AYI NEDJIMI Consultants

Air-gap et isolation réseau mythes et réalités en OT

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

Analyse critique de l'air-gap en environnement OT : mythes de l'isolation réseau, canaux de contournement, diodes de données et alternatives.

Résumé exécutif

L'air-gap, séparation physique totale entre les réseaux OT et IT, est souvent présenté comme la solution ultime et incontournable de sécurité industrielle par les équipes d'exploitation. La réalité est considérablement plus nuancée : les air-gaps véritables sont extrêmement rares dans les installations industrielles modernes où les besoins de remontée de données de production et de maintenance distante créent des connexions permanentes, les canaux de contournement physiques comme les clés USB sont nombreux et difficiles à contrôler, et les besoins légitimes de connectivité des sites industriels modernes rendent l'isolation totale incompatible avec les exigences opérationnelles et réglementaires. Ce guide analyse les mythes et réalités de l'air-gap en OT, les techniques de contournement documentées depuis Stuxnet, et propose des alternatives pragmatiques comme les diodes de données.

Le mythe de l'air-gap persiste dans la communauté industrielle comme une solution miracle de cybersécurité : si le réseau OT est physiquement déconnecté de tout autre réseau, aucune cyberattaque ne peut l'atteindre. Cette conviction, rassurante dans sa simplicité, se heurte à trois réalités incontournables. Premièrement, les air-gaps véritables sont extrêmement rares dans les installations industrielles modernes, les besoins de remontée de données de production, de maintenance distante et de mise à jour créant des connexions permanentes ou temporaires qui brisent l'isolation. Deuxièmement, même un air-gap authentique peut être contourné par des vecteurs physiques comme les clés USB, les ordinateurs portables de maintenance et les supports de transfert de données utilisés quotidiennement par les techniciens. Troisièmement, l'attaque Stuxnet a démontré de manière spectaculaire qu'un air-gap ne protège pas contre un attaquant suffisamment déterminé et doté de ressources étatiques, le malware ayant traversé l'air-gap des installations nucléaires iraniennes via des clés USB infectées introduites par des techniciens manipulés ou inconscients. Repenser la stratégie de protection OT au-delà du mythe de l'air-gap constitue un impératif pour les architectes sécurité industrielle qui doivent combiner défense en profondeur, surveillance active et contrôle des vecteurs physiques dans une approche réaliste et durable de la sécurisation des systèmes de contrôle critiques.

Le faux sentiment de sécurité de l'air-gap

Les audits de sécurité industrielle révèlent régulièrement que les **air-gaps supposés** n'existent pas réellement. Un réseau OT déclaré « air-gappé » dans la documentation d'architecture présente fréquemment des connexions non documentées : un câble réseau reliant un poste d'ingénierie au réseau IT pour les mises à jour antivirus, un modem 4G installé sur un commutateur pour la maintenance distante, une connexion WiFi configurée par un technicien pour accéder à la documentation en ligne depuis le réseau OT.

La première action lors d'un audit OT consiste à vérifier empiriquement l'existence réelle de l'air-gap déclaré. Un scan réseau depuis le réseau IT révèle souvent des dispositifs OT accessibles. L'analyse du trafic réseau sur les commutateurs de la prétendue DMZ montre des flux bidirectionnels non filtrés. Les clés USB circulent quotidiennement entre les postes IT et les stations d'ingénierie OT, transférant non seulement des fichiers de projet mais potentiellement des malwares. La segmentation réseau et l'approche Zero Trust offrent une protection plus réaliste et vérifiable qu'un air-gap théorique non maintenu dans le temps.

Stuxnet a franchi l'air-gap des installations d'enrichissement d'uranium de Natanz en Iran via des clés USB infectées. Le malware exploitait quatre vulnérabilités zero-day Windows pour se propager automatiquement dès l'insertion de la clé USB dans un poste connecté au réseau OT. Une fois à l'intérieur du réseau isolé, Stuxnet se propageait latéralement via les partages réseau et le protocole WinCC de Siemens pour atteindre les automates S7-300 contrôlant les centrifugeuses, démontrant qu'un air-gap physique ne constitue qu'un obstacle supplémentaire pour un attaquant étatique déterminé, et non une barrière infranchissable.

Quels canaux de contournement de l'air-gap existent ?

Les **canaux de contournement** de l'air-gap se classent en deux catégories : les vecteurs physiques conventionnels et les canaux auxiliaires exotiques. Les vecteurs physiques représentent la menace la plus réaliste : clés USB et supports amovibles (vecteur de Stuxnet), ordinateurs portables de maintenance connectés alternativement aux réseaux IT et OT (bridge involontaire), équipements de constructeurs livrés avec des malwares pré-installés (supply chain attack), et modems cellulaires ajoutés par les techniciens pour faciliter la maintenance distante.

