WHITE PAPER

The manufacturing complexity tax

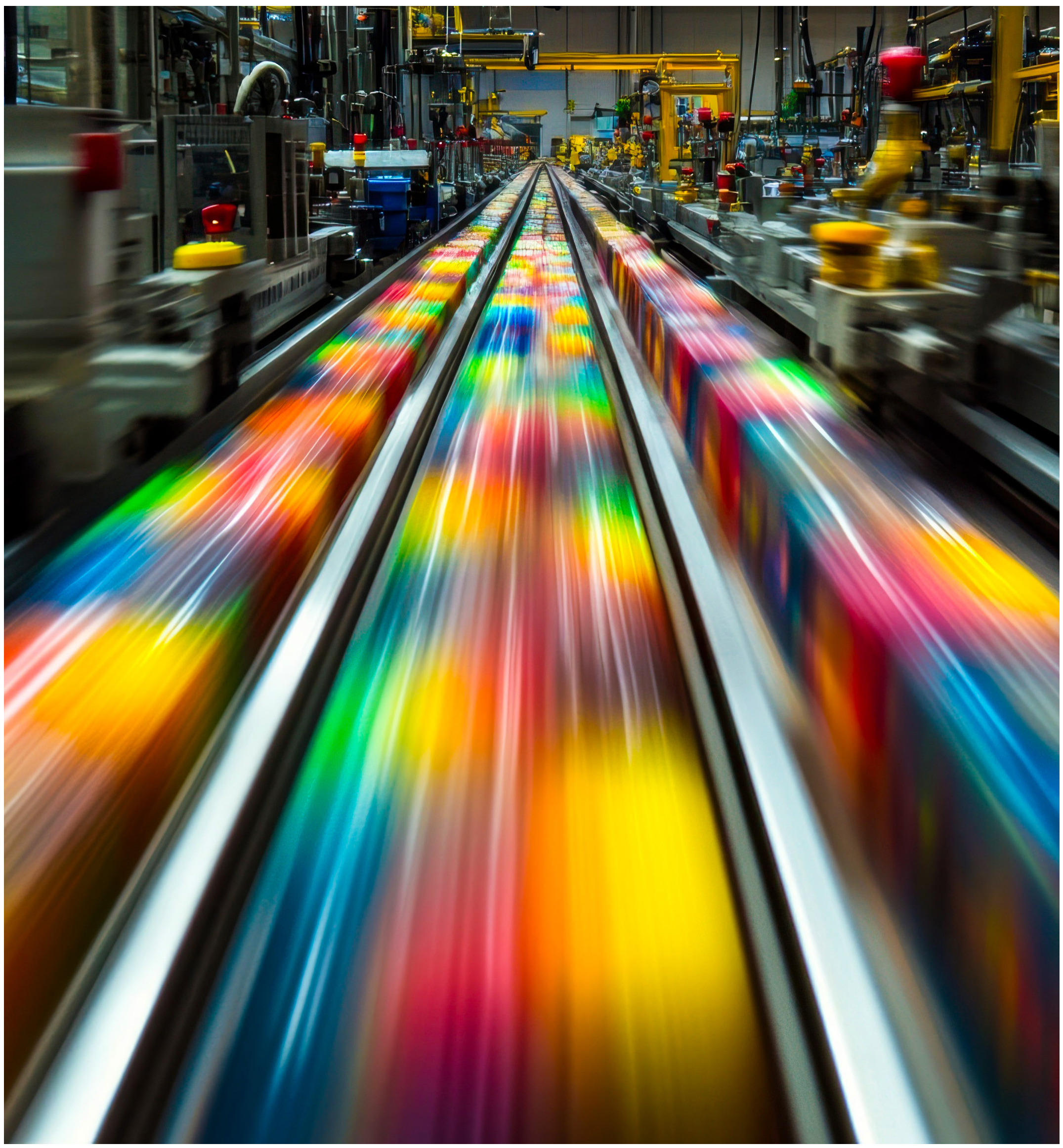
How manufacturers can change the math

The plant manager who can't explain exactly why last Tuesday's line stoppage happened, but knows it cost USD $80,000, is not the exception.

