Insight report

expereo

The Smart Factory **Assurance Gap**



From connected production to measurable resilience and operational control

What manufacturing technology leaders modelled online discussions suggest about the networks supporting Industry 4.0, industrial security and scalable operations.

Explore the report



Evidence and methodology

This report examines the connectivity challenges facing distributed, multi-site manufacturing organizations. It focuses on the interface between factory operations and enterprise networking, including the performance, resilience, security and management of connections linking production sites, applications, data environments and partners.

We used AI-assisted audience profiling and inferential modelling to analyze 103,080 publicly expressed online opinions over the 12 months ending 11 October 2026. The source platforms were X, Quora, Reddit, Bluesky, TikTok and Threads. Our research attributes a 95% confidence interval and 5% margin of error to its methodology. These are modelled interpretations of public discussion, not answers to a direct survey or audited measures of organizations' network practices.

We use selected social research findings as directional evidence and distinguish them from independent research, including Deloitte's 2025 US smart manufacturing survey and technical guidance from NIST, the Cybersecurity and Infrastructure Security Agency (CISA) and ISA. Different sources address different populations and questions; their figures should not be directly compared as if they share a common sample or measurement basis.

The research combines AI-assisted audience profiling with analysis of publicly expressed online opinions. Using inferential audience modelling, the research identifies discussions likely to reflect the perspectives of senior technology, infrastructure and network leaders within distributed, multi-site organizations.

The underlying analysis **examined 77,876 online opinions over a 12-month period** ending 11 October 2026, drawn from X, Quora, Reddit, Bluesky, TikTok and Threads. Our research reports a 95% confidence interval and 5% margin of error for its analysis. The findings are supplemented by independent industry research, technical standards and analysis from organizations including MEF, NIST, Uptime Institute and Enterprise Management Associates.

As the findings are derived from AI-modelled online opinions rather than direct survey responses, they should be interpreted as directional indicators of industry perspectives and emerging priorities, rather than independently verified measures of organizational adoption, performance or investment.

Executive summary

Smart factory connectivity keeps machines talking and production moving. But when factories span multiple locations, keeping everything running smoothly takes effort. From connecting older equipment to meeting growing automation demands, there's plenty to keep network teams busy. Reliable infrastructure and the right managed services help manufacturers keep factories connected and ready for whatever comes next.

Today, smart manufacturing is moving beyond isolated technology pilots. Connected production systems, industrial analytics and more automated workflows are creating new dependencies between factory operations, enterprise networks and cloud environments. Reliable connectivity matters, but so does knowing whether the network can support production when conditions change or a component fails.

The analysis suggests a tension between manufacturing ambition and operational assurance. Industry 4.0 and AI are prominent investment priorities, yet the same research classifies many discussions as lacking formal connectivity performance measurement. The latter finding requires careful interpretation, but it raises a useful leadership question: how can manufacturers show that their network operating model is ready for the demands being placed upon it?

The report develops five connected priorities for CIOs, infrastructure leaders and manufacturing IT/OT decision-makers.

Five themes consistently emerged across our research:

1. **Turn Industry 4.0 ambition into network requirements.** Start with the processes, data flows and operational outcomes that connectivity must support.
2. **Link network visibility to production impact.** Move beyond device status and uptime towards meaningful cross-site performance evidence.
3. **Secure IT/OT connections without disrupting operations.** Protect industrial systems with controls designed for availability, safety and clear ownership.
4. **Scale factories through coordinated network operations.** Standardize where it helps, while respecting local site conditions and dependencies.
5. **Make AI and automation accountable.** Use reliable data and governed processes before expanding autonomous intervention.

The central argument is that smart factory readiness depends less on the number of connected machines or networking technologies adopted than on whether manufacturers can demonstrate reliable, secure and manageable connectivity across their estate.



Expereo perspective:

> **Manufacturers aren't short of ambition. The gap is between what factories want their networks to do and what teams can prove those networks are actually doing. Uptime tells you a link is alive; it doesn't tell you whether production is getting what it needs. Closing that gap is the shift from being connected to being in control.**



Matthew Lea

Product Development Director, Expereo

Why this matters

For manufacturers, a production site is not simply another enterprise office. Connectivity choices can affect maintenance decisions, quality monitoring, site expansion, collaboration between operational teams and the ability to restore services during an incident.

