LEXART

Forged in Code. Driven by Challenge

Security in Industry 4.0: *Case - How Boiler Data Can Reveal How Well Your Competitors Are Doing*

Author: Alex Casadevall, CEO @ Architects Team

Introduction

LEXART

Industry 4.0 security is usually treated as an access problem. Firewalls, encryption, IAM, and zero-trust dominate the discussion.

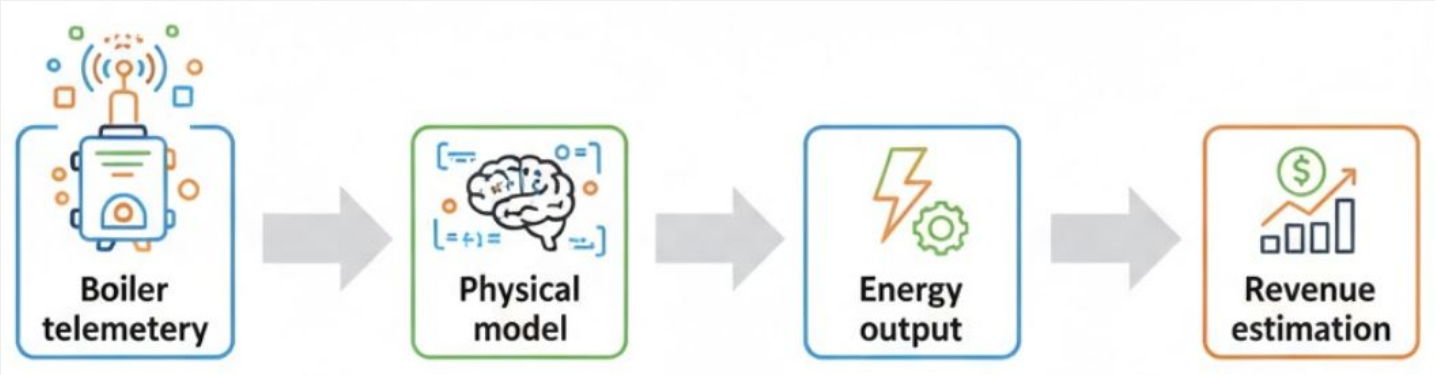
But there is a quieter risk. Even without any intrusion, operational IoT data can reveal how well a competitor is performing.

This work explores that blind spot. Using a realistic ethanol plant, we show how boiler telemetry and edge-level observability can be mathematically modeled to infer energy production and ultimately economic performance.

From boiler data to competitive intelligence

LEXART

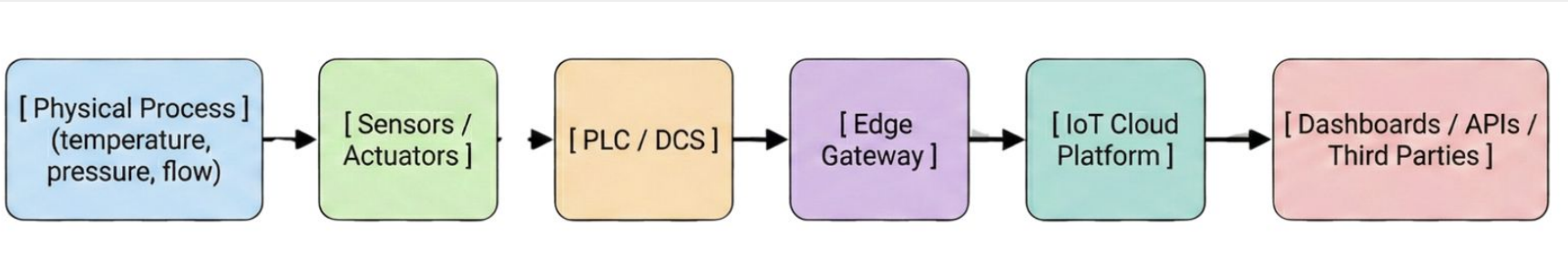
In ethanol plants with cogeneration, the boiler is not just an operational asset it is the **economic heart of the system**. *The core idea is simple:*



IoT architecture of an ethanol plant *

LEXART

A modern ethanol plant typically follows this structure:



The boiler as a fully observable physical system

LEXART

Typical boiler instrumentation includes:

- Steam temperature $T(t)$
- Pressure $P(t)$
- Steam mass flow $\dot{m}(t)$
- Operational state (load, startup, shutdown)

From a systems perspective: These variables define the thermodynamic state of the plant. Nothing “sensitive” is being measured yet everything important is encoded.