Most manufacturing facilities today are not poorly run. They are expertly managed under conditions that were never designed to be managed together: aging equipment wired to modern sensors, compliance obligations layered over production targets, workforce gaps filled by people who are capable but not yet as experienced and digital tools that generate data faster than anyone can act on it.

The result is a tax. It might not show up as a line item on any balance sheet, but manufacturers see a real, recurring cost that every plant absorbs in the form of unplanned downtime, reactive maintenance labor, quality escapes, energy inefficiency and the drag of decisions made on incomplete information.

This paper names that tax, traces where it comes from and makes the case that addressing it is an operational strategy. A strategy built on four disciplines that modern manufacturers are learning to treat as inseparable. Intelligence, control, reliability and protection.



Section 1

The tax nobody budgeted for

Complexity in manufacturing has always existed. What has changed is the rate at which it compounds.

Over the past decade, the average industrial facility has added IoT sensors, cloud analytics platforms, mobile workforce tools, compliance reporting systems and cybersecurity layers. Each new layer is introduced to solve a specific problem, each generating its own stream of data, each requiring its own maintenance, training and integration overhead. The tools multiplied. The connections between them did not.

The result is what researchers and practitioners now describe as a "fragmented operations" problem, and its financial profile is more serious than most organizations acknowledge. According to Deloitte's 2025 manufacturing outlook, nearly 60% of manufacturers cited inability to attract and retain workers as their top challenge.[1]

That figure matters as a complexity multiplier. When experienced people leave, they take institutional knowledge with them and the systems left behind rarely capture it. 86% of respondents in Octave's 2026 pulse of quality in manufacturing report say that product or service quality has suffered as a result of the increasing workforce shortage.[2]

The downstream costs are significant. Research published in Quality Magazine found that predictive maintenance raises productivity by approximately 25% while cutting equipment breakdowns by 70% and reducing maintenance costs by 25%.[3]

The gap between those outcomes and where most plants currently operate is, in large part, the complexity tax.

Section 1
(continued)

No single report outlines the six-line items of the complexity tax, but every plant manager recognizes them:

Unplanned downtime	Equipment failure without warning shuts lines, strains schedules and forces expensive emergency responses. A single unplanned stoppage in a mid-size discrete manufacturer routinely costs between USD $50,000 and $250,000 in lost output and recovery labor, before accounting for the downstream effects on delivery commitments.
Reactive maintenance labor	When maintenance is driven by failure rather than strategy, labor gets allocated to urgency rather than value. Teams spend their time responding rather than preventing. The next failure is already building, undetected.
Quality escapes	Defects that clear inspection but surface downstream in customer returns, rework or regulatory findings. These quality escapes represent some of the most expensive costs in manufacturing. They concentrate in plants where quality data and production data live in separate systems, although Octave's 2026 pulse of quality in manufacturing report highlights the worsening workforce shortage and tariffs as two of the biggest external factors impacting quality.[2]
Energy insufficiency	Industrial facilities without real-time visibility into energy consumption by asset or process have no reliable mechanism for reducing it. Energy waste is a cost problem and, in an era of carbon reporting requirements, an emerging compliance exposure.
Delayed decisions	When the data needed to make a good decision is scattered across three systems, two spreadsheets and the memory of a technician who left six months ago, decisions get delayed, diluted or made on instinct. The compounding effect of consistently suboptimal decisions across an entire facility is the largest component of the complexity tax and the least visible.
Labor and skills scarcity	The complexity tax amplifies the ongoing workforce and skills shortage. When experienced people leave, they take operational knowledge that disconnected systems were never designed to capture. The technician who knew which compressor ran hot in summer, which valve needed a workaround, which alarm could be safely silenced: that knowledge walks out the door. Facilities that can't capture, digitize and transfer that knowledge are understaffed and structurally fragile.

Octave's 2026 pulse of quality in manufacturing report

> *"External factors like fluctuating regulations and geopolitical shifts remain strong influences on plant operations but tariffs remain one of the biggest pressure points."*

Section 2

Why complexity compounds and why it's not your fault

It is tempting to frame the complexity tax as a management failure, or a sign that the plant wasn't digitized fast enough, or that technology investments weren't coordinated well enough, or that someone should have seen this coming. That framing is wrong, and it is worth saying so directly.

