Cybersécurité

Performance industrielle

Cyberrésillience et monitoring OT

L'analyse des données brutes de vos équipements industriels

Les équipements industriels sont robustes, mais pas suffisamment sécurisés

Vous êtes RSSI, DSI ou expert cyber OT ?
Connaissez-vous toutes les failles de cybersécurité dans votre usine ?

- → Les automates ne remontent pas toutes les données critiques.
- → Les données sont prétraitées et peuvent être falsifiées.
- → Les solutions IT ne voient pas les signaux terrain falsifiés.
- → Personne ne vérifie aujourd'hui les signaux physiques du système.
- → Il n'existe aucun moyen de vérifier l'intégrité des commandes envoyées à vos actionneurs.

+53%

d'augmentation annuelle moyenne des cyberattaques OT (2021 - 2023)

73

attaques industrielles recensées chaque mois en 2023

3 jours

pour stabiliser un système après une attaque, et des semaines de pertes d'exploitation

Quelles sont les conséquences d'une cyberattaque pour votre usine ?

Quand une cyberattaque passe inaperçue, les conséquences peuvent être lourdes pour votre production. Et pourtant, de nombreux signaux critiques restent invisibles pour les systèmes IT ou SCADA.

Impact opérationnel

Baisse de qualité

Cycle de commande faussé

Impact économique

Temps de diagnostic allongé

Semaines de pertes d'exploitation

Impact industriel

Détérioration d'équipements

Non-conformité réglementaire

L'industrie manque de données terrain fiables et exploitables

Ces données sont cruciales pour optimiser la performance d'une ligne de production. Sans elles, les dérives lentes, signaux faibles ou anomalies de consommation passent souvent inaperçus.

- → Pas de visibilité temps réel sur les équipements
- → Aucune alerte sur les dérives machines
- → Données énergétiques peu exploitables
- → Décisions prises sans données fiables
- → Diagnostic difficile des pannes et micro-arrêts

16%
des sites industriels seulement disposent d'une visibilité en temps réel sur l'ensemble de leurs processus de fabrication. (USA)

70%
des industries gèrent encore des données manuellement malgré l'augmentation de la collecte de données. (USA)

39%
des sites industriels seulement ont réussi à industrialiser une stratégie data au-delà d'un seul produit. (Grands groupes, monde)

Quelles sont les risques sur les opérations de votre usine ?

Dans l'atelier, chaque machine, chaque cycle et chaque signal comptent.
Mais sans données terrain fiables, les anomalies restent invisibles et les conséquences s'accumulent.

Impact opérationnel

Maintenance réactive uniquement

Temps d'arrêt sous-estimés

Impact économique

Surconsommation énergétique

Productivité dégradée

Impact industriel

Pas d'amélioration continue

Usure prématurée des équipements

NOTRE SOLUTION : SURVEILLER LES SIGNAUX ÉLECTRIQUES DES ÉQUIPEMENTS INDUSTRIELS

La seule solution non intrusive et modulaire capable de détecter les commandes industrielles falsifiées ou érronées

Captez les signaux bruts de vos équipements OT, détectez les anomalies invisibles (dérives techniques, commandes erronées ou cyberattaques) pour renforcer la sécurité, la performance et la disponibilité de vos installations industrielles.

NOTRE SOLUTION : 3 ÉTAPES

Comment fonctionne la solution AIoTrust ?