Les canaux auxiliaires exotiques, documentés dans la littérature académique, exploitent les émanations physiques des systèmes pour transmettre des données à travers l'air-gap : émissions électromagnétiques des câbles réseau (*AirHopper*), modulation de la luminosité des LED de status des commutateurs réseau (aIR-Jumper), émissions acoustiques des disques durs (DiskFiltration), et variation de la consommation électrique (PowerHammer). Ces techniques, bien que spectaculaires, présentent des débits très faibles et sont principalement pertinentes pour l'exfiltration de données sensibles plutôt que pour l'injection de commandes dans les systèmes OT. La menace réaliste reste les vecteurs physiques conventionnels, contre lesquels des contrôles stricts doivent être déployés.

Vecteur de contournement	Réalisme	Débit	Contre-mesure
Clé USB infectée	Très élevé	Illimité	Kiosques de décontamination
Laptop de maintenance	Élevé	Illimité	Postes dédiés OT, pas de dual-use
Modem cellulaire caché	Moyen	Élevé	Audit physique, détection RF
Supply chain compromise	Moyen	Variable	Vérification intégrité livraisons
Canaux EM/acoustiques	Faible	Très faible	Blindage, bruit de fond

Mon avis : L'air-gap est devenu un mythe dangereux en cybersécurité OT. Il procure un faux sentiment de sécurité qui décourage les investissements dans la surveillance réseau, la détection d'intrusion et la gestion des vulnérabilités, sous prétexte que « le réseau est isolé ». Un réseau OT correctement segmenté, surveillé et durci est objectivement plus sûr qu'un réseau prétendument air-gappé mais non surveillé, non mis à jour et traversé quotidiennement par des clés USB non contrôlées.

Comment sécuriser les transferts physiques vers le réseau OT ?

Les **kiosques de décontamination USB** constituent la première ligne de défense contre les vecteurs physiques. Ces dispositifs, déployés à l'entrée de la zone OT, analysent le contenu de chaque support amovible avec plusieurs moteurs antimalware avant d'autoriser son utilisation sur le réseau industriel. Les solutions comme OPSWAT MetaDefender Kiosk ou Honeywell Secure Media Exchange appliquent une analyse multi-moteurs (typiquement 8 à 12 antivirus) et peuvent convertir les fichiers dans des formats sûrs (Content Disarm and Reconstruction, CDR) pour éliminer les charges malveillantes intégrées dans des documents.

Les *postes de transfert sécurisés*, positionnés dans une zone intermédiaire contrôlée physiquement, servent de sas entre le monde IT et le réseau OT. Ces postes, durcis et non connectés à aucun réseau, permettent de transférer des fichiers de projet, des mises à jour logicielles et des correctifs de sécurité via un processus en deux étapes : dépôt sur le poste de transfert depuis le côté IT, analyse et validation, puis récupération depuis le côté OT. L'intégration avec les processus de détection engineering garantit que chaque transfert est journalisé et analysable en cas d'incident.

Disposez-vous d'un processus formalisé de décontamination des supports USB avant leur utilisation sur votre réseau OT ?

Pourquoi les diodes de données supplantent l'air-gap ?

Les **diodes de données** offrent le meilleur compromis entre sécurité et connectivité pour les environnements OT critiques. Contrairement à l'air-gap qui bloque toute communication, la diode autorise un flux de données strictement unidirectionnel (OT vers IT) tout en garantissant physiquement l'impossibilité de tout flux inverse. Cette garantie repose sur un principe physique (fibre optique sans récepteur côté OT) et non sur une configuration logicielle potentiellement contournable.

Les cas d'usage des diodes de données en environnement OT incluent la réplication des données de l'historien de production vers les systèmes IT pour le reporting et l'analyse, l'export des logs et événements de sécurité vers le SIEM pour la surveillance, et la transmission de données de supervision vers des centres de contrôle distants. Les principales solutions du marché (Waterfall Security, Owl Cyber Defense, solutions qualifiées ANSSI) intègrent des agents applicatifs qui encapsulent les protocoles OT pour la transmission à travers la diode, supportant OPC UA, Modbus, historiens PI et OSIsoft, et syslog. Le déploiement d'une diode nécessite une adaptation de l'architecture applicative mais offre une garantie de sécurité supérieure à tout pare-feu, et la gestion des logs peut être assurée via ce canal unidirectionnel sécurisé.

Faut-il abandonner complètement le concept d'air-gap ?