The operational complexity that most manufacturers carry today is the accumulated result of rational decisions made under real constraints over time. The CMMS that doesn't talk to the ERP was deployed before the ERP existed. The historian that sits apart from the quality management system was installed by a team that had a maintenance problem to solve, not a data architecture to design. The sensor network that generates more alerts than anyone can process was commissioned because unplanned downtime was the urgent problem at the time.

The World Economic Forum's Technology Convergence Insight Report characterizes the paradox between the added value that "combinatorial technology" can deliver and the operational constraints it can produce as a potential "reshaping of the entire value chain". A common pattern is that, with combinatorial technology, new bottlenecks emerge at the physical-digital interface".[3]

Each individual decision made sense. The problem is structural. Point solutions layered over point solutions eventually produce a system that is, in aggregate, more complex and more expensive than any of its parts were meant to be.

Deloitte's 2025 manufacturing report describes the operating environment manufacturers now face as one of "permanent constraint." It's a structural condition.[3] Capital costs have not returned to pre-2020 levels. Labor shortages are a demographic reality. Energy price volatility is a feature of the grid. The manufacturers who adapt are the ones building operating models capable of performing under conditions that won't change.[3]

World Economic Forum
"Technology Convergence: The New Logic for Competitive Advantage," 2026

"When technologies combine, they shift bottlenecks and change where value, power and risk sit across the ecosystem… A common pattern is that, with combinatorial technology, new bottlenecks emerge at the physical-digital interface."

Section 2
(continued)

This shift changes the calculus for every technology and operational investment. The complexity tax is strategically disqualifying in an environment where every resource counts. A workforce running lean can't afford to spend its hours firefighting. A capital budget under pressure can't sustain the cost of preventable failures. A compliance team already stretched thin can't rely on manual processes to catch what automated systems should be tracking.

The good news is, the complexity tax is reducible. It is the product of fragmentation, and fragmentation is a solvable problem. Addressing it doesn't require ripping out everything a facility has built. It requires a unified layer of intelligence that connects what already exists, turns its data into decisions and builds the four disciplines that separate reactive operations from confident ones.

Section 3

Intelligence: When data stops being noise

Most manufacturers don't have a data problem. They have a signal problem.

The average industrial facility generates more operational data in a single shift than its teams can meaningfully process in a week. Historians log every pressure reading. PLCs record every cycle. EAM systems track every work order. Quality platforms capture every inspection result. The data is there. What is missing, in most cases, is the context that turns any of it into action.

Operational intelligence means connecting data that already exists across the asset lifecycle so that a sensor reading on the floor can be understood in relation to the maintenance history of the equipment it monitors, the production schedule it supports, the quality targets it affects and the compliance obligations it touches. That chain of context is what separates a data point from a decision.

AI is accelerating this capability. Where traditional analytics required specialists to configure models and interpret output, AI-enabled systems can surface patterns and anomalies in real time, route alerts to the right people with relevant context and build predictive models from operational history that no human analyst could compile manually. According to IDC's April 2025 Worldwide SaaS Path Survey, 52% of enterprise asset management customers are already using generative AI in their current software, and 43% expect it in their next version.[9]

The practical consequence of that gap is significant. Human error and information-related deficiencies are among the leading causes of industrial incidents and unscheduled downtime, costing facilities hundreds of millions of dollars annually. That is an information architecture problem. People can't act well on information they can't see, find or trust.

Verdantix
"Strategic Focus: How Industrial Agility Is Shaping Digital Strategies," 2026

Only 18% of industrial firms had successfully centralized their on-site industrial and enterprise data into a cloud platform using a consistent data model. Nearly half (46%) still relied on various on-premise data stores sending data to a centralized cloud, depriving plant teams of the contextual insight they need.

Intelligence is the first discipline that reduces the complexity tax because it addresses the root cause: the gap between the data a facility generates and the decisions its people can make with it. Close that gap, and the downstream effects on maintenance posture, quality outcomes and labor effectiveness follow.

