IT / OT FIELD REPORT

Convergence: Successes & Failures

Where IT and OT integration actually works, where it breaks, and what leaders at every level can do to change the outcome.

FIVE FIELD REPORTS CONVERGENCE · DATA · AI · LEADERSHIP · ENERGY

CONTENTS

ABOUT THIS E-HANDBOOK

The gap between Information Technology and Operational Technology teams has defined — and often derailed — industrial digital transformation for decades. From AI deployments that stall at the pilot phase to cybersecurity failures born of cultural silos, the convergence story is rarely straightforward. The five articles gathered here explore where IT/OT integration succeeds, where it fails, and what leaders can do to change the outcome.

01 CONVERGENCE · INNOVATION p.03
IT-OT Convergence as a Driver for Manufacturing Innovation
How blurring the boundary between physical operations and digital systems creates a new competitive edge.

02 DIGITAL TRANSFORMATION · DATA ARCHITECTURE p.06
The Strategic Importance of Industrial Data Fabrics
Why a unified data fabric is the key to surviving cloud outages and network disruptions.

03 AI · OT CYBERSECURITY p.09
Where AI Belongs in OT — and Why Secure Integration Beats Speed
The moment AI enters an OT environment, it becomes operational technology.

04 LEADERSHIP · GOVERNANCE p.12
Why IT/OT Initiatives Fail When Engagement Stops at Sponsorship
Sponsorship secures funding. Sustained leadership is what delivers results.

05 ARTIFICIAL INTELLIGENCE · COMPETITIVENESS p.15
Competitiveness: How IT, OT, and AI Win Together
The biggest gains don't come from new machines — they come from what you already run.

01 · CONVERGENCE · INNOVATION

IT-OT Convergence as a Driver for Manufacturing Innovation

IT-OT convergence connects the intelligence of IT systems with the operational rigor of OT environments, unlocking new levels of efficiency, sustainability, and responsiveness. Gartner forecasts underscore the scale of this revolution: by 2025, 50% of large industrial organizations will use digital twins, achieving 10% operational efficiency improvements. Additionally, 75% of G2000 manufacturers will implement IT-OT integration strategies to accelerate product cycles and strengthen resilience.

WHAT YOU'LL LEARN

- Convergence is a competitive edge, not an IT side-project.
- Digital twins, Unified Namespace, and edge computing are the core building blocks.
- The biggest blockers are cultural and security-related — not technical.

WHAT IS IT/OT CONVERGENCE?

At its essence, IT-OT convergence integrates two traditionally siloed domains. IT is focused on data-driven decision-making, manufacturing ERP software, design tools like PLM, and analytics systems that provide strategic insights across the organization. OT encompasses the hardware and software that control and monitor physical processes on the shop floor, including SCADA systems, PLCs, and IoT sensors.

The synergy of these domains results in a seamless flow of information. Real-time OT data feeds into IT systems, enhancing analytics and enabling dynamic decision-making. By incorporating solutions that support the entire lifecycle of operations, factories can bridge the gap between the virtual world of planning and the physical world of production.

Key components include digital twins and virtual twins — virtual replicas of physical assets that integrate historical performance, real-time data, and predictive models to optimize operations and reduce risks. Unified architectures facilitate real-time data integration across all systems, transitioning from outdated models like the Purdue Enterprise Reference Architecture to event-driven frameworks such as the Unified Namespace (UNS). Edge computing ensures operational decisions are made closer to the source of data, reducing latency and enabling faster response times.

THE STRATEGIC BENEFITS OF IT/OT INTEGRATION

Predictive maintenance powered by integrated IT-OT platforms reduces unplanned downtime by **40%**. Automation of repetitive tasks leads to **15–20% cost savings** across operations. Unified dashboards provide actionable insights to identify and resolve bottlenecks immediately, and advanced monitoring systems ensure energy use aligns with production needs.

Integration with edge computing enables rapid adaptation to market changes, while machine learning models reduce supply-chain inefficiencies. IT-OT collaboration supports net-zero factories through energy optimization: virtual twins model energy flows, highlight inefficiencies, and inform sustainable strategies. Integrated QMS supported by real-time data catches defects early, and IT-OT integration aligns processes with regulatory standards.

AR tools powered by IT-OT integration enable faster training and troubleshooting. Collaborative platforms break down silos, improving communication and knowledge sharing. Cyber-physical systems strengthen security across IT and OT layers, and real-time monitoring and redundancy measures reduce risks from supply-chain disruptions.