The strategic opportunity is to join site-level requirements with a coherent, enterprise-wide network operating model: one that supports local production needs while giving central teams visibility, supplier coordination and clear accountability across locations.

The objective is to make connectivity an operational asset that can be measured, improved and trusted, enabling smarter manufacturing without adding unnecessary complexity or exposing critical production processes to unmanaged risk.

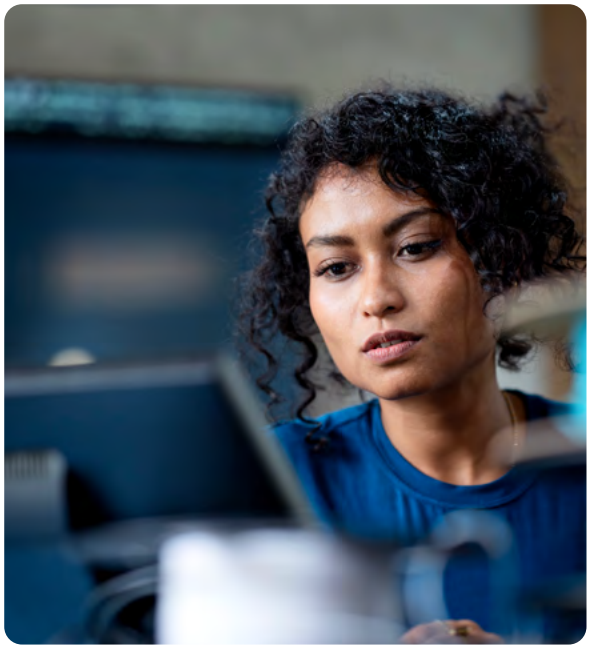


Theme 1:
Smart factory ambition is outpacing operational assurance

Why digital investment creates value only when the supporting network is ready for production demands.

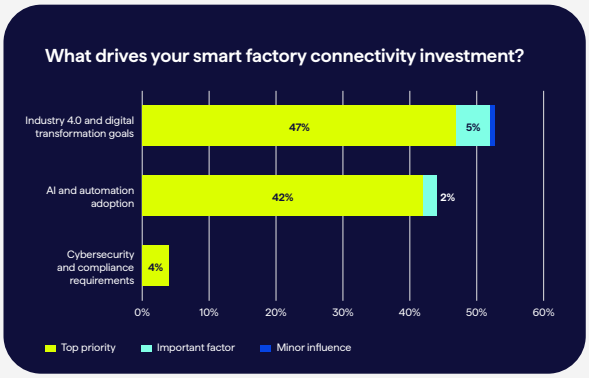
Manufacturing technology strategies increasingly depend on the flow of timely and trustworthy information. Production scheduling, quality analytics, equipment monitoring and enterprise planning may involve different applications and systems, but their value depends on data moving reliably between the right locations and people.

That makes connectivity a business-critical component of transformation rather than a background utility. It also changes the questions that technology leaders need to ask. Before expanding automation, organizations must understand which processes are sensitive to delay, which depend on external services and how failures will affect production at individual sites.



Investment priorities reveal the scale of ambition

Our research into manufacturing discussions found that 47% were classified as identifying Industry 4.0 and digital transformation as a top driver of smart factory connectivity investment; 42% identified AI and automation adoption as a top driver. These are categories of inferred opinion, rather than verified statements of spending or implementation.



Investment in the future has 3 focus points

The wider manufacturing context supports the importance of these investment goals. **Deloitte's 2025 Smart Manufacturing and Operations Survey**, based on 600 executives at large manufacturers with US headquarters or operations, found that 92% believed smart manufacturing would be a principal driver of competitiveness over the next three years. Its respondents reported benefits from earlier implementations but also identified operational risk and the challenge of managing transformation. Deloitte's figures describe a direct survey, not the same population or questions as our study.

The significance for network leaders is that automation programs and connectivity plans cannot be developed in isolation. A new monitoring platform, for example, may require data from older control systems at several factories, secure transmission to a central environment and consistent access for engineers. The business case rests on the complete chain working, not simply on the existence of a network connection.