What operational intelligence makes possible

Maintenance	A pressure anomaly becomes a work order before it becomes a failure.
Quality	A deviation traces back to a process variable before it becomes a recall.
Handovers	A shift handover happens with full operational context, not a verbal summary and a paper log.
Capital	An investment decision is made with asset performance data, not depreciation schedules alone.
Workforce	Institutional knowledge is digitized and searchable, not held by individuals who may leave.

Section 4

Control and reliability: Operating with confidence

Intelligence changes what a plant manager can see. Control determines what they can do about it.

Control, in the context of industrial operations, is the ability to act while operating within tolerance, on what the data shows. The ability to adjust a maintenance schedule, redirect a work order, modify a production run or respond to a compliance trigger without disrupting live operations, impacting quality specifications or creating additional risks. Having information and being able to move on it are two different things.

For most plant managers, the obstacle to control is integration. When maintenance systems, production systems and quality systems operate independently, acting on a signal from one often requires manual intervention in two others. That friction slows response, introduces error and places the cognitive burden of coordination on people who are already managing more than any system was designed for them to manage.

Automation is the competitive advantage in the current operating environment. Automation in this sense is less about replacing people and more about removing the coordination overhead that prevents people from doing the work that requires human judgment. Plants that automate routine coordination tasks, like work order generation, shift handovers, compliance checks and alarm prioritization, free their teams to focus on the decisions that matter.[3]

