Cybersecurity

Industrial performance

Cyber Resilience & OT Monitoring

Raw data analysis for your industrial equipment

YOUR INDUSTRIAL CYBERSECURITY CHALLENGES - THE CONTEXT

Industrial equipment is robust, but not secure enough

Are you a CISOs, CIO or OT cyber expert? Do you know all the cybersecurity vulnerabilities in your factory?

- PLCs do not report all critical data
- Data is pre-processed and can be falsified
- IT solutions do not detect falsified field-level signals
- No one today monitors the system's physical signals
- There is no way to verify the integrity of commands sent to your actuators

+53%

average annual increase in OT cyberattacks (2021 - 2023)

73

industrial attacks recorded each month in 2023

3 jours

to stabilize a system after an attack, and weeks of business interruption losses

What are the consequences of a cyberattack for your factory?

When a cyberattack goes undetected, the consequences for your production can be severe. Yet, many critical signals remain invisible to IT or SCADA systems.

Operational impact

Quality decline

Distorted order cycles

Economic impact

Extended diagnostic times

Weeks of business interruption losses

Industrial impact

Equipment deterioration

Regulatory non-compliance

YOUR MONITORING AND INDUSTRIAL PERFORMANCE CHALLENGES - THE CONTEXT

Industry lacks reliable and actionable field-level data

This data is crucial for optimizing production line performance. Without it, slow drifts, weak signals, or consumption anomalies often go unnoticed.

- No real-time visibility into equipment
- No alerts for machine drifts
- Poorly actionable energy data
- Decisions made without reliable data
- Difficult diagnosis of breakdowns and micro-stops

16%
of industrial sites only have real-time visibility into all their manufacturing processes. (USA)

70%
of industries still manage data manually despite the increase in data collection. (USA)

39%
of industrial sites have only successfully scaled a data strategy beyond a single product. (Large groups, global)

What are the risks to your factory’s operations?

On the shop floor, every machine, every cycle, and every signal counts. Yet, without reliable field-level data, anomalies remain invisible and consequences accumulate.

Operational impact

Reactive maintenance only

Underestimated downtime

Economic impact

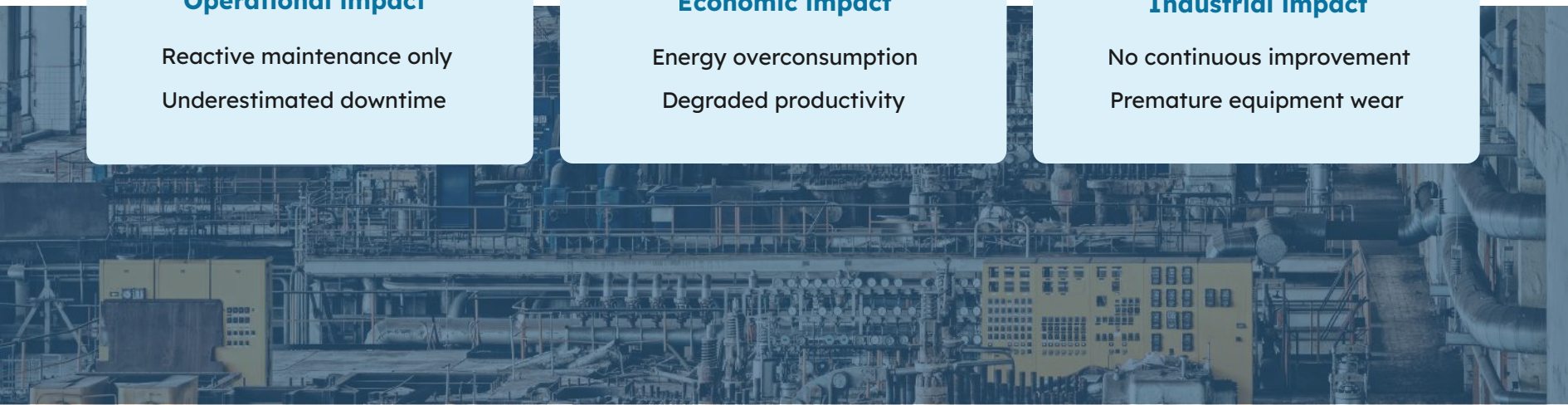
Energy overconsumption

Degraded productivity

Industrial impact

No continuous improvement

Premature equipment wear



OUR SOLUTION: MONITORING ELECTRICAL SIGNALS FROM INDUSTRIAL EQUIPMENT

The only non-intrusive and modular solution capable of detecting falsified or erroneous industrial commands

Capture raw signals from your OT equipment and detect invisible anomalies (technical drifts, erroneous commands, or cyberattacks) to strengthen the security, performance, and availability of your industrial facilities.