Why the Edge Gateway matters

LEXART

The Edge Gateway aggregates:

- OT data (boiler, turbine, bagasse feed)
- Environmental sensors (ambient temperature, humidity)
- Energy meters
- Maintenance telemetry

It also: Normalizes timestamps, Buffers high-frequency data, Exposes APIs (MQTT / HTTPS) and communicates with cloud platforms and third parties

Crucially: The gateway does not understand *economic sensitivity*. It only understands *operational relevance*.

Exploring the physical environment through edge data

LEXART

Beyond the boiler itself, edge devices often monitor:

- Bagasse conveyor load
- Fuel moisture
- Turbine vibration
- Cooling system performance
- Electrical export status

By correlating: boiler temperature, fuel feed stability and turbine operating regime an observer can infer how close the plant is to optimal efficiency. This answers a key competitive question: *Is my competitor running well, or are they underperforming?*

Mathematical formalism: from data to predictability

LEXART

Let the observable system state be: $\mathbf{x}(t) = [T(t),\ P(t),\ \dot{m}(t),\ u(t)]$

Where: $u(t)$ is a discrete operational mode (idle, ramp-up, nominal). This vector is sufficient to reconstruct energy production.

The enthalpy for superheated steam: $h = h(T, P)$

In industrial operating ranges: $\frac{\partial h}{\partial T} > 0$ where P varies within narrow design limits.

Knowing $T(t)$ allows bounding $h(t)$ even with uncertainty in P

Thermal and Electrical power estimation

LEXART

Thermal power output is $\dot{Q}(t) = \dot{m}(t)\,(h_{\text{out}}(t) - h_{\text{in}})$ With h_{in} approximately constant and $\dot{m}(t)$ stable in steady operation.

We obtain a simplified model $\dot{Q}(t) \approx k \cdot \dot{m}(t) \cdot T(t)$ this approximation is sufficient for economic inference, even if not for control.

Electric power is $P_e(t) = \eta \cdot \dot{Q}(t)$ where turbine efficiency $\eta \in [0.30,\ 0.40]$ this range is dictated by design, not guesswork.

Energy Reconstruction and Revenue predictability

LEXART

With IoT sampling at interval Δt: $E \approx \sum_{i=1}^{N} P_e(t_i)\,\Delta t$ higher sampling frequency has lower integration error.

If electricity is sold at price $p(t)$: $\text{Revenue} \approx \sum_{i=1}^{N} E(t_i)\,p(t_i)$

even with approximate prices, partial visibility and measurement noise. the trend, scale, and utilization efficiency become visible. This is usually all a competitor needs.

Security implications: no breach required

LEXART

What the attacker does not need: ERP access, Financial systems, Contracts, Market bids and Meter tampering.

What the attacker does need: Legitimate or semi-legitimate access to IoT data, domain knowledge, physical modeling and Time-series correlation. This is passive intelligence gathering, not cybercrime in the classical sense.

From the reconstructed signals, one can estimate: Capacity utilization, operational stability, downtime frequency, efficiency degradation and revenue trends.

Conclusion

LEXART

Operational telemetry becomes a proxy for financial health. In ethanol plants with Industry 4.0 architectures: the physics is known, the models are stable, the data is sufficient and the inference is unavoidable unless explicitly designed against.

IoT security is no longer just about protecting access. It is about protecting what can be inferred.

In a competitive industrial landscape, your boiler data may already be telling your competitors how well you are doing.