Nothing Happened — and That's the Story

When IT meets OT, one wrong move can ripple through operations — unless someone's watching.

GUARD

A security situation occurred in a newly built, automated facility – but was handled before it developed further. Thanks to continuous monitoring, clear role understanding, and OT- security competence, **the deviation was detected and neutralized – without consequences for operations, data, or system integrity.**

For confidentiality reasons concerning the facility's architecture and risk profile, we do not disclose technical details or names of involved parties.

The Challenge: IT security competence in an OT environment
During maintenance work on network infrastructure, a highly recognized IT consultancy was performing adjustments to a firewall.

The task seemed routine – but in a tightly coupled operational environment, even small changes can have large consequences. Without understanding the dependencies between control systems, the change effectively left critical infrastructure exposed to malicious actors. The consultant had strong IT expertise – but lacked insight into how operational systems were interconnected, and what could be affected by the modification.

How the Incident Was Averted
Because the facility was under active monitoring by Guard Automation's Security Operations Center (SOC), the irregularity was detected and managed immediately – before it had any real impact.

Operations continued without interruption, and system integrity was maintained.
This is an example of how quickly things can happen – and how important proactive measures, technical insight, and access to people who understand both systems and processes truly are.

"There was a collective cheer for Guard Automation," said the customer. «Not because something happened – but because it didn't»

IT and OT – Same Principles, Different Priorities

It can be tempting to apply the same tools and mindset across IT and OT.
But the reality is that the threat landscape – and the consequences – are fundamentally different.

Cybersecurity in both IT and OT revolves around **confidentiality, integrity, and availability**.
The difference lies in **the order of priority**.

- **IT: C → I → A**
  Confidentiality and integrity are often prioritized first, while availability can be temporarily sacrificed (for example, during updates or patching) to protect data.
- **OT: A → I → C**
  In operational environments, **availability** comes first to maintain continuous operation and physical control. **Integrity** of control logic and signals is critical to ensure safe and correct function. **Confidentiality** still matters, but is rarely the top concern.

Where IT attacks can compromise information, OT incidents can stop operations, damage infrastructure, endanger people and/or the environment.

That's why OT security requires domain experience:

- Understanding how control systems actually work
- Knowledge of real-time protocols and deterministic logic
- Awareness of how small changes can cause system-wide effects

This expertise cannot be built through IT training alone – it comes from years of work in automation, operations, and process industries.

The Result: Incident Prevented, Operations Uninterrupted

The deviation was detected and neutralized before it affected the facility.
No downtime, no data loss, and no operational consequences.
The event demonstrates the importance of continuous monitoring, operational insight, and clear role boundaries between IT and OT environments.

In today's connected world, IT is the front door to OT. Defending critical infrastructure demands more than firewalls — it demands people fluent in both language

«Cybersecurity in industrial environments is no longer about securing two separate domains — IT and OT. It's about securing their intersection. That's where most attacks begin, and where the right competence makes the greatest impact", says Jan-Terje Sørlie, CTO at Guard Automation.

Prevention rarely makes headlines.

Jan-Terje Sørlie, CEO & CTO, Guard Automation AS