1

Capture des signaux physiques bruts OT avec AIo_Tracks

- Installation non intrusive sur rail DIN
- Connexion directe aux E/S des équipements industriels
- Compatible avec tous les automates et signaux industriels
- Indépendant du SCADA et du réseau IT

2

Analyser et déclencher les alertes localement avec AIo_Insight

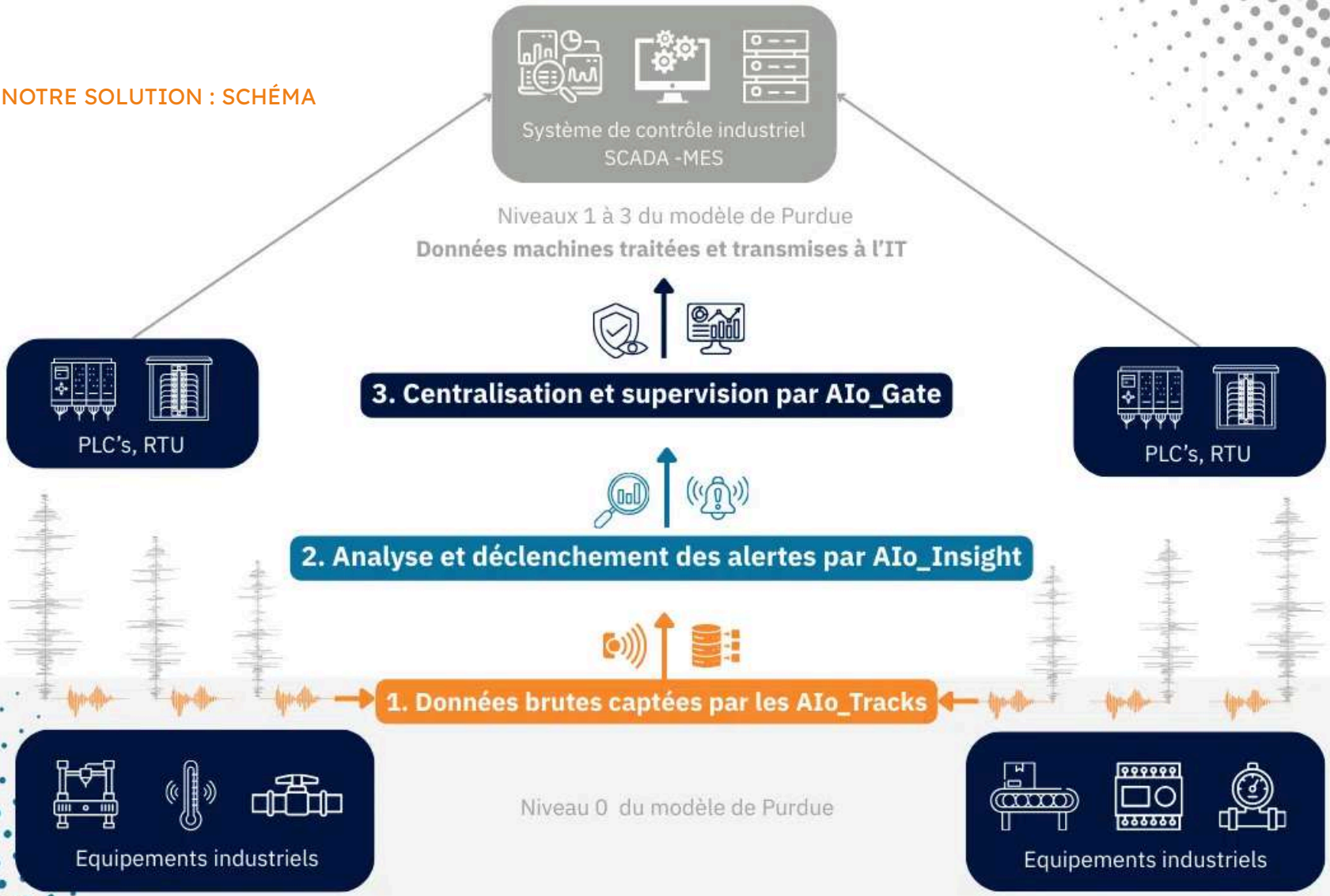
- Analyse en temps réel des signaux captés, directement au niveau des équipements
- Vérification de la cohérence entre les commandes et l'exécution réelle
- Détection d'anomalies : écarts, dérives, falsifications ou erreurs
- Alertes immédiates en cas de comportement suspect

