

7 Trends

Shaping the Future of Manufacturing & Distribution

A 2027 outlook for the teams that keep industrial operations running

Introduction: An Industry in Transition

Manufacturing and distribution will enter 2027 more connected, more automated, and more data-driven than at any point in history. Factory networks that were once isolated now exchange data with enterprise systems, AI has moved from the analyst's dashboard toward the plant floor, and the line between a physical process and its digital representation continues to blur. Each of these shifts promises real gains in productivity, quality, and resilience, and each is already reshaping how plants are designed, staffed, and defended.

Taken together, the seven trends in this paper describe a single arc. Operations that were once isolated, manual, and static are becoming connected, automated, and adaptive. Data moves freely between the plant floor and the enterprise, software makes more decisions with less human intervention, and the physical process and its digital model increasingly shape each other in real time. The result is an industry that can do more, and do it faster, than at any point before it.

That same progress raises the stakes on a question that tends to receive less attention than innovation itself: when a more connected, more automated system is interrupted, whether by a cyberattack, a hardware failure, or a simple bad edit, how quickly can it be brought back? Each trend adds capability, and with it a new dependence on the software that runs production. Keeping that software understandable and recoverable is a thread that runs quietly through all seven trends. The sections that follow take each trend in turn, ground it in current data, and consider what it asks of the people who run the plant.

~50%

Of enterprises will use AI agents to redefine how humans and machines collaborate by 2027

IDC

49%

Year-over-year rise in ransomware groups hitting industrial firms

Dragos, 2026 Year In Review

\$1.4T

Annual cost of unplanned downtime, world's 500 largest firms

Siemens, True Cost of Downtime

~20%

Of OT incidents take more than a month to remediate

SANS, 2025 State of ICS/OT

01

The Line Between IT and OT Continues to Disappear

The isolation that once protected the plant floor is gone

The separation between information technology (IT) and operational technology (OT), once enforced by air gaps and separate teams, has largely dissolved. Competitive pressure to use plant-floor data, combined with a threat environment that no longer respects the old boundaries, has pushed convergence from a gradual trend to the default state of the modern plant. The practical consequence is that the plant floor is now part of the enterprise attack surface rather than a world apart, connected to the same networks, and reachable through the same pathways, as the rest of the business.

The difficulty is that convergence connects systems faster than it secures them. In its 2026 review, Dragos found poor IT/OT segmentation in 81 percent of the assessments it conducted, and SANS reported that half of the OT incidents it studied began with unauthorized external access. A breach that once stayed in the enterprise can now reach the controllers that run production, which means the blast radius of an incident has grown even as detection has improved.

Because the plant floor is no longer isolated, prevention is only half the assignment. When an attack reaches OT through one of these new IT-to-OT connections, the question that decides the outcome is how quickly ICS code can be restored to a known-good state. Convergence raises the stakes on recovery precisely because it removes the isolation that used to limit damage. But when recovery is designed into these connected systems from the start rather than treated as an afterthought, convergence becomes a source of resilience, instead of exposure.

02

Version Control Comes to Industrial Code

Faster change without rollback is just faster risk

Industrial engineering teams are modernizing how they manage change. Under pressure to move faster, standardize across sites, and coordinate across the IT, OT, and security functions that once worked in isolation, plants are adopting more collaborative, more automated ways of proposing, reviewing, and releasing changes to the code that runs production. The gains are real: shorter cycles, higher quality, and better coordination than previous manual models offered.

That acceleration exposes an old gap. Enterprise software teams have had version control, change history, and automated rollback for decades. Industrial code has largely gone without. Configuration snapshots are often exported by hand before a firmware update, stored in scattered folders, and rarely tested for whether they will load again. Increasing the pace of change on top of that foundation raises both quality and risk, because every faster deployment is also a faster path to an unrecoverable state if something goes wrong.

This is where an OT backup and code management platform comes into play: the version control, automated backup, and change-visibility discipline that IT has had and OT has lacked. A platform like this gives every change to industrial code an author, a timestamp, and a rollback point, so a change that behaves badly can be reversed to the last known-good version rather than reconstructed from memory.

03

Agentic AI Moves Onto the Factory Floor

AI is moving from advising operators to acting alongside them

Artificial intelligence in manufacturing continues to advance beyond the copilot stage toward agentic systems that can plan and act with limited supervision. IDC predicts that by 2027, half of enterprises will be using AI agents to redefine how humans and machines collaborate. On the plant floor, that trajectory points toward agents that schedule maintenance, tune processes, and adjust supply-chain decisions on their own, promising speed and consistency that manual operation cannot match.

