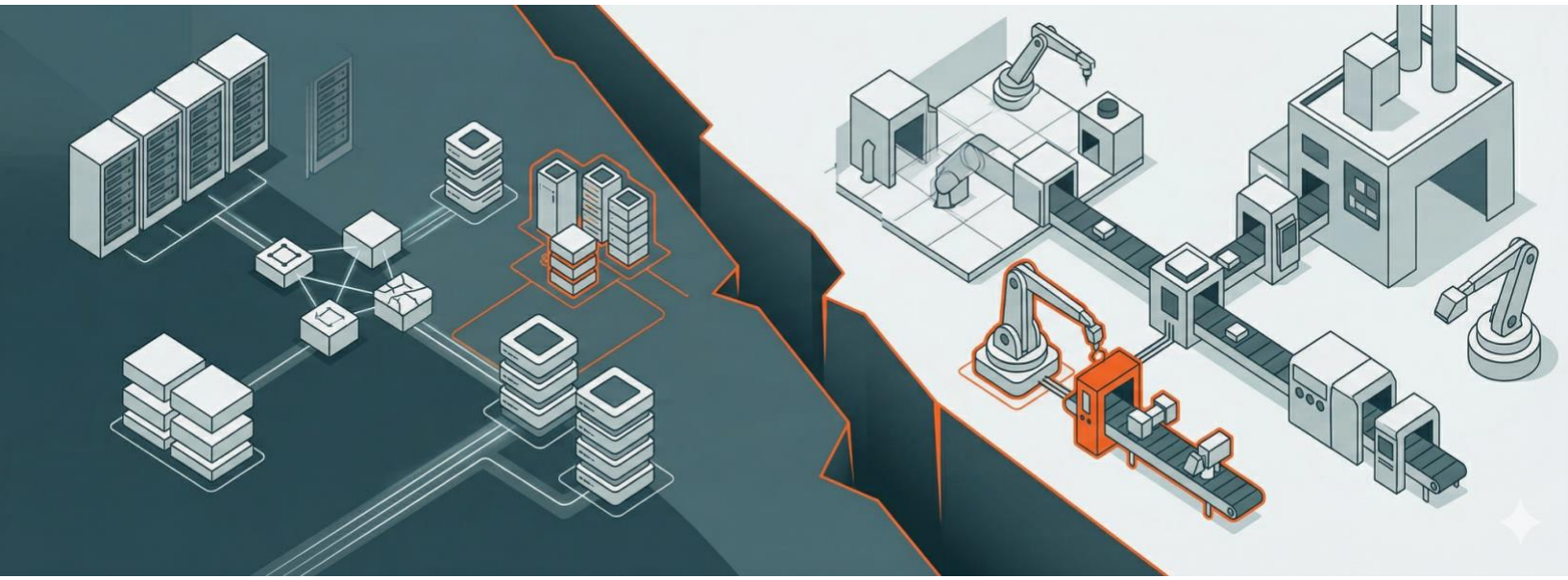
heliqx

The IT/OT Gap Is Now a Business Risk

Why manufacturers need a new model
to maximise visibility, security and operational continuity.

By Thomas Herrmann, heliqx CEO
May 2026



As industrial companies push ahead with ambitious digital transformation programmes, expectations continue to grow. Leaders want smarter, more connected and resilient factories. Better visibility, stronger cybersecurity, fewer operational surprises and tools for continuous improvement are also on their checklist.

In theory, the path is clear.
But the reality is much more complex.

As more sensors, systems, tools and data layers are added to manufacturing environments, the challenge moves far beyond technology adoption. We need to make increasingly complex OT environments governable, visible, secure and workable at scale. And this is where many organisations struggle.

For all the bold promise of Industry 4.0, the day-to-day reality at industrial sites is often still fragmented. Legacy infrastructure coexists with newer technologies. Plants may operate with different standards, levels of maturity and ways of managing risk. Responsibilities are dealt out across teams with diverging priorities and expertise.

This is where the gaps begin
IT teams are usually well equipped to manage enterprise networks, apply governance and strengthen cybersecurity. But industrial environments bring different, often unfamiliar demands, from older assets to production-critical systems, hard-to-access sites, limited maintenance windows and a low tolerance for disruption.