CASE IN POINT

Scaling reliability across 350 data centers

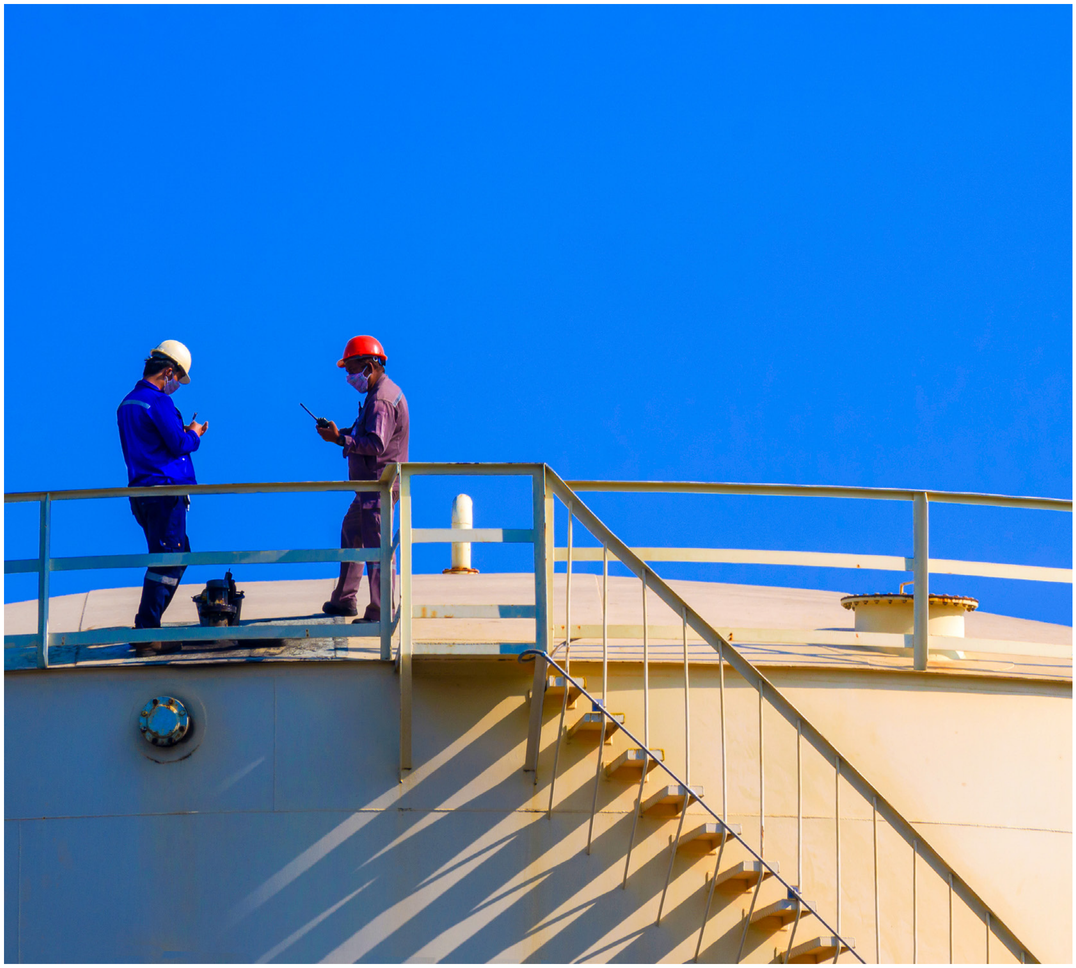
Multinational technology organization

Challenge: A global technology conglomerate operating hundreds of data centers and thousands of fulfillment facilities needed a scalable platform to unify asset management across its infrastructure divisions. Maintenance was fragmented, uptime requirements were non-negotiable and the asset base was expanding rapidly.

Key outcomes

- Reduced downtime and measurable cost savings from heightened visibility and proactive management of infrastructure assets
- Increased efficiency and operational consistency through streamlined asset management processes
- Expanded from 6,000 to 10,000 users across more than 350 data centers as the platform scaled to meet growth
- Strengthened agility to support new operational demands, including a satellite manufacturing initiative requiring stringent security and compliance standards

Read the full case study.



Section 4
(continued)

Reliability is what control, applied consistently, produces over time. Assets perform as expected on a predictable basis, deviations are detected early and responses are coordinated rather than improvised. The difference between a plant that runs and a plant that runs well.

Reliability is also the metric that most directly reflects the complexity tax. A facility carrying a high tax (i.e., fragmented data, reactive maintenance, disconnected quality tracking) shows it in its numbers: high planned-to-reactive maintenance ratios, elevated scrap rates, inconsistent throughput. Reduce the tax and those numbers move.

With capital allocation decisions centralized and payback expectations compressed, the business case for investments that improve asset reliability is among the clearest in any operational improvement portfolio. An asset that fails less, gets maintained more efficiently and runs more consistently pays back faster than almost anything else a facility can invest in.[3]

Together, intelligence and control produce something harder to quantify but easy to recognize: confidence. The plant manager who can see a problem building and respond before it becomes a crisis operates differently than the one who finds out when the line stops. That confidence compounds in decision quality, in team effectiveness and in the ability to take on more without adding more.

Section 5

Protection: The complexity tax has a security surcharge

There is an irony built into the complexity tax worth naming.

As manufacturers add connected systems to reduce operational complexity, they simultaneously expand the attack surface available to external threats. Every new endpoint is a potential entry point. Every OT-IT integration is a potential vulnerability. The digital connectivity that enables operational intelligence also creates exposure that, left unaddressed, can erase the gains it produces.

The cost of that exposure is not theoretical. In 2017, a ransomware attack on Merck & Co. caused more than USD $300 million in losses and halted production for weeks. Manufacturing has since become one of the most targeted sectors for cyberattacks,[5] with ICS and OT environments now regularly compromised through IT-OT integration points that were never designed with security in mind.[6] These environments were historically air-gapped and assumed safe. They no longer are.

For plant managers, cybersecurity often feels like someone else's problem; it falls under the domain of IT or the CISO. That is changing. When a ransomware event takes down a production line, the plant manager explains why output stopped. When a vulnerability in a historian exposes process data, the plant manager carries part of that operational risk. Security is a condition of operational continuity, not a separate initiative.

Verdantix
"Strategic Focus: How Industrial Agility Is Shaping Digital Strategies," 2026

Manufacturers face growing cyber-physical risk as IT and OT environments converge. Firms that strengthen OT network visibility and configuration management — rather than treating cybersecurity as an IT concern — achieve both improved operational resilience and measurable reductions in cyber risk exposure.

The risk is three-dimensional

Assessing OT and ICS risk requires three distinct types of context. Most facilities are missing at least one of them.

Environmental context is the foundation. A comprehensive inventory of every endpoint (e.g., hardware, software, firmware and the communication paths between them) is the starting point. Without it, a facility can't know its attack surface, can't assess how a vulnerability in one asset might propagate to others and can't prioritize where to focus remediation. Most facilities have partial inventories at best, assembled from systems that were never designed to share data.