Autonomy also multiplies the ways a plant's known-good state can quietly drift. The same technology introduces new exposure: IBM found that elevated use of unsanctioned, or shadow, AI added an average of 670,000 dollars to the cost of a breach, and that 63 percent of organizations still have no AI governance policy in place. Gartner expects more than 40 percent of agentic AI projects to be abandoned by the end of 2027, often because governance and oversight could not keep pace. Agents that can modify control logic, without a reliable record of what they changed, turn a productivity tool into an untraceable source of drift.

The safeguard is not to slow the technology but to make its changes visible and reversible. When agents write and adjust industrial code, a reliable record of that code becomes essential: continuous change history that captures who, or what, changed a controller, clear summaries of what changed, and the ability to roll back to a known-good state when an automated decision goes wrong. Governance frameworks and human oversight matter here, but so does the more basic ability to see and undo what an agent did. Autonomy is safe to adopt in proportion to how well an organization can understand and reverse the actions its agents take.

04

Reliability Becomes a Financial Discipline

Every idle hour is margin walking out the door

Reliability is moving from a maintenance concern to a boardroom metric. As margins tighten and new capacity is expensive and slow to add, leaders are recognizing that the cheapest production is the production they already have, provided they can keep it running. Unplanned downtime is the single largest drain on that capacity, and its cost compounds: a stopped line idles labor, wastes energy and material, delays orders, and forces expensive catch-up. Treating uptime as a financial discipline, rather than a number the maintenance team watches alone, is becoming a defining trait of well-run operations.

The scale of the loss is significant. Siemens estimates that unplanned downtime now costs the world's 500 largest companies about 1.4 trillion dollars a year, equal to 11 percent of their revenues, up from 8 percent in 2019. ABB found that the average financial burden of unplanned downtime is about 170,000 dollars per hour. Measured against numbers like these, reliability is not a cost center. It's one of the largest and most controllable levers on margin that a plant has.

This is where recovery enters the efficiency conversation. Uptime is decided not only by how rarely a line stops, but by how quickly it comes back once it does. The faster an operation can restore a known-good state, the fewer hours it loses to idle equipment, reprocessing, and scrap, and the more of its capacity turns into finished product. Recovery is also indifferent to the cause. A flood, a failed controller, a bad edit, or a retiring engineer who took undocumented knowledge with them all require the same thing: a trusted, known-good state to restore. Building that capability once shortens the path back from every kind of stoppage, which is why reliability and fast recovery are becoming two names for the same objective.

05

Digital Twins Become Autonomous

A digital twins is only as trustworthy as the code it mirrors

Digital twins have evolved from static visualizations into systems that use real-time data to predict, optimize, and increasingly act on their own. Adoption reflects the momentum: roughly 69 percent of manufacturers already use digital twin technology in some form, the market is projected to grow from about 36 billion dollars in 2026 to well over 200 billion dollars within the next decade, and Gartner expects 40 percent of large companies to apply digital twins to revenue-generating projects by 2027. Organizations that have deployed them report meaningful gains, including reductions in unplanned downtime of around 65 percent.

A twin, however, is only as trustworthy as the code and configuration it mirrors. When the real ICS code drifts away from the modeled one, through an ad-hoc change on the floor, an agent's adjustment, or an undocumented fix, the twin begins optimizing against a version of the plant that no longer exists. The more autonomous the twin, the more consequential that gap becomes, because it's acting on the wrong version.

Keeping a twin honest depends on the same discipline that enables recovery. Version control establishes a verified baseline of the real industrial code, and continuous drift detection surfaces the moment the physical environment diverges from the trusted state. That baseline does double duty. It keeps the twin aligned with reality, and it's the exact known-good state you restore to when something goes wrong. In an autonomous plant, the model and the recovery point are two uses of the same source of truth.

06

The Workforce Is Retiring Faster Than It Can Be Replaced

When a veteran engineer leaves, the knowledge to run the line can go too

The workforce that built and programmed much of today's installed base is retiring, and there are not enough new workers to take its place. [Deloitte and the Manufacturing Institute](#) estimate that manufacturers could need as many as 3.8 million new workers between 2024 and 2033, and that roughly half of those openings, about 1.9 million jobs, could go unfilled if the skills gap is not closed.