Define what a production-ready network must deliver

The term “smart factory connectivity” can cover several layers, from industrial Ethernet and local wireless access to wide-area connectivity, cloud access and remote engineering. They do different jobs. A low-latency control loop may need to operate locally even if its connection to enterprise reporting systems is interrupted; a central analytics workload may tolerate some delay but need dependable access to data across many plants.

A useful starting point is to classify production systems by their tolerance for disruption and their external dependencies. That allows technology and operations teams to separate requirements for local safety and control from the wider needs for monitoring, information exchange and remote service access. It also reduces the risk of specifying the same architecture for every facility regardless of what the site produces.

Deloitte’s survey found that 45% of respondents reported using an architecture standard and 54% a data standard for smart manufacturing initiatives. The percentages do not establish how effective those standards are, but they reflect the role of common design and data practices in more repeatable transformation. For distributed manufacturers, an equally important principle is to document where local variation is necessary and who approves it.

Expereo perspective:

“Every automation program makes a promise to the business, and the network has to keep it. The manufacturers making real progress start with the production outcome, then work back to what the network must deliver at each site. Do it the other way around and you end up with impressive technology sitting on foundations nobody has tested.”



Jean-Philippe Avelange

Chief Information Officer, Expereo

Strategic insight

Smart factory maturity begins when network requirements are defined against production outcomes, not just technology deployment milestones.

Once those outcomes are clear, the next task is to make the network performance behind them visible and measurable.

For manufacturing leaders, this means ensuring that connectivity investments support the operational priorities that matter most: maintaining production continuity, enabling automation, protecting critical systems and scaling connected operations across multiple facilities.

Achieving this requires closer alignment between IT, OT and business teams, with clear expectations around network reliability, performance, security and accountability. Rather than treating connectivity as a supporting infrastructure decision, organizations should recognize it as an essential component of their wider manufacturing transformation strategy.

Once these outcomes are established, the next challenge is ensuring that network performance can be consistently monitored, measured and linked to the production activities it supports.

Move from activity to evidence

Manufacturers should set explicit measures for critical workloads before deploying additional connected systems. These can include availability of the relevant service path, application response times, incident detection and restoration, and the ability to continue essential operations when an external connection is unavailable. Success may look different at a high-volume assembly line, a batch-production plant or a remote processing site.

A transformation program should also define its operational owners. Engineering teams understand how equipment behaves; security teams evaluate exposure; network teams understand paths, providers and traffic. None of these perspectives alone can establish whether a connected production process is ready to run at scale.



Theme 2:

The visibility gap between network performance and production outcomes

Why knowing a connection is active does not tell an organization how well it supports manufacturing.

Manufacturers may monitor links, devices and service availability without being able to explain whether network behavior is affecting production. A plant might report no wide-area outage while data from a machine historian arrives late, an engineering application becomes unresponsive, or a remote quality team loses timely access to operating information.

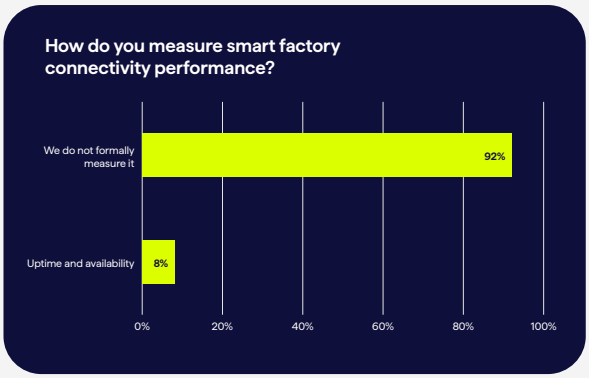
This distinction matters across a multi-site estate. Network teams need to understand where a problem begins and how far it extends, but factory operations leaders need to understand which production activities it affects. Effective assurance connects these two views.



The gap in formal performance measurement

The research classified 92% of manufacturing discussions as indicating that smart factory connectivity performance is not formally measured, compared with 8% associated with uptime or availability measurement.

This suggests a potential gap between maintaining connectivity and systematically evaluating its effectiveness. Without established performance measures, manufacturers may struggle to identify recurring network issues, assess service quality consistently or demonstrate whether connectivity investments are supporting production requirements.



Performance is not a major metric.