CHALLENGES ON THE ROAD TO CONVERGENCE

Despite the transformative potential of IT-OT integration, many manufacturers encounter formidable hurdles. Cybersecurity threats, outdated systems, cultural divides, and skill shortages can significantly delay or derail progress. According to recent industry analyses, nearly **60%** of organizations cite cybersecurity and legacy technologies as top barriers to digital transformation, while more than half struggle with cultural misalignment and workforce readiness.

Over **23%** of OT environments experienced cyberattacks in 2023, underscoring the urgent need for robust safeguards. With **55%** of organizations still managing IT and OT separately, bridging the cultural gap remains a critical priority. The demand for hybrid skill sets — combining domain expertise, analytics, and IoT capabilities — continues to outpace supply.

A COMPETITIVE IMPERATIVE

The convergence of information technology and operational technology marks a pivotal shift in manufacturing. As the virtual twin concept demonstrates, the potential now extends beyond the traditional digital twin: it's about transforming data into actionable intelligence that continuously guides operations. Those who embrace this integration will lead in efficiency, sustainability, and resilience.

> **Those who do not, as Gartner warns, risk competitive irrelevance in a rapidly evolving landscape.**

02 · DATA ARCHITECTURE

The Strategic Importance of Industrial Data Fabrics

Recent outages have disrupted cloud services across a wide range of industries. From streaming services to smart water filters, each incident is an eye-opening demonstration of just how pervasive cloud services have become — and, for industrial operators, how much rides on staying resilient when they fail.

WHAT YOU'LL LEARN

- With a modern data infrastructure, disruption does not need to result in data loss or operational downtime.
- Industrial data fabrics must maintain operations when cloud connectivity is interrupted.
- Modern data fabrics are purpose-built to operate where network reliability cannot be assumed.

For businesses that rely on cloud-hosted applications, the impact of an outage is immediate: dashboards become inaccessible, analytics pipelines stall, and data flow is interrupted. But for many industrial companies using a modern data infrastructure with an industrial data fabric, disruption does not need to result in data loss or operational downtime. A lot can be learned from the role of industrial data fabrics in supporting operational resiliency when it's needed most.

WHAT'S AN INDUSTRIAL DATA FABRIC?

An industrial data fabric is a unified architecture that connects and contextualizes data from across OT and IT systems. It enables secure, scalable data movement from the edge to the cloud, while maintaining visibility and control across the entire data lifecycle. These systems support real-time monitoring, AI initiatives, digital twins, predictive analytics, ERP systems, and enterprise-wide decision-making — often by facilitating the hydration of cloud technologies with OT data.

RESILIENCE AT THE EDGE: STORE-AND-FORWARD IN ACTION

Industrial data fabrics must maintain operations when cloud connectivity is interrupted. While many platforms claim hybrid capabilities, few offer true edge resilience; some rely heavily on cloud infrastructure for processing and orchestration, which can leave them exposed during outages.

A modern industrial data fabric includes distributed data collectors deployed on-premise or at the edge. These collectors acquire data directly from industrial sources like OPC servers, PLCs, and historians. When upstream systems become unavailable, they buffer data locally — each data point timestamped and queued for delivery — through tightly integrated store-and-forward (SaF) logic. The system retains data during transmission failures and forwards it in correct chronological order once connectivity resumes.

This ensures no gaps appear in the historical record, which is critical for time-series data used in compliance reporting, performance analysis, and root-cause investigations. Losing access to this data can lead to compromised data integrity, operational blind spots, delayed decisions, and regulatory risk.

DECOUPLED SYSTEM DESIGN

Some industrial data fabrics support hybrid deployments, where local components manage data acquisition and processing on-site while centralized systems — often cloud-hosted — handle analytics, reporting, and long-term storage. To maintain true data continuity, it's important to identify data fabrics well-suited to this hybrid model, where local components can operate autonomously during upstream disruptions.

This allows use cases such as MES integration, calculations, and logic execution to continue without interruption, even when connectivity to cloud services is unavailable. The design reflects the operational realities of industrial environments: systems must function independently of centralized infrastructure, especially in remote or bandwidth-constrained locations.

PREPARED FOR MORE THAN JUST OUTAGES

Effective industrial data fabrics are designed for resilience across a range of scenarios: network instability, cybersecurity threats, and operational diagnostics. Secure data flows and authentication mechanisms are crucial in protecting against unauthorized access and tampering. Data must be encrypted both in motion and at rest, and cybersecurity threat surfaces must be limited by minimizing the number of ports through which data flows.

