AYI NEDJIMI Consultants

Architecture sécurité OT/IT convergente et segmentation

Catégorie : Sécurité Industrielle OT/ICS Lecture : 8 min Publié le : 12/03/2026 Auteur : Ayi NEDJIMI

Guide complet sur l'architecture sécurité OT/IT convergente : segmentation par zones, modèle Purdue, DMZ industrielle et bonnes pratiques 2026.

Résumé exécutif

La convergence des réseaux OT (Operational Technology) et IT (Information Technology) expose les systèmes industriels à des menaces cyber croissantes qui nécessitent une refonte architecturale complète. Ce guide détaille les architectures de segmentation par zones et conduits selon le modèle Purdue révisé et la norme IEC 62443, avec des recommandations concrètes pour déployer une DMZ industrielle robuste, des pare-feu de nouvelle génération capables d'inspecter les protocoles OT, et des stratégies de micro-segmentation adaptées aux contraintes de disponibilité des environnements de production industrielle. Chaque niveau de l'architecture Purdue fait l'objet de recommandations spécifiques de sécurisation, du niveau 0 des capteurs et actionneurs jusqu'au niveau 5 des systèmes d'entreprise, en passant par la DMZ industrielle critique qui constitue le point névralgique de toute architecture convergente OT/IT sécurisée face aux cybermenaces modernes ciblant les infrastructures industrielles critiques.

La transformation numérique des sites industriels accélère la fusion entre les réseaux de technologie opérationnelle et les systèmes d'information traditionnels. Cette convergence OT/IT, portée par la quête de gains de productivité et de supervision centralisée, crée simultanément une surface d'attaque élargie que les architectes sécurité doivent impérativement maîtriser. Les automates programmables, les systèmes SCADA et les capteurs IoT industriels, historiquement isolés sur des réseaux propriétaires, se retrouvent désormais interconnectés avec des plateformes cloud, des ERP et des outils de business intelligence. Cette exposition nouvelle exige une refonte fondamentale des architectures réseau selon des principes de défense en profondeur, de segmentation stricte et de contrôle des flux entre zones de confiance distinctes. Le modèle Purdue, référence historique de l'architecture industrielle, doit être repensé à l'aune des menaces modernes et des exigences réglementaires comme NIS 2 et IEC 62443, tout en préservant la disponibilité opérationnelle qui reste la priorité absolue en environnement OT. Les secteurs de l'énergie, de la chimie, du traitement de l'eau et des transports sont particulièrement concernés par cette problématique de convergence sécurisée, chaque secteur présentant des contraintes opérationnelles spécifiques qui influencent directement les choix architecturaux en matière de segmentation et de contrôle d'accès réseau.

Le modèle Purdue révisé pour la convergence OT/IT

Le **modèle Purdue** (ISA-95) structure l'architecture industrielle en niveaux hiérarchiques, du processus physique (niveau 0) jusqu'aux systèmes d'entreprise (niveau 5). Dans sa version traditionnelle, ce modèle reposait sur un air-gap entre les niveaux OT (0-3) et IT (4-5). La convergence impose un nouveau paradigme où la **DMZ industrielle** (niveau 3.5) devient le point névralgique de l'architecture sécuritaire.

Cette DMZ ne se limite pas à un simple pare-feu : elle constitue une zone tampon où transitent les données de production vers les systèmes IT via des mécanismes de rupture protocolaire, des serveurs relais et des diodes de données. Les flux doivent être strictement unidirectionnels lorsque possible, et chaque connexion bidirectionnelle nécessaire doit faire l'objet d'une analyse de risque documentée selon les principes de segmentation réseau et Zero Trust.

Le niveau 2 (systèmes de supervision HMI, serveurs historiens) et le niveau 1 (automates PLC, RTU) requièrent des protections spécifiques. Chaque niveau forme une zone de sécurité avec des conduits contrôlés vers les niveaux adjacents. La communication directe entre niveaux non adjacents constitue une violation architecturale à proscrire absolument.

Mon avis : Trop d'organisations déploient une DMZ industrielle de façade, avec un unique pare-feu entre IT et OT, sans réelle rupture protocolaire. Cette approche offre une illusion de sécurité. La vraie segmentation exige des investissements conséquents en infrastructure et en compétences, mais le coût d'un incident majeur sur un site de production justifie largement cet effort.

Zones et conduits IEC 62443 : mise en œuvre pratique

La norme **IEC 62443** formalise le concept de zones et conduits. Une zone regroupe des actifs partageant un même niveau de sécurité requis (Security Level, SL). Un conduit représente le canal de communication entre deux zones, avec ses propres exigences de protection. La démarche consiste à cartographier l'ensemble des actifs OT, les regrouper en zones cohérentes, puis définir les conduits nécessaires avec leurs contrôles associés.