While not every production interruption is caused by connectivity problems, the absence of consistent measurement makes it harder to distinguish network-related disruption from equipment failures or wider operational issues. This can complicate troubleshooting, investment decisions and efforts to improve performance across multiple sites.

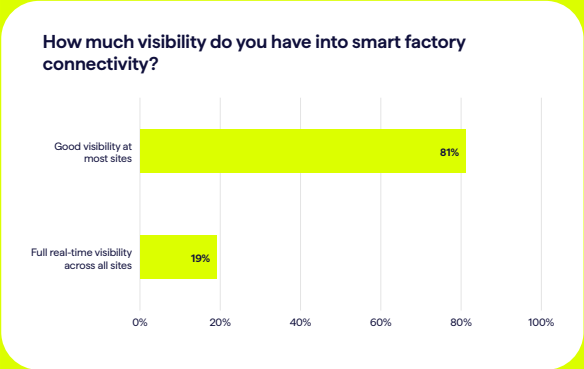
Even where uptime and availability are monitored, these measures offer only part of the picture. A network may remain technically available while latency, packet loss or intermittent degradation affect the applications and systems supporting production.

For manufacturing technology leaders, the priority should therefore extend beyond measuring whether networks are operational towards understanding how effectively connectivity supports production continuity, operational efficiency and business performance.

Visibility does not automatically mean assurance

A separate finding provides another perspective. The research classified 81% of discussions as indicating good connectivity visibility at most manufacturing sites, while 19% were associated with full real-time visibility across all sites.

This distinction matters for distributed manufacturers. Having visibility across most facilities can support everyday network management, but maintaining a consistent view across every location becomes more challenging when sites operate different technologies, equipment and connectivity arrangements.



Visibility is mostly high

Importantly, these two questions were analyzed separately. We cannot conclude that organizations reporting good **visibility are the same organizations that do not formally measure network performance.**

Nevertheless, the findings highlight a useful distinction: visibility provides information about network conditions, while operational assurance requires agreed performance measures and an understanding of how those conditions affect production.

Another research finding reinforces the importance of this distinction. Some 37% of discussions indicated uncertainty about how much production downtime could be attributed to connectivity issues, highlighting a potential gap between monitoring network conditions and understanding their operational consequences.

Without consistent incident attribution and performance measurement, manufacturers may struggle to distinguish connectivity-related disruption from equipment failures, application issues or other production challenges. This makes it harder to identify recurring problems and prioritize improvements across facilities.

Develop a shared view of critical dependencies

The A credible measurement approach starts with knowing which assets and connections matter. In August 2025, CISA and international partners issued **Foundations for OT Cybersecurity: Asset Inventory Guidance**, recommending that operators document OT assets, their communications and their criticality. The guidance also addresses network and system diagnostics, performance monitoring and reporting. It is a technical reference, not a survey of manufacturing maturity.

Consider a manufacturer whose three plants send production data to a shared analytics platform. The central dashboard may report missing readings, but each site could have a different root cause: a local device gateway, congested Internet path or service interruption at the application provider. A common incident record, aligned service telemetry, and a documented dependency map help narrow the fault domain before teams decide on corrective action.

The information must also have context. Latency thresholds that are acceptable for scheduled reporting may be unsuitable for a real-time remote collaboration session. Likewise, a short interruption affecting non-essential analytics is not equivalent to a loss of connectivity supporting time-critical plant coordination.

Measure service quality and production impact together

Enterprises should use a compact set of measures that can be collected consistently across priority sites: path and application availability, latency and packet loss where relevant, time to detect and restore service, repeat incidents, and the number or duration of business-impacting events. Operational teams can then record which production process was affected, what workaround was available and whether an incident crossed the boundary between OT, site IT, WAN and cloud.

The aim is not to attribute every production stoppage to networking. Many interruptions originate elsewhere, and causal attribution should be supported by evidence. Rather, the aim is to understand when connectivity contributes to degradation and whether changes to network design or service management reduce the operational impact.

A useful baseline can be established plant by plant and then compared across sites with similar requirements. This can reveal whether one location has recurring access issues, whether multiple sites share a failing dependency or whether the problem is specific to an application. It also supports more defensible decisions about upgrading access, changing routes or reviewing provider arrangements.



Strategic insight

Network visibility creates business value when it translates into measurable service quality, clearer incident attribution and a better understanding of production impact.

