices de simulation (phishing ciblé, clé USB piégée déposée dans les locaux) permettent de mesurer la vulnérabilité et d'ancrer les bons réflexes. La formation de l'encadrement OT — chefs d'équipe, responsables de maintenance — est particulièrement importante car ils sont les décideurs des accès et des procédures au quotidien. En France, des organismes comme le CESI, l'IMT ou des cabinets spécialisés en sécurité industrielle proposent des formations certifiantes adaptées au personnel OT.

Historian industriel et sécurité des données OT

L'**historian industriel** — base de données temps réel stockant l'historique des mesures de processus (OSIsoft PI, GE Historian, Wonderware Historian) — est un composant OT à fort enjeu de sécurité, souvent positionné à la frontière IT/OT. Sa compromission permet à un attaquant de lire l'intégralité des données de processus (valeurs de capteurs, états d'équipements, événements d'alarmes) sur des mois ou des années, et potentiellement de modifier des données historiques — faussant les analyses et les décisions basées sur l'historique. La sécurisation de l'historian passe par l'authentification forte des accès (Active Directory avec MFA pour les interfaces d'administration), le chiffrement des communications côté OT (via des connecteurs sécurisés), le chiffrement de la base de données au repos, la séparation des rôles entre lecture et écriture, et un monitoring des accès inhabituels. La configuration de la connexion historian dans la DMZ OT (ni côté OT pur, ni côté IT) est l'architecture recommandée par l'ANSSI. AVEVA (ex-OSIsoft) PI System est l'historian industriel le plus utilisé en France, notamment dans les secteurs énergie et utilities, et a fait l'objet de plusieurs CVE significatives ces dernières années, justifiant un patch management rigoureux.

Détection d'anomalies comportementales dans les réseaux OT

Au-delà de la détection basée sur les signatures (IOC, règles de pare-feu), la **détection comportementale** est la technique la plus efficace pour identifier les menaces avancées dans les

réseaux OT. Les solutions de monitoring OT comme Claroty et Nozomi établissent des *baselines comportementales* : ils apprennent, pendant une période d'observation (typiquement 2-4 semaines), le comportement normal du réseau — quels équipements communiquent avec quels autres, sur quels protocoles, à quelle fréquence, avec quels codes de fonction Modbus ou quels types de messages DNP3. Tout écart significatif par rapport à cette baseline déclenche une alerte : un automate qui commence à communiquer avec une destination inconnue, un code de fonction Modbus inhabituel (écriture de registres quand seule une lecture est normale), une connexion hors des horaires d'exploitation habituels. Cette approche par baseline comportementale est particulièrement efficace contre les attaques lentes et furtives typiques des APT ciblant les infrastructures industrielles, qui évitent délibérément les comportements bruaux détectables par des règles statiques. La principale limite est le taux de faux positifs pendant la période d'apprentissage et lors des changements de configuration planifiés — une coordination entre les équipes OT et sécurité est indispensable pour contextualiser les alertes et éviter la fatigue d'alerte.

Continuité d'activité et reprise après sinistre OT

Les plans de **continuité d'activité (PCA)** et de **reprise après sinistre (PRA)** pour les systèmes OT doivent être conçus avec les contraintes spécifiques des environnements industriels. La sauvegarde des configurations d'automates est le premier élément : les projets TIA Portal (Siemens), Studio 5000 (Rockwell), Unity Pro (Schneider) doivent être sauvegardés régulièrement dans un coffre-fort numérique sécurisé, versionnés et testés pour assurer leur restaurabilité. La **documentation des configurations réseau** — adresses IP, VLAN, règles de pare-feu, configurations SCADA — doit être maintenue à jour et stockée hors-ligne. Des exercices de simulation de reprise après sinistre OT doivent être conduits régulièrement pour s'assurer que les équipes savent restaurer les systèmes dans un délai acceptable. Pour les sites critiques, des **configurations de recours** — des automates de substitution préconfigurés, prêts à être substitués en cas de panne — peuvent réduire significativement le délai de reprise. La coordination avec les fournisseurs d'équipements (Siemens, Schneider, Rockwell) pour les contrats de support d'urgence et les délais d'intervention est un élément essentiel du PRA OT.