In many plants, the details of how a line actually runs, the quirks of a particular controller, the reason a program was written a certain way, and the fix that appears in no manual, live in the memory of the person who has run it for 20 years. That knowledge is rarely written down, and it doesn't always transfer well. In a [2025 survey by APQC](#), a knowledge-management research organization, 41 percent of organizations said they rarely or never capture the know-how of employees before they retire, even as respondents expected roughly half of their workforce to leave or retire within five years. When those workers go, a plant can lose not only expertise but the ability to recover when something breaks.

This is why capturing knowledge in the code itself, rather than in people, is becoming a priority. When every controller program and configuration is automatically backed up, versioned, and attributed, the record of how a plant runs no longer depends on who is still on staff. A newer engineer can see what changed, when, and why, and can restore a known-good version without reconstructing it from someone's memory. Automation will keep taking on more of the work, but the more of a plant that runs on software, the more its resilience depends on that software being captured and recoverable rather than carried in the heads of a shrinking, aging workforce.

07

Cybersecurity Becomes a Board-Level Priority

Attention is on closing the OT recovery gap

Industrial cybersecurity has become a standing board concern, driven by an attack surface that keeps expanding as agentic AI, IT/OT convergence, and increasingly convincing phishing and impersonation attacks open fresh paths in. The threat data explains the attention. Dragos reported that 119 ransomware groups struck industrial organizations in 2025, a 49 percent increase over the 80 groups tracked the year before, affecting some 3,300 organizations, with manufacturing accounting for more than two-thirds of the victims. The average industrial-sector breach reached 5.56 million dollars, the largest year-over-year increase of any sector studied, according to IBM.

The instinct at board level is still to fund prevention, yet the current data shows that prevention is not where industrial organizations are failing. Nearly half of OT incidents are detected within 24 hours, and most are contained within 48 hours, but close to 20 percent still take more than a month to fully remediate, and a small share take longer than a year, according to SANS. The same research found that only 57 percent of organizations have an OT-specific incident response plan, just 25 percent test it at least quarterly, and only 14 percent feel fully prepared for emerging threats. The gap is not detection, but restoration—that's the OT recovery gap.

Boards are beginning to ask a sharper question: not whether the organization can keep every attacker out, which no one can promise, but how quickly it can restore production when one gets through. That reframing moves meant time to recovery (MTTR) to the center of the conversation and positions OT disaster recovery as the last line of defense. Detecting a breach is not recovering from one. The board-level metric that matters in 2027 is how fast the plant comes back.

A Common Thread: Designing for Resilience

Placed side by side, the seven trends tell one story. Operations are becoming more connected, more automated, and more autonomous, and in the process more of what makes a plant run is moving out of people's hands and into software. Convergence opens new pathways between the enterprise and the plant floor. Modernized change management and agentic AI increase the pace and independence of change. Digital twins turn live production into a working model, and an aging, retiring workforce makes capturing how a plant runs more urgent than ever. The economics of reliability raise the cost of every idle hour, and cybersecurity moves the whole subject into the boardroom. Different as they are, each trend increases the amount of control-system logic in production, the number of ways it can change, and the cost of losing it.

That shared direction points to a capability worth planning for deliberately: the ability to restore a known-good state when something interrupts production, whoever happens to be on shift when it does. In enterprise IT, systems are versioned, backed up automatically, and restored in days. In operational technology, ICS code is often unversioned and backed up by hand, held together by the memory of the people who wrote it, which is one reason industrial incidents can take substantially longer to resolve, with close to 20 percent taking more than a month to fully remediate, according to SANS. As plants adopt the technologies in this paper and their most experienced engineers retire, capturing that knowledge in versioned, recoverable code, rather than leaving it in individual hands, becomes less a security afterthought and more a design decision made alongside the rest of the modernization.

Conclusion: Adopt Deliberately

The future of manufacturing and distribution is being built now, and it runs on more code, more connection, and more autonomy than ever before, and increasingly on the expertise of a workforce that is beginning to retire. Each trend in this paper offers real advantage, and each deepens the plant's dependence on software that has to keep working, and that has to be recoverable when it does not. The organizations that lead through 2027 will not simply be the ones that adopt these technologies fastest. They will be the ones that adopt them deliberately, pairing new capability with the visibility, discipline, and resilience needed to depend on it, so that what runs the plant is captured and recoverable rather than carried in the heads of a shrinking pool of experts. Progress and preparedness are not competing priorities. In a modern plant, they are the same project.

About Copia Automation

Copia Automation brings version control, automated backup, and recovery discipline to industrial code, giving engineering and security teams a single system of record for the software that runs the plant. Learn more at copia.io.