For manufacturers operating across multiple sites, this means moving beyond basic connectivity monitoring towards a consistent view of network performance, critical applications and operational dependencies. By establishing shared performance measures and connecting network incidents to production outcomes, organizations can identify recurring issues, prioritize improvements and make more informed infrastructure investment decisions.

In industrial environments, however, improving network performance and visibility must go hand in hand with protecting production continuity. As IT and OT environments become increasingly connected, manufacturers must ensure that efforts to strengthen security and operational control do not introduce additional risks to the systems keeping production running.

Expereo perspective:

“A small exchange of production data can matter more than a large transfer of sensor readings. Missing work instructions or unavailable inspection results can delay production even when network dashboards show no fault. The useful measure is whether each connection supports the task that depends on it. Linking network and application performance to those tasks helps teams establish whether connectivity is contributing to a delay and where an improvement would have the greatest effect.”



Julian Skeels
Chief Digital Officer, Expereo



Theme 3: **Securing connected production without compromising continuity**

Why industrial cybersecurity must account for reliability, safety and the realities of existing equipment.

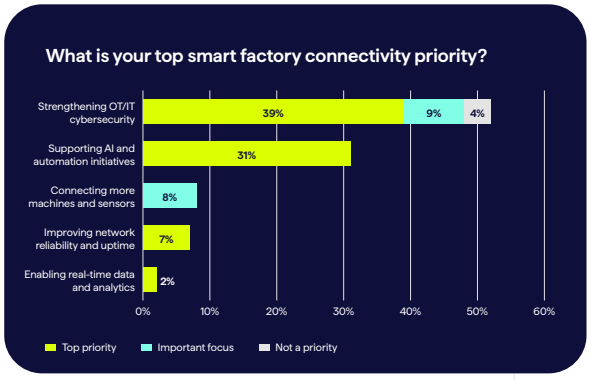
Connecting factory environments to enterprise applications and external partners can create new business value, but it also changes the pathways through which risks can reach production systems. Manufacturers must protect these connections while recognizing that industrial environments have different operational constraints from conventional office networks.

For example, a security control that requires frequent reauthentication or automatically blocks a service may be acceptable for a non-critical office application. The same behavior could disrupt an industrial workflow if it interrupts a communication path at the wrong point in a production cycle.

Security is an operational priority, not a separate project

The research classified 39% of discussions as identifying stronger OT/IT cybersecurity as the top smart factory connectivity priority, ahead of supporting AI and automation initiatives (31%) and improving network reliability and uptime (7%).

This reflects the importance of protecting increasingly interconnected manufacturing environments, where operational equipment, enterprise IT systems and external services often depend on shared infrastructure.



Priorities differ across factory floors.

For manufacturers operating across multiple facilities, cybersecurity cannot be treated solely as a technology implementation or compliance exercise. Security decisions must account for the availability of production-critical systems, the risks associated with connecting previously isolated equipment and the operational consequences of restricting access or changing network configurations.

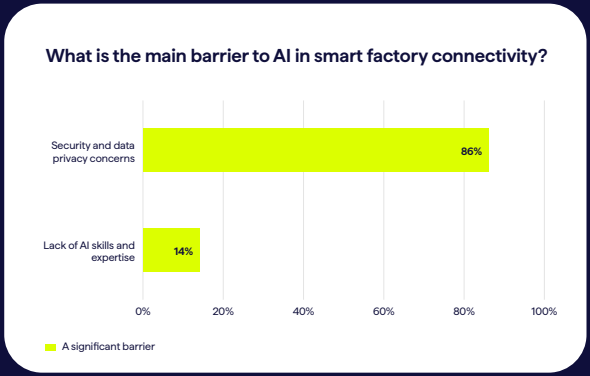
The **NIST Guide to Operational Technology Security, SP 800-82 Revision 3** reinforces this distinction, recognizing that industrial security must address the specific performance, reliability and safety requirements of operational technology. Because these systems interact directly with physical processes, security controls and changes need to be evaluated alongside operational and engineering requirements to avoid introducing unnecessary disruption.

The **ISA/IEC 62443 standards series** provides a complementary perspective by emphasizing shared responsibility across asset owners, system integrators, product suppliers and service providers. For distributed manufacturers, this reinforces the need for clearly defined security responsibilities, particularly where global network partners, local automation suppliers and site-specific maintenance teams operate across interconnected environments.