Vulnerability context is what environmental data makes actionable. As new threats emerge and new vulnerabilities are disclosed, the ability to automatically match them against a known asset inventory determines whether a given vulnerability is present and what risk it carries in this specific environment. Security teams working without this capability are responding to generic threat intelligence rather than their actual exposure.

Temporal context is what most facilities lack entirely. Configuration changes like modifications to control logic, firmware updates and changes to safety system parameters, are among the most reliable early indicators of both operational risk and security compromise. A change that deviates from a known good baseline may signal a process adjustment, a maintenance error or a deliberate intrusion. Continuous configuration monitoring is what separates facilities that detect these signals from those that find out when something breaks.

Configuration management as operational safeguard

One of the most practical and underused tools in ICS and OT security is configuration management. Establishing a known good baseline for critical assets and monitoring continuously for deviations.

The value runs in two directions. Certain types of configuration changes have a statistically high probability of causing operational or cyber incidents. Automating the detection of those specific changes, and routing alerts to the right people with the right context, prevents a significant share of unplanned downtime before it occurs. When incidents do happen, the ability to pinpoint exactly what changed, when and on which asset compresses time from detection to recovery. Mean time to recovery drops because teams arrive informed, not investigating from scratch.

This is where the operational and security disciplines converge most directly. Configuration management is an operational practice with security consequences. A plant running within established, monitored parameters is more reliable, more predictable and harder to compromise.

Section 5
(continued)

CASE IN POINT

Building a cybersecurity program from the ground up

Electronic materials manufacturer | Octave Cyber Integrity

Challenge: Following a corporate spin-off, a U.S.-based electronic materials company producing advanced semiconductor materials had to build a new enterprisewide cybersecurity program across 14 production facilities in 12 months with limited IT/OT resources. Gaps in OT asset visibility and control system baseline configurations surfaced quickly.

Key outcomes

- Automatically built a detailed OT asset inventory across all sites, covering all installed hardware, software, firmware, I/O cards and control strategies across multi-vendor systems.
- Identified patch levels and vulnerabilities across systems, including older equipment that required remediation planning.
- Implemented configuration management workflows to ensure continuous cyber risk assessment when control system configurations changed.
- Achieved full program deployment within 12 months, providing complete visibility into assets, connections and vulnerabilities on schedule and within constraints.
- Established the foundational inventory and configuration visibility required for future digital transformation initiatives, including data lakes, 5G and AI

Read the full case study.

The manufacturers who treat protection as integral to their operational strategy complete the confidence picture. Uptime, quality and efficiency are the operating goals. Protection is what ensures they hold when conditions turn hostile.

Section 6

Changing the math: A practical path forward

The complexity tax is not paid all at once. It accumulates, shift by shift, in the decisions that couldn't be made because the data wasn't there, the failures that weren't caught because the signals weren't connected, and the hours spent responding to things that should have been prevented.

Reducing it works the same way. It's done incrementally, with each discipline building on the last. The sequence matters. Manufacturers that try to jump to advanced analytics before they have operational visibility, or to automation before they have control, get stranded. The path forward has a logic to it.

World Economic Forum "Technology Convergence: The New Logic for Competitive Advantage," 2026

Industry winners are not the most technically advanced, but the most ready to integrate. Their advantage comes from their ability to integrate new systems into existing workflows, coordinate cross-functional teams and scale solutions in real operating conditions.

Stage 1: Establish visibility

Map asset, production and engineering data availability. Identify where operational and data single points of failure exist. Before anything can improve, the plant needs an accurate picture of what it has and where the gaps are. Most facilities discover they have more data than they thought. They also discover just how disconnected that data is.

Stage 2: Connect the workflows

Stabilize digital work execution by linking EAM, maintenance and production systems. The goal here is consistency: standardized workflows, real-time production dashboards and the elimination of manual data re-entry between systems. A maintenance event should automatically update the production schedule. A quality flag should trigger a review, not a phone call.

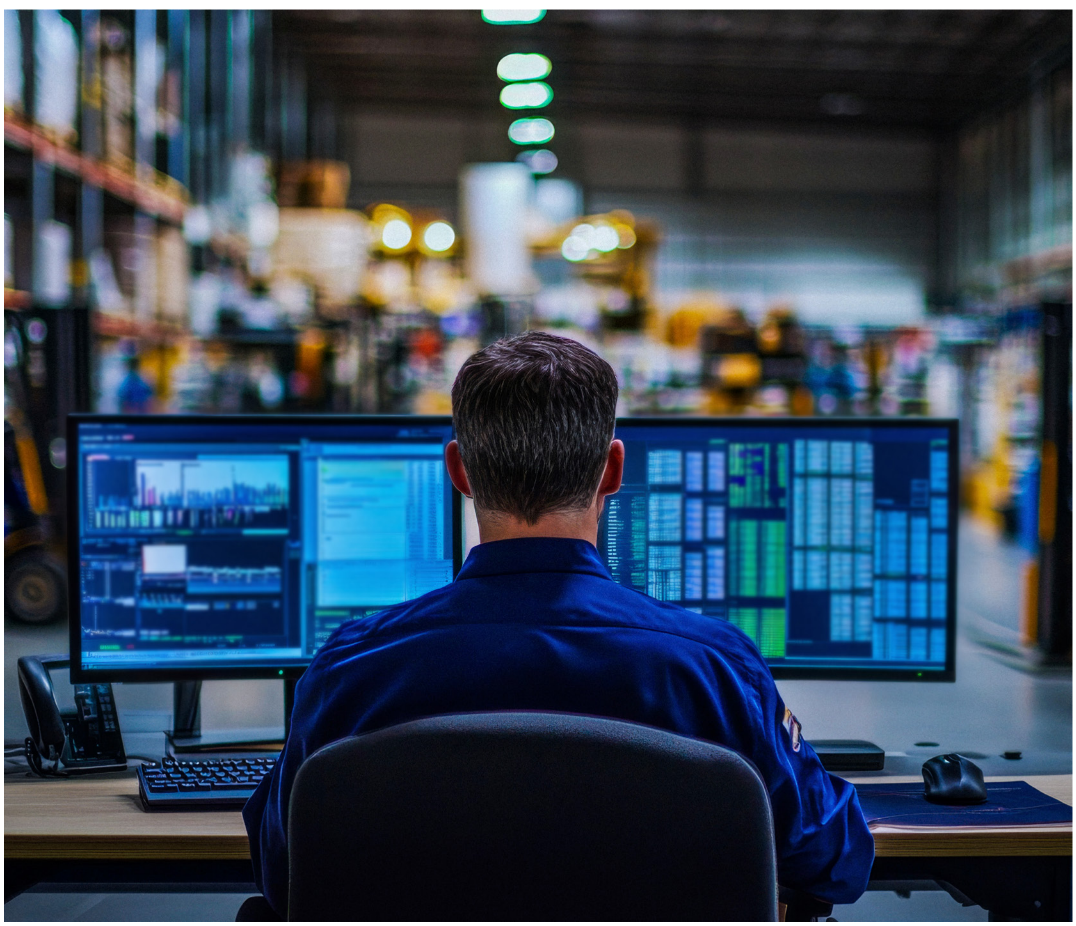
Stage 3: Build predictive capability

With connected systems and consistent data, predictive intelligence becomes achievable. Asset performance management analytics, early warning models and AI-assisted maintenance planning shift the posture from reactive to anticipatory. This is where planned-to-reactive maintenance ratios begin to move, where quality data starts feeding forward into production decisions and where labor efficiency improves without adding headcount.

AI is the accelerant at this stage. AI-enabled asset management systems can monitor thousands of signals simultaneously, flag degradation patterns before they manifest as failures and generate prescriptive guidance for maintenance teams. These capabilities would typically require dozens of specialists to replicate manually. According to IDC, agentic AI systems that can set goals, make decisions and take actions autonomously are now arriving in industrial applications, with leading software vendors actively delivering them.[7]

Stage 4: Protect what you've built

As connectivity increases through stages 1 to 3, so does exposure. OT cybersecurity, configuration management and asset inventory visibility become operational necessities, not IT line items. The final stage of the math change is ensuring that the gains from intelligence, control and reliability are protected when conditions turn hostile.