Patch management OT : contraintes et stratégies

Le **patch management** dans les environnements OT est l'un des défis les plus complexes de la cybersécurité industrielle. Contrairement au monde IT où un patch peut être déployé en quelques heures avec un redémarrage rapide, les systèmes OT fonctionnent souvent en continu (24h/7j, 365 jours par an pour les sites critiques) avec des fenêtres de maintenance planifiées rares et courtes. La stratégie de patch management OT doit donc être conçue différemment. L'**inventaire continu** des équipements OT avec leurs versions firmware et logicielles est le prérequis indispensable — un inventaire souvent absent dans les sites industriels qui n'ont pas de solution de monitoring comme Claroty ou Nozomi. La **priorisation des patchs** doit intégrer les contraintes de disponibilité : un patch critique sur un automate gérant un processus en cours ne peut pas être appliqué immédiatement. Les **tests en environnement de qualification** sont indispensables avant déploiement en production, car un patch mal testé peut provoquer des incompatibilités avec des configurations spécifiques ou des régressions de performance. Les **fenêtres de maintenance planifiées** (arrêts annuels, arrêts de weekend pour les sites moins critiques) doivent être utilisées pour déployer les patchs prioritaires, avec coordination entre les équipes IT, OT et les fournisseurs d'équipements. Pour les vulnérabilités critiques ne pouvant pas être patchées immédiatement, des **mesures compensatoires** (segmentation réseau renforcée, monitoring accru, signatures IDS spécifiques) permettent de réduire le risque en attendant la fenêtre de maintenance.

Tests d'intrusion OT passifs : outils et méthodologie

Le test d'intrusion des réseaux OT nécessite une approche radicalement différente des pentests IT classiques. L'utilisation d'outils de scan agressifs (nmap avec des scripts NSE intrusifs, Metasploit sans précautions) sur des réseaux OT peut provoquer des pannes d'équipements, des déclenchements d'alarmes ou des arrêts de processus — des conséquences inacceptables. La règle d'or du pentest OT est la **passivité maximale** : préférer l'écoute passive à l'envoi de sondes actives. Des outils comme **Wireshark** avec des dissecteurs de protocoles industriels (Modbus, DNP3, IEC 61850, PROFINET) permettent de cartographier le réseau OT sans aucune

interaction. **Nmap** peut être utilisé avec des précautions extrêmes : vitesse de scan minimale (-T1 ou -T0), un seul port à la fois, sur des plages horaires avec opérateurs présents et prêts à intervenir. Des outils spécialisés comme **Redpoint NSE scripts** (NMAP NSE pour ICS) et **PLCscan** permettent d'identifier les équipements Siemens S7, Allen-Bradley et d'autres automates sans les perturber. Notre article détaillé sur le pentest industriel OT/ICS couvre l'ensemble de la méthodologie, des outils et des précautions opérationnelles.