The strategic challenge is therefore to establish consistent security governance across manufacturing sites while preserving the operational flexibility and control required to keep production running.

Security concerns are also influencing AI readiness

Another finding classified security and data privacy concerns as a significant barrier to AI adoption within smart factory connectivity for 86% of discussions, compared with 14% identifying a lack of AI skills and expertise.



Barriers to entry are still tough.

This highlights an additional consideration as manufacturers explore AI-enabled monitoring, predictive maintenance and more intelligent network operations.

These capabilities may depend on access to information from operational systems and enterprise networks, creating new requirements around data governance, access permissions and the protection of sensitive production information.

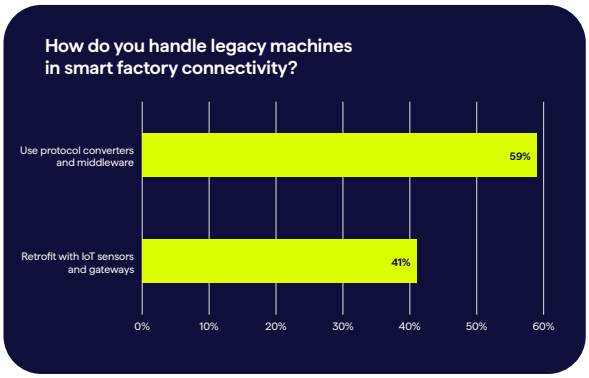
Manufacturers therefore need to consider not only whether their infrastructure can support new AI applications, but also how these technologies can be introduced safely, governed consistently and monitored without compromising essential production processes.

The challenge is not simply to strengthen security controls, but to ensure that they support innovation without introducing unacceptable risks to operational continuity.

Both findings reflect inferred online discussion patterns rather than independently verified organizational practices. They address separate questions and should not be interpreted as directly comparable measures.

Legacy equipment shapes the security and integration challenge

59% of the opinions on handling legacy equipment were classified as favoring protocol converters or middleware and 41% as favoring retrofitted IoT sensors and gateways. These are useful examples of integration approaches, but they are not mutually exclusive engineering choices. A facility may use both depending on equipment age, available interfaces and the data required.



Legacy approaches are divided into two approaches.

Infrastructure leaders in distributed manufacturing handle legacy machines in smart factory connectivity by bringing older equipment online without having to replace machinery that's still doing its job. Legacy machines account for more than **70% of manufacturing equipment**. Replacing all that machinery would come at an enormous cost, so finding ways to bring older equipment online makes financial sense.

A practical integration plan should begin with an inventory of assets and dependencies, then distinguish systems that can be connected through supported interfaces from those needing additional gateways or compensating controls. Many older devices were designed for long operational lives, not for exposure to modern enterprise networks. Increased data access may therefore require segmented architectures, tightly scoped remote access and verified recovery procedures.

The CISA-led 2025 asset-inventory guidance recommends documenting OT assets and the network relationships between them, including supported protocols and criticality. Such records support both cybersecurity and reliability because they help teams understand which connections should be protected and what could be affected by a change.

Design security around safe operating conditions

Manufacturers should separate administrative access from production data flows, limit third-party access to what is necessary and review how credentials, segmentation and monitoring work across the IT/OT boundary. The aim is not to assume that any single label, including zero trust or SASE, proves safety or resilience. These approaches can support security objectives, but they are not substitutes for equipment-level engineering requirements or tested operational processes.

The response to a cyber incident must also be planned jointly. Isolating a compromised system may reduce exposure, but the plan should specify how production teams will maintain safe operation, who authorizes disruptive changes, and how services will be restored. These responsibilities become more complicated when access providers, managed network partners and plant specialists are different organizations.

Security and continuity are therefore complementary rather than competing objectives. They require risk-based controls that can be implemented and tested without creating unnecessary production disruption.

Strategic insight

Secure factory connectivity depends on industrially appropriate security controls, clear accountability across IT, OT and service providers, and an operating model that protects production continuity.

For manufacturers managing multiple facilities, this requires a coordinated approach to network security, access management, incident response and operational governance. Responsibilities must be clearly defined across internal teams and external partners, while security measures need to accommodate the performance, reliability and safety requirements of production environments.