Le concept d'air-gap conserve sa pertinence pour les systèmes les plus critiques où aucun besoin de connectivité n'est justifiable. Les **systèmes instrumentés de sécurité** (SIS), conçus pour protéger les vies humaines en cas de défaillance du système de contrôle, doivent idéalement être isolés physiquement du réseau de contrôle et a fortiori du réseau IT. L'attaque Triton a ciblé précisément le SIS, démontrant que même ces systèmes de dernière protection attirent l'attention des attaquants les plus sophistiqués.

Pour les systèmes de contrôle-commande nécessitant une remontée de données vers l'IT, l'approche recommandée remplace l'air-gap par une **architecture de défense en profondeur** combinant diodes de données pour les flux unidirectionnels, DMZ industrielle avec rupture protocolaire pour les flux nécessairement bidirectionnels, surveillance réseau passive sur chaque segment, et contrôle strict des vecteurs physiques. Cette architecture, conforme aux exigences de la norme IEC 62443 et vérifiable par audit, offre une protection supérieure à un air-gap théorique non maintenu dans la réalité opérationnelle. Le cadre de MITRE ATT&CK for ICS aide à valider que cette architecture couvre les techniques d'attaque documentées contre les systèmes de contrôle industriels.

Comment auditer l'efficacité réelle de l'isolation réseau OT ?

L'audit de l'isolation réseau OT combine des **techniques actives et passives** pour vérifier empiriquement l'absence de connexions non documentées. L'analyse du trafic réseau sur chaque interface des commutateurs OT révèle les flux réels, potentiellement différents des flux théoriques documentés dans l'architecture. Les outils de découverte réseau passive comme ceux de Nozomi Networks identifient chaque dispositif communiquant sur le réseau OT et cartographient les interconnexions, révélant les ponts réseau non documentés.

L'audit physique des infrastructures complète l'analyse réseau. L'inspection des armoires réseau OT vérifie l'absence de modems cellulaires non autorisés, de câbles réseau non documentés reliant des commutateurs OT à l'infrastructure IT, et de points d'accès WiFi bridgeant les deux réseaux. La détection de *signaux radiofréquence* dans les zones OT identifie les communications sans fil non autorisées (WiFi, Bluetooth, cellulaire) qui contournent l'isolation réseau. Les

résultats de ces audits alimentent le processus d'amélioration continue de l'architecture de segmentation, en cohérence avec les principes de pentest infrastructure adaptés aux spécificités des environnements industriels critiques.

Sources et références : CISA ICS · ANSSI

Quelles politiques de gestion des supports amovibles en zone OT ?

La gestion stricte des **supports amovibles** constitue le contrôle le plus critique pour maintenir l'intégrité de l'isolation OT. La politique de sécurité doit définir clairement quels types de supports sont autorisés (clés USB chiffrées d'entreprise uniquement, pas de supports personnels), le processus obligatoire de décontamination avant utilisation en zone OT, la traçabilité de chaque utilisation (qui, quand, quels fichiers) et les sanctions en cas de non-respect des procédures.

Les **stations de décontamination** positionnées physiquement à l'entrée de chaque zone OT appliquent une analyse multi-moteurs antimalware et un processus de Content Disarm and Reconstruction (CDR) transformant les fichiers dans des versions sûres. Les fichiers exécutables sont systématiquement bloqués ; seuls les formats de données autorisés (fichiers de projet automate, configurations, documentation) transitent vers le réseau OT. Le registre de traçabilité des transferts, intégré dans la plateforme de log management, fournit une piste d'audit exploitable en cas d'investigation forensique pour reconstituer le vecteur d'introduction d'un éventuel malware dans l'environnement OT protégé par ces mesures de contrôle des supports amovibles.

À retenir : L'air-gap véritable est rare en pratique et contournable par des vecteurs physiques comme l'a démontré Stuxnet. Les diodes de données offrent une alternative supérieure pour les flux unidirectionnels, tandis que la défense en profondeur (segmentation, DMZ, surveillance, contrôle des supports amovibles) assure une protection vérifiable et maintenue dans le temps. La sécurité OT réelle repose sur des contrôles actifs et vérifiables, pas sur l'absence supposée de connexion.

La stratégie de protection post-air-gap doit également intégrer la surveillance des accès physiques aux zones OT. Les systèmes de contrôle d'accès par badge, les caméras de surveillance et les registres de visiteurs tracent les entrées dans les zones contenant des systèmes de contrôle industriels. La corrélation entre les événements d'accès physique et les activités réseau OT permet de détecter des schémas suspects, comme un accès physique non planifié suivi d'une modification de configuration d'automate, renforçant la posture globale de détection au-delà de la seule surveillance réseau.

Ayi NEDJIMI Consultants — Expert cybersécurité offensive & intelligence artificielle

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