Here is the impact that the line items can make when the tax is being paid down:

Focus area	Cost of doing nothing	Impact
Labor and skills	The manufacturing skills gap could leave 1.9 million jobs unfilled by 2033, with the potential cost to the U.S. economy estimated at USD $1 trillion by 2030. Facilities that capture and digitize institutional knowledge reduce their structural dependence on individual experience — a direct hedge against that exposure.[10]	Workforce gaps become knowledge continuity. Institutional knowledge is captured in systems, not carried by individuals.
Downtime	The average large manufacturing plant loses USD $253 million per year from unplanned downtime. Predictive maintenance reduces unplanned downtime by 35–50%.[11]	Unplanned failures become planned maintenance ratios. The same team accomplishes more without adding headcount.
Quality	40% of respondents in Octave's 2026 pulse of quality in manufacturing[2] cite reducing costs as a top driver of quality investments.	Quality escapes become quality data feeding forward. Deviations surface during production, not after ship.
Energy	Applying the right energy efficiency levers might reduce up to 50% of the energy cost baseline for industrial organizations.[12]	Energy waste becomes energy visibility. Anomalies route to the right technician with full context attached.
Decisions	The value of optimizing processes and decision-making delivers immediate and tangible benefits without necessitating structural changes. Benefits can be dramatic, including increased speed to market through simplification, a reduction in nonessential meetings, and faster, higher-quality decisions.[13]	Delayed decisions become confident decisions. Shift handovers happen through structured digital records, not verbal summaries.
Security	Cybersecurity is about readiness. It means planning ahead and investing in proactive measures like monitoring, assessments, testing, controls and training. The alternative, relying primarily on reactive measures (e.g., response, customer care, remediation, recovery, litigation and fines), is more costly, risky and unsustainable. 60% of business and tech leaders rank cyber risk investment in their top three strategic priorities in response to ongoing geopolitical uncertainty.[14]	Compliance checkboxes become operational safeguards. Configuration monitoring catches risk before it disrupts production.

None of these scenarios require a facility to start over. They require the connections between existing systems to be made, and a layer of intelligence to do something useful with what those connections reveal.

The plant manager who reaches this operating state doesn't stop dealing with hard problems. Hard problems don't go away. What changes is the quality of the information available when those problems arrive, and the speed and confidence with which they get addressed.

That's the other side of the complexity tax. **A confident facility.**

Sources

1 Deloitte, "2025 Manufacturing Industry Outlook," 2025
2 Octave, "2026 pulse of quality in manufacturing," 2026
3 World Economic Forum, "Technology Convergence: The New Logic for Competitive Advantage," 2026
4 Quality Magazine, "How Industrial IoT Trends Are Reshaping the Manufacturing Industry," 2025
5 Deloitte, "2026 Manufacturing Industry Outlook," 2026
6 Verdantix, "Strategic Focus: How Industrial Agility Is Shaping Digital Strategies," 2026
7 IBM Security, "X Force Threat Intelligence Index 2024," 2024.
8 Dragos, "ICS/OT Cybersecurity Year in Review 2024," 2024.
9 IDC, "IDC MarketScape: Worldwide AI-Enabled Asset-Intensive Enterprise Asset Management Applications 2025–2026 Vendor Assessment," 2025.
10 John Coykendall , Kate Hardin , John Morehouse , Victor Reyes , Gardner Carrick, "Taking charge: Manufacturers support growth with active workforce strategies," Deloitte, 2024
11 Siemens, "The True Cost of Downtime 2024," 2024
12 McKinsey, "Playing offense: Industrials staying ahead in the energy transition," 2024
13 McKinsey, "Want to break the productivity ceiling? Rethink the way work gets done," 2025
14 PWC, "New world, new rules: Cybersecurity in an era of uncertainty," 2025

About Octave

Octave is a leader in enterprise software, turning data into decisive action and intelligence into your edge. Our software solves for and simplifies complexity, from the design and build to operations and protection of people, property, and assets– for any scope, at any scale. For decades, we've partnered with customers to sharpen performance, elevate efficiency, and amplify results. From factory floors to entire cities, our solutions are tuned to scale up what's possible from day one onward.