Incidents réels OT en France : retour d'expérience 2024-2025

L'analyse des incidents cybersécurité OT documentés en France sur la période 2024-2025 révèle des patterns récurrents que les équipes de sécurité industrielle doivent anticiper. La majorité des compromissions initiales exploitent non pas les protocoles OT directement, mais les **points de jonction IT/OT** : postes de supervision connectés aux deux réseaux, VPN de télémaintenance mal configurés, ou accès distants d'intégrateurs tiers. Une fois dans le réseau IT, l'attaquant peut pivoter vers le réseau OT si la segmentation est insuffisante. L'exploitation de Modbus TCP ou DNP3 non authentifiés intervient dans un second temps, une fois l'accès au réseau OT obtenu. Un incident notable en 2025 dans une collectivité territoriale française a impliqué la compromission d'un système de gestion de l'eau via un VPN Fortinet non patché (CVE-2024-21762), donnant accès au réseau de supervision SCADA depuis lequel des automates de dosage étaient accessibles en Modbus TCP. La détection n'a eu lieu que deux semaines après la compromission initiale, grâce à une alerte CERT-FR. Cet incident illustre l'importance critique du patch management des équipements de frontière IT/OT et du monitoring continu des réseaux de supervision. Notre conviction, assumée : les organisations qui n'ont pas encore déployé de solution de monitoring passif OT en 2026 prennent un risque inacceptable face à la professionnalisation des groupes d'attaquants ciblant les infrastructures industrielles françaises.

Coûts d'un incident OT : impact financier et opérationnel

Contrairement aux incidents IT qui impactent principalement les données et la réputation, un incident cybersécurité OT peut provoquer des dommages physiques, des arrêts de production et des risques pour la sécurité des personnes. Les coûts d'un incident OT majeur comprennent plusieurs composantes. L'**arrêt de production** est la composante la plus immédiate : pour une usine de fabrication automobile, une heure d'arrêt non planifiée peut coûter entre 50 000 et 200 000 euros. Les **coûts de remédiation** sont plus élevés que dans le monde IT car le remplacement ou la reprogrammation des équipements OT (automates, IED) nécessite des techniciens spécialisés et des délais d'approvisionnement potentiellement longs. Les **dommages physiques** — équipements endommagés par des commandes malveillantes, voire destructions d'infrastructure — ajoutent une dimension supplémentaire. Les **risques réglementaires** : pour les OIV et OSE, un incident OT mal géré peut déclencher des sanctions NIS 2 et des obligations de reporting contraignantes. Le contexte assurantiel OT évolue rapidement : les assureurs cyber imposent désormais des preuves de segmentation IT/OT et de monitoring actif comme condition de souscription pour les sites industriels. Notre guide cyber assurance 2026 détaille les critères spécifiques aux environnements OT.

Perspectives : convergence IT/OT et Zero Trust industriel

La tendance de fond pour les architectures OT en 2026 est la convergence progressive des pratiques de sécurité IT et OT, sous l'impulsion des initiatives IIoT et Industrie 4.0. Le concept de **Zero Trust**, longtemps considéré comme incompatible avec les contraintes OT (latence, équipements legacy), fait l'objet d'adaptations pragmatiques. Le **Zero Trust OT** ne signifie pas l'abandon du modèle périphérique zones/conduits, mais son enrichissement par des mécanismes d'authentification forte pour les accès humains et machine, la micro-segmentation au niveau des équipements les plus critiques, et la surveillance comportementale continue. Des solutions comme **Claroty xDome** et **Armis** permettent d'appliquer des principes Zero Trust aux équipements OT existants sans modification des équipements eux-mêmes. L'enjeu des prochaines années pour les équipes de sécurité industrielle sera de concilier cette modernisation

avec la contrainte fondamentale de disponibilité — une évolution qui nécessite une collaboration renforcée entre les équipes IT, OT et les fournisseurs d'équipements industriels. Pour les nouveaux projets industriels (Greenfield), l'intégration de la sécurité dès la conception (Security by Design) et le choix de protocoles natifs sécurisés comme OPC-UA permettent d'éviter les dettes techniques sécurité qui pèsent sur les installations existantes.

Pour approfondir la sécurité de vos environnements industriels, consultez notre guide sur le pentest OT/ICS, notre article sur la sécurité des passerelles et protocoles OT, notre comparatif des outils open source pour le SOC OT, ainsi que notre analyse de la cyber assurance pour les sites industriels. Côté normes, les ressources de l'ANSSI (guides ICS) et de la norme IEC 62443 (ISA) sont les références incontournables pour la cybersécurité industrielle en France.