> **When the cloud goes dark, a well-built data fabric is the difference between a blip and a blackout.**

03 · AI · OT CYBERSECURITY

Where AI Belongs in OT — and Why Secure Integration Beats Speed

Manufacturers are exploring artificial intelligence to improve operational decision-making, optimize processes, and predict equipment failures. The benefits aren't hard to see — but recent joint guidance from the NSA and CISA is a reminder that in OT, integration must be handled with the utmost care.

WHAT YOU'LL LEARN

- If used, AI must strengthen essential services — it cannot be an avenue for compromise.
- The digitalization of OT equipment is still ongoing, and many legacy systems remain in operation.
- AI's training data is inherently historical; when conditions change, performance can degrade.

In theory, AI in OT leads to improved efficiency, fewer unplanned outages, and tighter control of product quality. But recent joint guidance from the National Security Agency and the Cybersecurity and Infrastructure Security Agency stresses that all integrations must be handled with the utmost care. As CISA acting director Madhu Gottumukkala put it: "OT systems are the backbone of our nation's critical infrastructure, and integrating AI into these environments demands a thoughtful, risk-informed approach."

If used, AI must be put to work strengthening essential services — it cannot be an avenue for compromise. Deploying AI in OT requires governance, assurance, and risk management before models enter production. The consequences run far more severe than in enterprise IT: poor analytics may cause financial loss or inefficient planning in the office, but in operational environments, incorrect AI outputs can interrupt production, introduce regulatory exposure, or put worker safety at risk.

A DIFFERENT RISK LANDSCAPE

AI introduces novel failure modes. Data-integrity problems can quickly erode trust and effectiveness, models can drift, and the decision logic of AI systems can be quite opaque. Couple these with a wider attack surface and the possibility for hackers to introduce adversarial inputs designed to mislead or poison models, and the danger comes into sharp focus.

OT environments also operate under unique constraints. Equipment lifecycles are long, upgrade windows are limited, and downtime carries direct operational costs. The digitalization of OT equipment is still ongoing, and many legacy systems remain in operation. AI developed in isolated testing environments may behave very differently once connected to live production data. Its training data is inherently historical — it reflects past operating conditions, and when those conditions change, model performance can degrade. If operators treat AI outputs as authoritative without understanding their limits, they build fragility into what should be a robust control system.

WHERE AI BELONGS IN OT

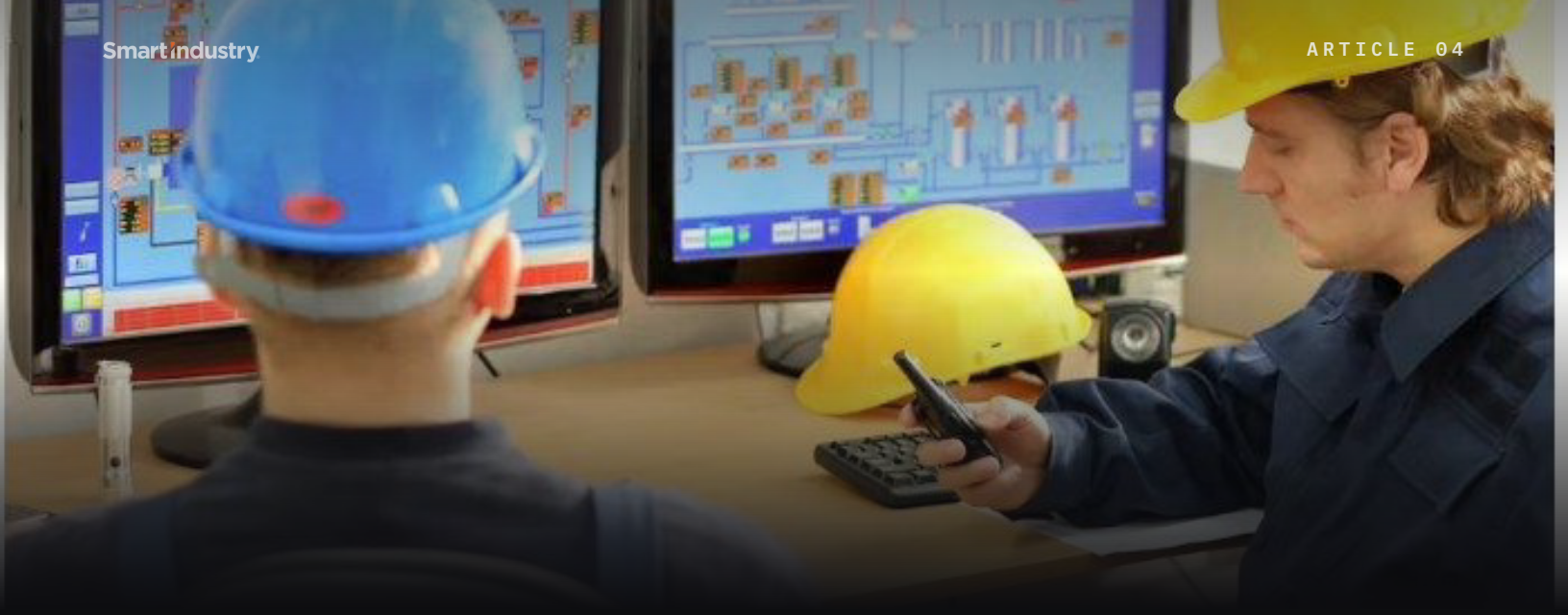
AI's role within OT architecture determines its operational risk. Advisory systems put the human in the loop, allowing clear oversight and preserving operational authority. Autonomous systems introduce a direct dependency between model behavior and plant operations. An AI system that recommends maintenance schedules adds very little operational risk; a system that integrates directly with OT hardware and adjusts production parameters or influences safety-related controls requires much stricter governance.