En pratique, la segmentation par zones s'appuie sur des **VLAN industriels**, des pare-feu de nouvelle génération capables d'inspecter les protocoles OT (Modbus TCP, EtherNet/IP, OPC UA), et des listes de contrôle d'accès granulaires. Chaque zone se voit attribuer un Security Level cible (SL-T) de 1 à 4, déterminé par l'analyse de risque. Les conduits entre zones doivent garantir que les flux traversants ne dégradent pas le SL de la zone destination. Pour approfondir les méthodologies d'évaluation, consultez notre guide sur le pentest infrastructure et ses outils.

Zone Purdue	Actifs typiques	SL recommandé	Contrôles clés
Niveau 0-1	PLC, RTU, capteurs	SL 3-4	Whitelisting applicatif, contrôle physique
Niveau 2	HMI, SCADA, historien	SL 2-3	Pare-feu OT, surveillance réseau
Niveau 3	Serveurs de site, MES	SL 2-3	Antivirus, gestion des correctifs
DMZ (3.5)	Serveurs relais, jump hosts	SL 3	Rupture protocolaire, diodes
Niveau 4-5	ERP, Cloud, bureautique	SL 1-2	Contrôles IT standards

Comment déployer une DMZ industrielle efficace ?

Le déploiement d'une **DMZ industrielle** robuste repose sur plusieurs composants essentiels. Le premier élément est la paire de pare-feu : un pare-feu orienté IT en bordure haute et un pare-feu orienté OT en bordure basse, idéalement de constructeurs différents pour éviter qu'une vulnérabilité unique ne compromette les deux barrières. Entre ces pare-feu, les serveurs relais assurent la rupture protocolaire.

Les serveurs historiens miroirs dans la DMZ reçoivent les données de production et les mettent à disposition des systèmes IT sans connexion directe vers le réseau OT. Les solutions de type Claroty ou Nozomi Networks permettent une visibilité complète des flux OT traversant la DMZ. Les jump hosts sécurisés, avec authentification multifacteur et enregistrement de session, constituent le seul point d'accès distant autorisé vers les systèmes OT pour la maintenance. Chaque accès distant doit être tracé et limité dans le temps, conformément aux recommandations de l'ANSSI pour les systèmes industriels critiques.

Lors de l'attaque contre le réseau électrique ukrainien en décembre 2015, les attaquants ont exploité l'absence de segmentation entre les réseaux IT et OT pour atteindre les systèmes SCADA depuis des postes de travail bureautiques compromis par du spear-phishing. Une DMZ industrielle correctement implémentée avec rupture protocolaire aurait considérablement ralenti la progression latérale des attaquants entre les niveaux du réseau.

Pourquoi la micro-segmentation change la donne en OT ?

Au-delà de la segmentation macro par zones Purdue, la **micro-segmentation** applique des politiques de contrôle d'accès au niveau de chaque actif ou groupe d'actifs OT. Cette approche, inspirée du Zero Trust, devient réalisable grâce aux solutions de surveillance réseau OT qui cartographient automatiquement les communications légitimes entre automates, HMI et serveurs.

La micro-segmentation en OT diffère significativement de son équivalent IT. Les communications entre automates suivent des patterns extrêmement prévisibles et stables : un PLC communique avec un ensemble fixe de périphériques selon des cycles déterministes. Cette prévisibilité facilite la création de règles de whitelisting précises. En revanche, la tolérance aux faux positifs est quasi nulle : bloquer une communication légitime entre un automate et un capteur de sécurité peut provoquer un arrêt de production voire un incident de sûreté.

L'approche par SOC et architecture de supervision doit intégrer ces contraintes spécifiques OT. Les solutions de micro-segmentation OT comme celles de Guardicore (désormais Akamai) ou Illumio s'adaptent progressivement aux environnements industriels, offrant une visibilité granulaire sur les flux entre automates et permettant l'application de politiques de segmentation sans modification de l'infrastructure réseau sous-jacente. Cette approche software-defined facilite le déploiement itératif, commençant en mode monitoring avant d'activer le blocage des flux non conformes après validation par les équipes OT.

Avez-vous déjà audité la matrice de flux réels entre vos automates et comparé avec les flux théoriquement autorisés ?

Quelles erreurs éviter lors de la segmentation OT/IT ?

La première erreur fréquente consiste à déployer un unique *pare-feu* entre IT et OT sans véritable DMZ. Cette configuration en « flat network » segmenté offre une protection minimale : une fois le pare-feu traversé, l'attaquant dispose d'un accès complet au réseau OT. La deuxième erreur est l'utilisation de règles pare-feu trop permissives (any-to-any sur certains ports) pour « ne pas perturber la production ». Ces règles doivent être resserrées progressivement en mode apprentissage.