3

Superviser et centraliser avec AIo_Gate

- Configuration et supervision des modules AIo_Tracks et AIo_Insight
- Centralisation des données et des alertes issues des équipements surveillés
- Analyse et historique horodaté des événements détectés
- Intégration avec les systèmes industriels (SIEM, SCADA, MES, API)

NOTRE SOLUTION : SCHÉMA



NOTRE SOLUTION : DÉMONSTRATION

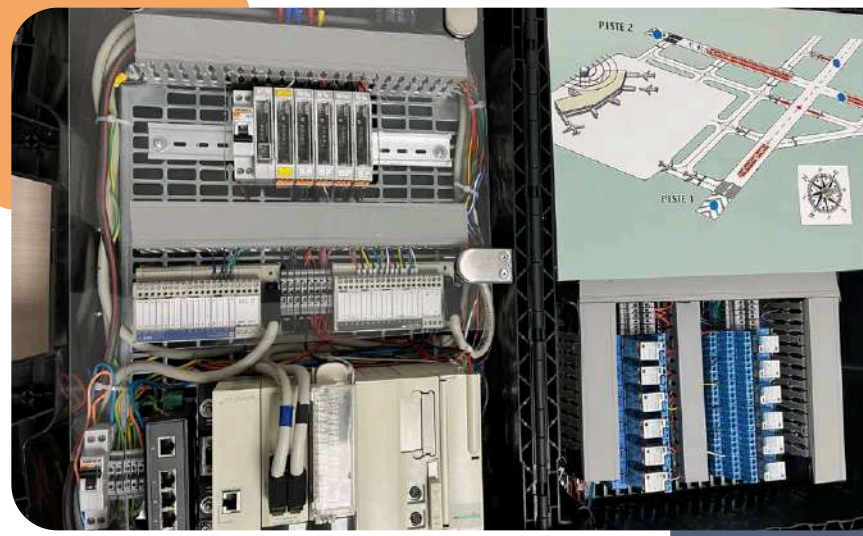
Essayez AIoTrust en 30 minutes

Démonstration autonome, sans connexion réseau : simulez des attaques sur l'automate et observez le déclenchement d'alertes sur un scénario simulé :

Prise de contrôle du système de commande
Simulation d'une attaque qui modifie les commandes envoyées aux équipements, sans alerter le SCADA.

Falsification de données
Données retournées par l'automate volontairement modifiées pour masquer la réalité (ex. : une donnée analogique modifiée).

Perturbation de process / destruction d'équipements
Simulation d'un comportement déviant entraînant une surcharge ou un risque de défaillance physique.



SECTEURS D'ACTIVITE

Une solution adaptée à tous les secteurs

Chaque secteur présente ses propres exigences de continuité, de sécurité et de performance. AIoTrust vous aide à détecter les signaux faibles, à prévenir les dérives et à sécuriser vos équipements critiques quelle que soit votre activité.

Industrie manufacturière et agroalimentaire

Sites de production, lignes de fabrication, ateliers d'assemblage ou chaînes agroalimentaires

Bâtiments automatisés

Data centers, immeubles de bureaux, établissements publics ou centres commerciaux

Eau et environnement

Stations de traitement, réseaux d'eau potable ou d'assainissement, capteurs environnementaux

SECTEURS D'ACTIVITÉ

Explorez des exemples concrets et cas d'usage par secteur sur notre site internet.

Pétrochimie

Sites SEVESO, raffineries, terminaux pétroliers, pipelines ou usines chimiques

Hôpitaux

Équipements techniques, fluides médicaux, systèmes critiques

Aéronautique - défense

Aéroport, base aérienne, usine de production ou d'assemblage, infrastructure critique civile ou militaire

66 Bd Niels Bohr, 69100 Villeurbanne, France

frederic.breussin@aiotrust.io

+33 608 76 83 00

AIoTRUST