MAINTAINING TRUST IN MODEL PERFORMANCE

AI models degrade when operating conditions diverge from the data used during training. Manufacturers must establish structured processes for monitoring performance and identifying drift early — setting clear thresholds for retraining, validating predictions against real-world outcomes, and auditing model behavior over time. Without these controls, a model may gradually become unreliable without its operators even being aware.

Handled with care, AI can deliver measurable value in manufacturing environments. Predictive maintenance, quality analysis, and process optimization all benefit from advanced analytics. Deployment should be aligned with safety-engineering practices, cybersecurity controls, and operational governance.

> **The NSA and CISA guidance reflects one reality: the moment AI is deployed in an OT environment, it becomes operational technology in itself.**



04 · LEADERSHIP · GOVERNANCE

Why IT/OT Initiatives Fail When Engagement Stops at Sponsorship

Today, IT and OT initiatives are a top priority for many manufacturers. Whether the goal is improving visibility, strengthening cybersecurity, or connecting plant operations to the enterprise, these initiatives often start with strong executive sponsorship — yet they frequently fail to deliver sustained results.

KEY TAKEAWAYS

- The issue usually isn't the technology selected — it's what happens after approval.
- Many manufacturing organizations still treat IT and OT as distinct domains.
- Network, cybersecurity, data, and support often sit in the IT/OT overlap — where things stall.

The crux of the issue isn't usually the technology that's selected. More often, it's what happens after the initiative is approved at the C-suite level and implementation begins. Typically, executives champion IT-OT initiatives early by securing budget, aligning stakeholders, and setting the direction. But once implementation begins, that engagement often fades — and without sustained leadership, even well-designed initiatives can stall, fragment, or fall short of expectations.

> **Executives champion IT/OT initiatives early. But once implementation begins, that engagement often fades.**

SHIFTING FROM SPONSORSHIP TO SUSTAINED LEADERSHIP

To close this gap, organizations need to rethink what executive engagement looks like. Sponsorship secures funding and sets direction; sustained leadership is what ensures results — and that requires executives to stay actively involved in how teams align, operate, and deliver value long after a project is approved.

01 **Establish clear ownership and governance.** One of the most common breakdowns is ambiguity around who owns what. Network infrastructure, cybersecurity, data management, and system support often sit in the overlap between IT and OT, creating gaps where responsibilities are unclear or inconsistently executed.

02 **Reinforce the initiative's "why."** The rationale executives articulate at the start doesn't always reach the people responsible for execution. Operators, engineers, and maintenance teams may experience change as new requirements without understanding the purpose — so reinforce the "why" continuously, at every level.

03 **Align teams around shared outcomes.** Define measurable goals from the onset — improved reliability, reduced downtime, stronger cybersecurity posture, better production visibility — and reinforce them through KPIs, decision-making frameworks, and cross-functional communication.

04 **Invest in people and capabilities.** Many IT/OT initiatives rely heavily on a small number of experienced individuals who understand both environments. Executives must invest in the workforce by prioritizing cross-training and building capabilities that extend beyond individual expertise.

05 **Standardize processes across the organization.** In many manufacturing environments, critical processes such as patching, backup and recovery, access control, and change management evolve organically. Overcoming this requires standardization coming from the top down.

