Manufacturing in the age of AI:

The network driving the factory floor and beyond

Analysis of findings from manufacturing, production, and distribution respondents in “No time to wait: The accelerating impact of AI on campus and branch networks”

Introduction

The manufacturing sector is currently navigating one of the most consequential technology crossroads in modern history. As AI transitions from experimental pilots to enterprise-wide deployment, it is exposing vulnerabilities in the campus and branch networking infrastructure that powers factory floors, distribution centers, and branch operations.

84% of manufacturing leaders say that executive leadership views campus and branch networks as strategic enablers of AI and business growth.

Data from the Cisco report **No time to wait: The accelerating impact of AI on campus and branch networks** (April 2026), a global survey of more than 3,400 senior IT and network leaders, reveals that manufacturers are not passive observers of this shift. In fact, manufacturing leaders are moving faster than their peers to adopt AI. At the same time, they are hitting a wall.

The following four themes define this critical inflection point and provide a roadmap for IT leaders looking to bridge the gap between ambition and reality.

The confidence gap: Aligning AI ambition with infrastructure reality

There is a notable disconnect among manufacturing leadership. While boardroom-level awareness is high, IT leaders are increasingly wary of the underlying foundation.

The study shows that 84% of respondents agree that their respective executive leadership view campus and branch networks as strategic enablers of growth for both AI and business. Yet, there is a realization that their networks are now supporting intensive, bursty traffic from AI tools and agentic workflows that those networks were not designed to handle.

72% of manufacturers have more confidence in their AI strategy than in their network's ability to support it.

The confidence gap is not merely a technical concern; it is a business risk. When the infrastructure cannot reliably deliver the data throughput or the low-latency response times required by sophisticated AI models, the entire investment in AI software becomes a sunk cost.

Strategic takeaway

By auditing current networking infrastructure against specific AI roadmap requirements, manufacturers can shift the conversation from strategic vision to operational results. This requires a transparent dialogue with stakeholders about the necessity of foundational upgrades as a prerequisite for AI success, ensuring that business ambitions are backed by technical reality.

Physical AI as a new frontier for connectivity

Unlike other industries that primarily grapple with cloud-based generative AI, manufacturing is contending with physical AI—the integration of robotics, autonomous systems, and connected machinery. Physical AI creates unique, bursty, and high-density traffic patterns that legacy networks were never architected to handle.

But the need to handle the issue is imminent. While manufacturing respondents expect to see 99% increases in overall network traffic from physical AI deployments in the next three years, they expect this increase to reach 48% within the coming year.

Many manufacturing networks are already seeing this massive influx of machine-to-machine traffic, where robots, sensors, and autonomous guided vehicles communicate in real-time to optimize production lines. These systems rely on a constant stream of data to function, and they are highly sensitive to even micro-seconds of latency. When the wireless network falters, the physical production line halts.

52% of manufacturing respondents point to wireless networks within campus locations as the area with the greatest increase in performance and capacity requirements.

For the modern factory, Wi-Fi has evolved from a convenience layer into mission-critical infrastructure. With 52% of respondents identifying campus wireless as their greatest pressure point, it is evident that any degradation in connectivity translates directly into unplanned operational downtime and reduced throughput. To succeed, manufacturing networks must evolve to support the specific latency requirements of autonomous systems.

Strategic takeaway

Because physical AI systems have zero tolerance for latency, manufacturers must transition from best-effort connectivity to precision-engineered performance. This means ensuring they have the latest wireless and high-density switching capabilities to handle the specific, bursty traffic patterns of autonomous systems. The wireless network needs to be as reliable as a wired connection.

The security paradox: convergence in an era of complexity

Manufacturing environments are uniquely complex due to the convergence of information technology (IT) and operational technology (OT). This blend creates a sprawling attack surface to which AI is not just adding new traffic; it is fundamentally complicating the policies, monitoring, and controls that security teams rely upon.

Manufacturing leaders are not standing still. Recognizing that reactive security postures are insufficient against the sophistication of AI-enabled threats, 88% of manufacturing organizations have implemented new security controls. Yet the pace of those AI-driven threats is still outstripping the ability of traditional security teams to manage them.

72% of manufacturing respondents agree that AI-related security threats are evolving faster than their organization's ability to adopt security controls.

The result is a major blind spot that can jeopardize security posture. As AI workloads expand the number of endpoints and data flows, security teams are struggling to maintain coherent, enforceable policies. Undetected anomalies within the network can lead to significant operational disruptions or, worse, physical safety risks on the factory floor.

Strategic takeaway

Move beyond perimeter-based security. Protect critical operations with the network itself. Today's IT/OT convergence and increasing east-west traffic from AI require consistent segmentation and a zero-trust approach to access—ensuring that every entity connecting to the network, human, or AI agent, is authenticated and verified.

The high cost of wait-and-see

The research also showed a direct correlation between network stagnation and business failure. In a sector where competitive advantage is won or lost on the production line, the wait-and-see approach is no longer a neutral position—it is a strategic liability.

Seventy-five percent of manufacturing IT leaders explicitly acknowledge that delaying network modernization puts near-term AI initiatives in jeopardy. This, in turn, places that organization at risk of falling behind competitors who are already leveraging AI to redefine productivity.

76% of manufacturing respondents agree that failure to adapt their network infrastructure could result in missed business opportunities.

In a sector where leaders agree that failure to adapt can come at the price of missed opportunities, incremental improvements to legacy infrastructure will not suffice for the next wave of AI-driven applications. The decision to modernize today is not just an IT expense but, in effect, a proactive measure to protect market share and ensure the agility needed to capitalize on the next wave of AI innovation.

Strategic takeaway

View the network modernization as the critical backbone for all other AI investments. Strategic modernization is essential to ensure the network scales with the pace of AI, drives performance that bests the competition, and upholds the heightened security demands of the AI era.

The imperative: A roadmap for modernization

The era of treating campus and branch networks as passive commodity infrastructure is over. For manufacturing, the network is now the primary determinant of whether an organization can compete, innovate, and operate securely.

To move forward, IT leaders should focus on three core pillars:

- **Infrastructure audit:** Mapping current network capacity against the projected traffic demands of upcoming physical AI and IoT deployments.
- **Unified policy management:** Breaking down the silos between IT and OT security to ensure comprehensive visibility across the entire operational footprint.
- **Executive alignment:** Leveraging the current boardroom interest in AI to audit infrastructure against specific roadmap goals and prioritize AI-ready infrastructure that makes those outcomes possible.

The question for manufacturing leaders is no longer whether to modernize, but how quickly they can pivot. When asked if they expect to face network capacity limits within the next 2-3 years due to AI growth, 75% of manufacturing respondents said yes—placing manufacturers among the top industries anticipating such constraints. This reflects an understanding that network modernization is not an IT project but a strategic business imperative.

By addressing the confidence gap, prioritizing the unique demands of physical AI, and tackling the security paradox head-on, IT leaders can transform their networks from a bottleneck into the engine of their company's future.

There's no time to wait.

See how the AI-ready Secure Network Architecture from Cisco is built for the reality modern manufacturing companies face.

Learn More

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices**