AYI NEDJIMI Consultants

IA et SCADA/ICS : Détection d'Anomalies sur les Protocoles

Catégorie : Intelligence Artificielle Lecture : 2 min Publié le : 28/02/2026 Auteur : Ayi NEDJIMI

Modèles ML pour la détection d'anomalies sur Modbus, OPC-UA, DNP3 en environnement OT. Autoencoders, isolation forest et solutions Claroty, Nozomi.

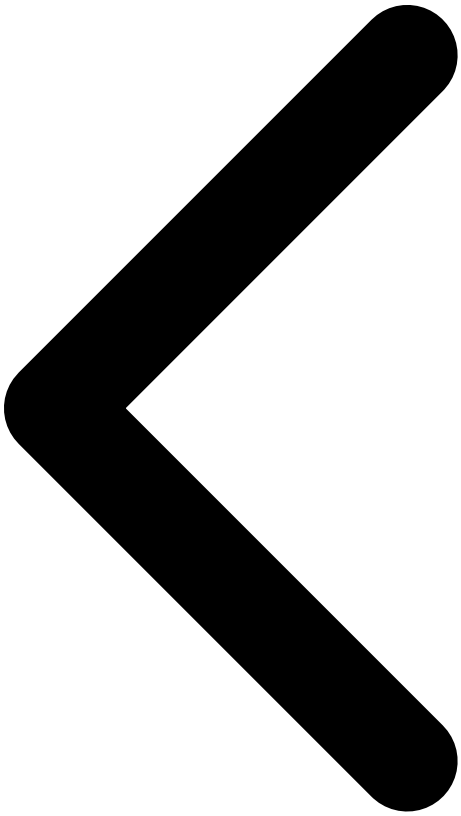
Le déploiement de solutions de détection d'anomalies par IA en environnement OT est soumis à des **contraintes architecturales drastiques** que l'on ne rencontre pas dans le monde IT. Le principe fondamental est que la solution de sécurité ne doit en aucun cas perturber le processus industriel — la disponibilité prime sur tout. Modèles ML pour la détection d'anomalies sur Modbus, OPC-UA, DNP3 en environnement OT. Autoencoders, isolation forest et solutions Claroty, Nozomi. Dans un contexte où l'intelligence artificielle transforme les pratiques de cybersécurité, la maîtrise de ia scada ics detection anomalies devient un avantage stratégique pour les équipes techniques. Les professionnels y trouveront des recommandations actionnables, des commandes prêtes à l'emploi et des stratégies de mise en œuvre adaptées aux environnements d'entreprise.

Monitoring passif et architecture de référence

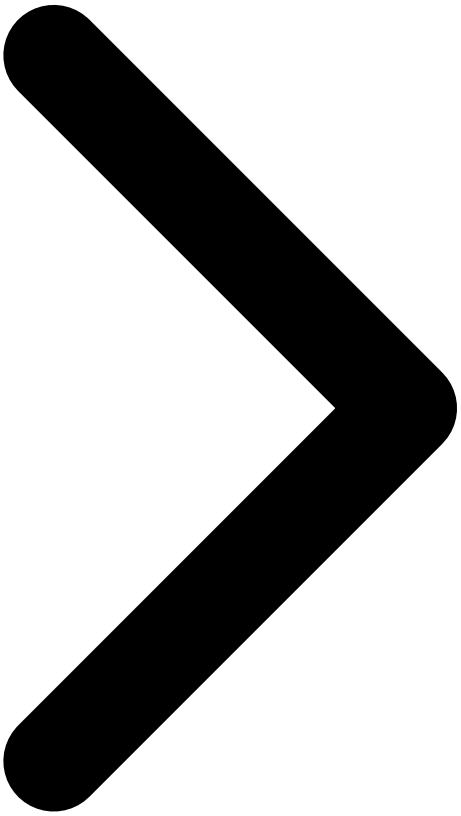
Le déploiement en environnement OT repose sur le **monitoring passif** via des TAP réseau (Test Access Point) ou des ports SPAN/mirror sur les switchs industriels. Le capteur de la solution ML reçoit une copie du trafic réseau sans aucune interaction avec les flux de production. Cette architecture est non intrusive, invisible pour les automates et stations SCADA, et ne peut en aucun cas provoquer de perturbation du processus industriel. Le capteur ML opère typiquement dans la zone DMZ industrielle (niveau 3.5 du modèle Purdue), avec une **diode de données unidirectionnelle** pour les installations les plus sensibles (nucléaire, défense) garantissant physiquement l'impossibilité de toute communication depuis le réseau IT vers le réseau OT. Les modèles de ML sont entraînés on-premise, sans aucun envoi de données vers le cloud, et les mises à jour logicielles sont déployées via des supports amovibles vérifiés selon des procédures strictes.

Les contraintes matérielles sont également spécifiques. Les capteurs doivent fonctionner dans des **environnements industriels** (température étendue -40/+70C, vibrations, poussière, compatibilité électromagnétique) et supporter les débits des réseaux industriels sans perte de

paquets. Les modèles de ML doivent s'exécuter sur du hardware embarqué (Intel Atom, ARM industriel) avec des contraintes de mémoire et de calcul significatives. C'est pourquoi les modèles légers (Isolation Forest, arbres de décision optimisés, réseaux de neurones compacts) sont privilégiés par rapport aux architectures deep learning lourdes. La **latence de détection** est un critère critique : pour être utile, une alerte doit être générée en quelques secondes, pas en quelques minutes — le temps de réaction d'un opérateur face à une anomalie sur un processus chimique se mesure en secondes.



Détection Anomalies Architecture Air-Gapped Solutions



Sources et références : ArXiv IA · Hugging Face Papers

Articles connexes

- Détection de Menaces par IA : SIEM Augmenté : Guide
- AI Act et LLM : Classifier vos Systèmes IA : Guide Complet
- IA pour la Génération de Code : Copilot, Cursor, Claude
- Data Platform IA-Ready : Architecture de Référence 2026

Ayi NEDJIMI Consultants — Expert cybersécurité offensive & intelligence artificielle

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