As manufacturers introduce AI, automation and increasingly connected systems, security must also become an integral part of technology planning rather than a barrier addressed after deployment. Establishing these foundations enables organizations to adopt new capabilities with greater confidence while managing operational risk.

The next challenge is ensuring that these standards, responsibilities and controls can be applied consistently as manufacturers expand, connect new facilities and modernize existing production sites.

Expereo perspective:

“In a factory, a security control that stops production causes the outage it was meant to prevent. Industrial environments need protection designed around how they run, with clear ownership across IT, OT and every partner involved. Security and continuity aren’t competing goals: get the design and accountability right and each strengthens the other.”



Jean-Philippe Avelange
Chief Information Officer, Expereo



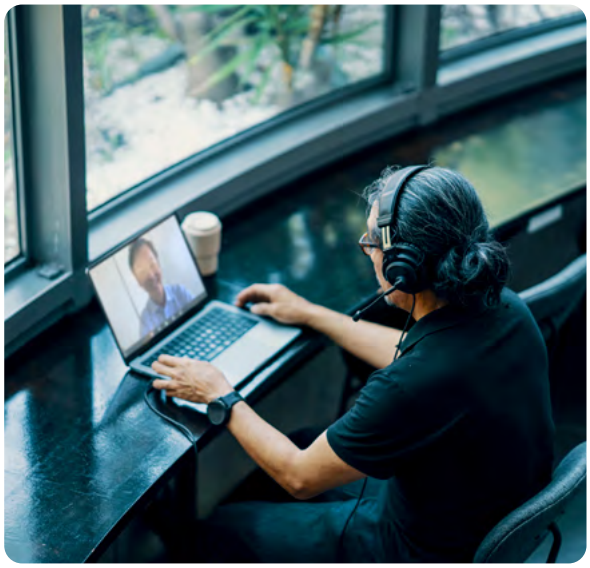
Theme 4:

Scaling smart factories requires a coordinated network operating model

Manufacturers need repeatable service management without losing the local flexibility production demands.

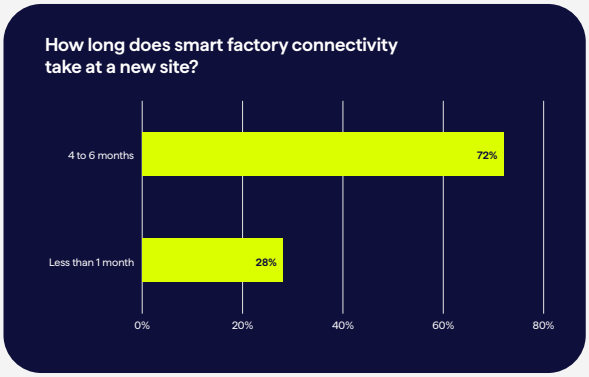
A multi-site manufacturer rarely operates identical plants. Facilities may have different machines, operating schedules, local access markets and levels of digital maturity. Yet corporate technology teams are often expected to maintain common security standards, dependable enterprise applications and a clear view of connectivity performance across all of them.

The strategic challenge is to coordinate this diversity rather than erase it. A local factory may need an independently operating OT network, while shared IT services and production data flows depend on resilient inter-site and cloud connectivity. Both sets of requirements must be addressed in the wider network operating model.



New-site deployment is about more than ordering a circuit

72% of the analyzed opinions on new-site deployment reported four to six months to establish smart factory connectivity, while 28% indicated less than one month. A fully commissioned factory network involves more activities than provisioning an Internet connection or managed WAN service, and this distinction matters commercially.



Factory commissioning may involve on-site cabling, safety checks, machine integration, network testing, security approval and coordination with production windows. A global connectivity partner may influence lead times for access and enterprise networking but cannot necessarily control the timetable for all local industrial infrastructure.

For leadership teams, the actionable question is which delays are repeatable and preventable. A site rollout that starts from scratch may need to rediscover technical requirements, access availability, security exceptions and support responsibilities. Standard network profiles, agreed documentation and early checks of local carrier options can reduce avoidable handovers without pretending that every site is the same.