OUR SOLUTION: 3 STEPS

How does the AIoTrust solution work ?

1

Capturing raw physical OT signals
with AIo_Tracks

- Non-intrusive DIN rail installation
- Direct connection to industrial equipment I/O
- Compatible with all PLCs and industrial signals
- Independent from SCADA and IT networks

2

Analyzing and triggering alerts locally
with AIo_Insight

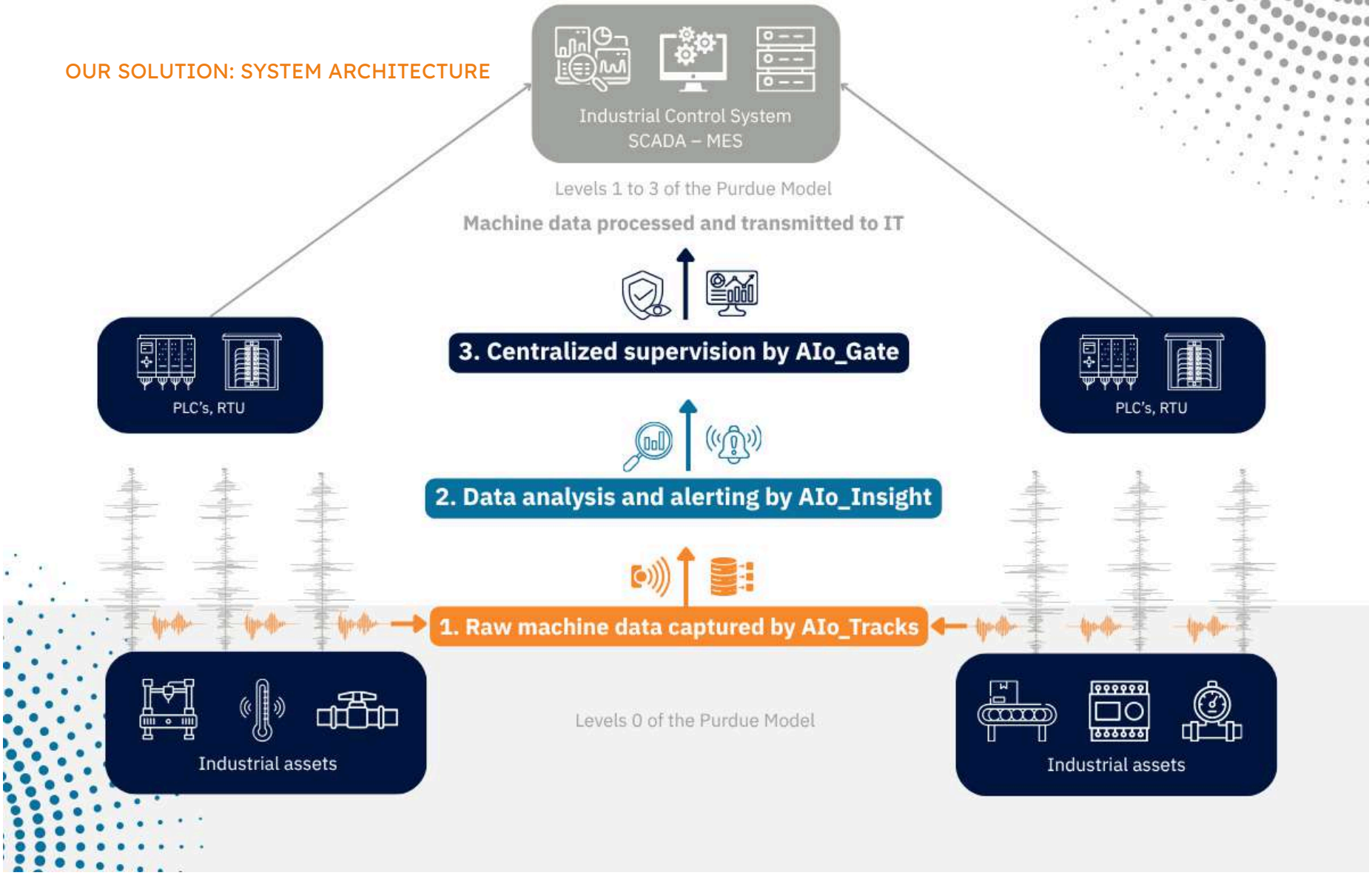
- Real-time analysis of captured signals, directly at the machine level
- Consistency check between commands and actual execution
- Anomaly detection: gaps, drifts, falsifications, or errors
- Immediate alerts in the event of suspicious behavior

3

Monitoring and centralizing
with AIo_Gate

- Configuration and supervision of AIo_Tracks and AIo_Insight modules
- Centralization of data and alerts from monitored equipment
- Analysis and time-stamped history of detected events
- Integration with industrial systems (SIEM, SCADA, MES, API)

OUR SOLUTION: SYSTEM ARCHITECTURE



OUR SOLUTION: DEMONSTRATION

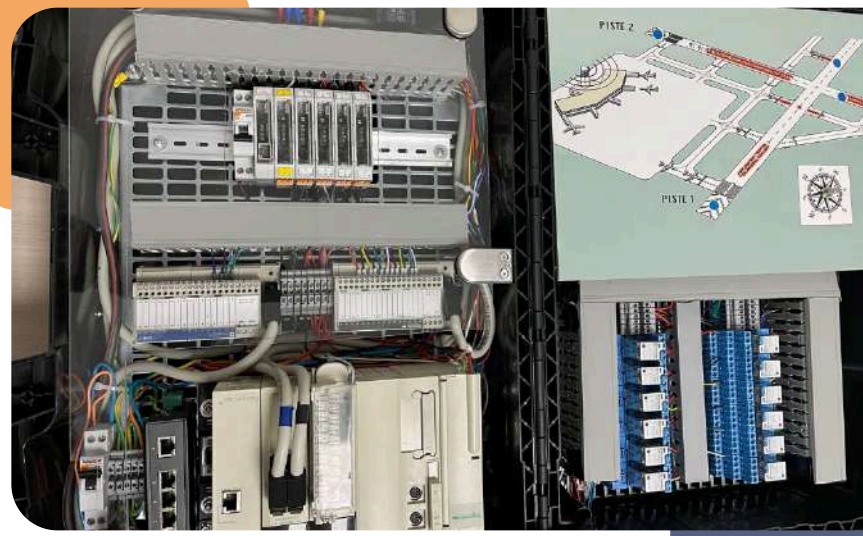
Try AIoTrust in 30 minutes

Standalone demonstration, no network connection required: simulate attacks on the PLC and observe alert triggering in a simulated scenario:

Control system takeover
Simulation of an attack modifying commands sent to equipment, without alerting the SCADA.

Data falsification
Data returned by the PLC is intentionally modified to mask reality (e.g., modified analog data).

Process disruption / Equipment destruction
Simulation of deviant behavior leading to an overload or a risk of physical failure.



SECTORS OF ACTIVITY

A solution tailored to all sectors

Every industry has its own requirements for continuity, security, and performance. AIoTrust helps you detect weak signals, prevent drifts, and secure your critical equipment, regardless of your sector of activity.

Manufacturing, Food & Beverage

Production sites, manufacturing lines, assembly workshops, or food processing lines

Automated Buildings

Data centers, office buildings, public institutions, or shopping malls

Water & Environment

Treatment plants, drinking water or wastewater networks, environmental sensors

SECTORS OF ACTIVITY

Explore real-world examples and industry-specific case studies on our website.

Petrochemicals

SEVESO sites, refineries, oil terminals, pipelines, or chemical plants

Hospitals

Technical equipment, medical gases, critical systems

Aerospace & Defense

Airports, airbases, production or assembly plants, civil or military critical infrastructure

66 Bd Niels Bohr, 69100 Villeurbanne, France

frederic.breussin@aiotrust.io

+33 608 76 83 00

AIoTRUST