La troisième erreur critique est l'absence de **supervision des flux OT**. Sans visibilité sur les communications réseau industrielles, il est impossible de détecter un comportement anormal. Les outils de Network Detection and Response (NDR) spécialisés OT, déployés en mode passif via des ports miroir, apportent cette visibilité sans risque d'impact sur la production. Quatrièmement, négliger la segmentation interne au sein même du réseau OT : les communications entre sous-systèmes indépendants (par exemple, entre l'atelier peinture et l'atelier assemblage) doivent être cloisonnées. La mise en place d'une architecture de log management adaptée aux environnements industriels complète cette stratégie de détection.

Faut-il adopter le SASE pour les sites industriels distants ?

Le modèle **SASE** (Secure Access Service Edge) séduit pour les sites industriels distants (stations de pompage, sous-stations électriques, sites éoliens). Ces sites, souvent dépourvus d'expertise sécurité locale, bénéficieraient d'une gestion centralisée des politiques de sécurité via le cloud. Les solutions SD-WAN industrielles intègrent désormais des fonctions de segmentation et de chiffrement adaptées aux protocoles OT.

Toutefois, la dépendance à une connectivité internet fiable pour accéder aux fonctions de sécurité cloud pose un risque de disponibilité en environnement OT. La latence introduite par le routage via un point de présence cloud peut être incompatible avec certains protocoles industriels temps réel. L'approche hybride, combinant un *appliance de sécurité locale* pour les fonctions critiques avec une orchestration SASE pour la gestion des politiques et la télémétrie, représente le meilleur compromis actuel pour les architectures multi-sites.

Comment mesurer l'efficacité de la segmentation OT ?

L'évaluation de l'efficacité de la segmentation repose sur des indicateurs objectifs. Le **taux de conformité des flux** mesure le pourcentage de communications réseau OT correspondant aux flux autorisés dans la politique de segmentation. Toute communication non référencée doit être analysée et soit légitimée soit bloquée. Le temps moyen de détection d'un flux anormal (MTTD) et le temps de blocage (MTTR) constituent des métriques opérationnelles essentielles.

Les exercices de *tabletop* et les tests d'intrusion réguliers valident la résistance de la segmentation face à des scénarios d'attaque réalistes. La méthodologie de threat hunting adaptée aux environnements OT permet de rechercher proactivement des indicateurs de compromission traversant les frontières de zones. Les rapports de conformité IEC 62443 et les audits ANSSI fournissent un cadre formel pour cette évaluation continue.

À retenir : Une architecture OT/IT sécurisée repose sur trois piliers : une segmentation hiérarchique selon le modèle Purdue révisé, une DMZ industrielle avec rupture protocolaire réelle, et une micro-segmentation progressive basée sur les flux légitimes observés. La supervision continue des communications OT est indispensable pour maintenir l'efficacité de cette segmentation dans le temps.

Sources et références : CISA ICS · ANSSI

Quelles technologies de diode de données pour la DMZ OT ?

Les **diodes de données** constituent la solution la plus robuste pour garantir l'unidirectionnalité des flux entre le réseau OT et la DMZ industrielle. Contrairement à un pare-feu configuré en mode unidirectionnel, une diode de données repose sur une contrainte physique (fibre optique unidirectionnelle) qui rend tout flux retour physiquement impossible. Les solutions comme Waterfall Security, Owl Cyber Defense et Fox-IT DataDiode sont déployées dans les environnements les plus critiques : centrales nucléaires, infrastructures militaires et sites de production chimique à haut risque Seveso.

Le déploiement de diodes de données nécessite une adaptation des applications qui traversent la frontière OT/IT. Les protocoles bidirectionnels comme OPC UA doivent être encapsulés via des agents spécialisés situés de part et d'autre de la diode. Les données de l'historien OT sont répliquées vers un historien miroir dans la DMZ via un flux unidirectionnel, rendant disponibles les données de production aux systèmes IT sans jamais exposer le réseau OT à un flux entrant. Cette approche, combinée aux principes de disaster recovery adaptés aux environnements industriels, garantit à la fois la sécurité et la continuité opérationnelle des systèmes de contrôle. Les organisations exploitant des systèmes certifiés IEC bénéficient de guides de déploiement spécifiques pour l'intégration de diodes de données dans leurs architectures de zone et conduit existantes, assurant une compatibilité avec les exigences normatives en vigueur.

Ayi NEDJIMI Consultants — Expert cybersécurité offensive & intelligence artificielle

ayinedjimi-consultants.fr · ayi@ayinedjimi-consultants.fr