OT teams, on the other hand, understand the machinery, the production environment and operational realities on the ground. They know what can't fail and where practical workarounds have evolved over time. But they aren't always set up to manage the complexities of cybersecurity, asset visibility, access control, vulnerability prioritisation and cross-site governance.

This opens up gaps in both skills and operations.

These widening gaps have multiple impacts, from unclear ownership to inconsistent visibility, disconnected workflows, delayed responses, siloed decision-making and technologies that don't join up properly. The result? Friction between teams, slower progress and avoidable risk in critical environments.

Consequences are no longer marginal
When IT and OT don't work using a shared model, the consequences ripple well beyond occasional inconvenience. Security exposures can remain hidden. Operational issues can take longer to detect and resolve. Compliance becomes harder to demonstrate consistently across sites. Critical decisions depend too heavily on local knowledge or manual intervention. When downtime does occur, the cost can quickly tally into hundreds of thousands of euros, or more.

It's clear that conversations around industrial digitalisation need to evolve.

For far too long, the market has tried to solve OT challenges by adding one more tool, another dashboard or an extra security layer. Sometimes, IT cybersecurity solutions are pushed into OT with limited adaptation. Other times, OT visibility tools are introduced without focusing on broader issues such as

coordination, governance and operational response.

Although well intentioned, these efforts fail to reach the root of the problem.

Because it isn't just about technology
What's missing is an integrated model for governing, running and securing OT environments in a way that actually works in the real world.

This model needs to recognise that each industrial environment is different. Factories are often shaped by years of decisions, local adaptations and inherited infrastructure. Fragmented management initiatives and isolated solutions just don't cut it. Overstretched internal teams can't be expected to master every single aspect of OT cybersecurity, operational visibility and multi-site coordination all on their own.

Joining the dots
Rather than another disconnected product or an advisory exercise rolled into a slide deck, industrial organisations need a practical, joined-up model that wraps strategy, implementation, visibility and ongoing operational support together. This model should make it easier for IT and OT teams to align, strengthen control across sites and make ambition a reality on the shopfloor.

That's where heliqx comes in.

Heliqx was built to help IT teams manage complex OT environments, by combining elements that conventional approaches leave fragmented. Rather than treating OT as an IT offshoot or jamming new tools onto an already crowded stack, heliqx provides an integrated model designed for industrial operations.

Shaping a practical path forward
At the centre of this model stands OT PULSE: a zero-gaps IT solution for OT. Through four connected components, it helps organisations strengthen security, improve visibility, support compliance and protect uptime, while also making it easier for IT and OT teams to collaborate.

First, consulting
To lay solid foundations, heliqx helps organisations define a blueprint aligning cybersecurity, operational continuity and digital progress, while taking into account the specificities of their sites, systems and teams.

Second, technical teams
Industrial organisations often need specialist expertise and additional delivery capacity. Heliqx provides the technical depth and hands-on support to implement solutions in critical environments.

Third, a unified platform
Enabling a unified operational picture across assets, networks, sites and workflow, PULSE OT helps teams see what matters, act quickly and manage OT environments in a structured, consistent way

Fourth, operations support
OT resilience depends on what happens from deployment onwards, including monitoring, issue management, governance, access control, prioritisation and response. Heliqx supports organisations in sustaining their OT performance over time.

From fragmented efforts to full control
Together, these elements connect strategic intent with operational execution, across multiple sites.

This is essential given that successful IT/OT integration relies on alignment between people, processes, priorities and decision-making. It creates an environment where IT can extend governance and resilience into OT, while OT teams can operate safely and effectively.

With the right model, organisations can shift from reactive management to proactive control. In concrete terms, this means full visibility, better coordination across locations and teams, and faster responses to incidents and vulnerabilities. Governance and resilience become scalable, repeatable and grounded in operational reality.

The future of industrial operations depends on better joined-up digitalisation. And the winners will be those who enable IT and OT to succeed together. By simplifying, securing and strengthening the most critical and vulnerable part of your manufacturing infrastructure, your IT and OT teams can move forward feeling confident and being in control.