06 **Stay engaged beyond project completion.** Too often, success is defined by system deployment rather than business impact. IT/OT initiatives only deliver value when fully adopted, properly maintained, and continuously improved. When leadership disengages too early, initiatives lose momentum; when leadership stays involved, they become embedded in how the organization operates.

> **Technology rarely decides whether an IT/OT initiative succeeds. Sustained leadership does.**

05 · AI · COMPETITIVENESS

Competitiveness: How IT, OT, and AI Win Together

At Hannover Messe 2026, during a session on "AI and Industrial Energy," one message became unmistakably clear: industrial competitiveness is entering a new phase, defined by how effectively companies connect IT, OT, and artificial intelligence to generate measurable value inside operations.

WHAT YOU'LL LEARN

- The biggest gains don't come from buying new machines — but from what plants already have.
- Integrated into process control, AI optimizes consumption in real time, faster than manual methods.
- Modernization doesn't mean rip-and-replace — it means connecting operations to intelligence.

Across energy-intensive sectors and advanced manufacturing, opportunity is no longer theoretical. It is immediate, quantifiable, and already reshaping how leading plants operate. What is changing is not ambition — it's the standard. Results must show up in stability, throughput, quality, and energy performance. The biggest gains do not come from buying new machines; they come from extracting more performance from what plants already have.

— ENERGY EFFICIENCY ISN'T AN ASSET CHALLENGE — IT'S A DATA CHALLENGE

Energy efficiency has become a defining battleground — not because industry lacks equipment, but because it often lacks operational intelligence. Recent research highlighted the sobering reality that the industrial sector leaves approximately **17%** of potential energy efficiency untapped. This loss isn't due to a lack of physical assets or machinery; it's due to a lack of operational intelligence — a data challenge.

When AI is integrated into process control, it can optimize consumption in real time, adapting to changing conditions faster than manual approaches can. That's where competitiveness becomes tangible: less waste, more stability, better output, stronger resilience. There is plenty of noise around artificial intelligence. In industry, noise does not matter — value must be measurable. AI becomes real when it's embedded in daily operations, close to the process, improving decisions where performance is actually created.

What remains expectation rather than reality are generic initiatives that sit on top of operations as disconnected digital layers. AI cannot be a side project; it must become part of how the plant runs. Scaling AI is not primarily a technology problem — it's an integration problem. Most legacy OT environments weren't designed for real-time data integration or autonomous optimization. Modernization is essential, but it doesn't mean rip-and-replace. It means connecting operational systems to digital intelligence, step by step, with clear ownership and clear KPI targets.

THE TRIPLE THREAT OF IT, OT, AND AI

True value emerges when IT, OT, and AI work in unison. IT brings architecture, cybersecurity, governance, and scalability. OT brings process truth, control, and operational constraints. AI brings optimization, prediction, prescription, and decision support in real time. When these layers operate together, technology stops being an experiment and becomes part of the plant's operating culture.

Many AI projects fail for one reason: they never leave pilot mode. Scaling happens when AI is tied to operational KPIs and has clear ownership inside the plant — not in a disconnected innovation lab, not as a proof of concept without accountability, but inside operations, with responsibility, governance, and measurable targets. Industry's future belongs to companies that stop treating technology as an isolated initiative and start embedding it into the fabric of operations.

> **Competitiveness won't be won by who talks most about AI. It'll be won by who integrates IT, OT, and AI to deliver performance, every day.**

ABOUT THIS PUBLICATION

Smart Industry

Smart Industry is a business-to-business brand dedicated to delivering the most relevant and actionable news, analysis, and technical guidance for professionals navigating the intersection of Information Technology and Operational Technology in industrial manufacturing environments.

Published by Endeavor Business Media — headquartered in Nashville, Tennessee — Smart Industry serves plant engineers, IT/OT professionals, automation specialists, and C-suite leaders responsible for digital transformation and Industry 4.0 initiatives across discrete and process manufacturing sectors.

EDITORIAL

Smart Industry Editorial Team

Story ideas, article submissions, and editorial inquiries on industrial digital transformation, IT/OT convergence, AI, automation, IIoT, and cybersecurity.

smartindustry.com/contact-us

ADVERTISING & SPONSORSHIP

Endeavor B2B Manufacturing Group

Advertising opportunities, sponsored content, webinar partnerships, and event sponsorships within the Smart Industry brand.

manufacturing.endeavorb2b.com/smart-industry