Standardize the operating model, not every site configuration

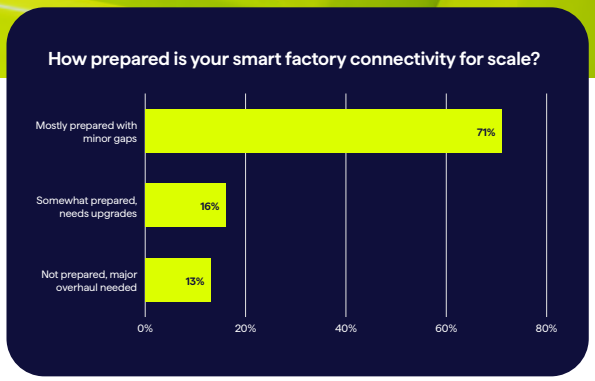
Deloitte's 2025 Smart Manufacturing and Operations Survey indicates that some large manufacturers are developing common architecture and data standards to support smart manufacturing. Among 600 surveyed manufacturing executives, 45% reported using an architecture standard, 54% a data standard or unified data model, and 48% a training and adoption standard.

These findings suggest that manufacturers are establishing more consistent approaches to technology deployment, data management and organizational readiness. For network leaders, this reinforces the value of defining common service requirements, operating controls and deployment processes across facilities, while allowing flexibility for site-specific machinery, connectivity conditions and safety requirements.

A coordinated operating model should cover how connectivity services are ordered, monitored, changed and restored, including the responsibilities of local teams, central IT, network providers and specialist integrators. One view of service ownership and incident escalation can be more useful than forcing every plant into a single access technology or network configuration.

This also changes how supplier diversity should be evaluated. Manufacturers may benefit from different access carriers or connectivity technologies in different regions, whether for availability, resilience or local practicality. The problem arises when contracts, service information, support channels and performance reporting cannot be coordinated across those providers.

At the factory floor, Wi-Fi, wired industrial networks and private cellular technologies may each have a place. Across sites, SD-WAN and managed Internet services address different needs such as traffic management, access to applications and inter-site connectivity. These are complementary architectural layers, not competing answers to the same question. The appropriate combination depends on the workload and site.



Preparedness is not a one-size-fits-all standard.

Make scalability an operational capability

Our research classified 71% of opinions as describing their smart factory connectivity as mostly prepared for scaling, albeit with minor gaps; 16% as somewhat prepared but needing upgrades; and 13% as requiring a major overhaul. These classifications suggest that scaling often involves incremental improvements, but they should not be interpreted as independently assessed readiness scores.

These findings suggest that manufacturing organizations face different levels of network readiness as they expand connected operations. For some, scaling may involve targeted improvements to network capacity, monitoring or connectivity management. Others may need more substantial infrastructure upgrades or changes to their network operating model before supporting additional sites, equipment and applications.

The challenge is compounded by the diversity of technologies found across manufacturing environments. Equipment from different suppliers may rely on incompatible protocols, legacy machinery can require additional integration, and increasing numbers of connected systems create greater demands on network performance, security and operational oversight.

Scalability should therefore be understood as more than the ability to accommodate additional devices or bandwidth. It is the ability to expand connected operations while maintaining consistent performance, resilience, security and operational control across different manufacturing sites.

These classifications highlight why manufacturers should evaluate scalability against their specific operational requirements rather than assuming that existing connectivity will accommodate future demands.

Manufacturers can test that readiness through a repeatable site-assessment process. Before a new plant is connected or an existing one expands, teams should verify site criticality, capacity and resilience requirements, carrier availability, application and OT dependencies, security boundaries, support ownership and a staged acceptance process. Where possible, the same information should feed service management and ongoing monitoring after launch.

Deployment success should be judged through meaningful measures, including time from approved design to service readiness, number of avoidable rework cycles, consistency of service documentation and the ability to meet performance requirements after go-live. These measures help distinguish a faster launch from a launch that merely transfers problems into operations.

Strategic insight

Scaling connected manufacturing requires more than network capacity. It depends on a coordinated operating model that combines consistent standards, measurable performance and clear accountability across diverse sites and providers.

For manufacturers operating multiple facilities, the priority is to establish repeatable approaches to connectivity deployment, service management and operational assurance, while retaining the flexibility needed to accommodate different equipment, local infrastructure and production requirements. Rather than treating each expansion or modernization project as a standalone exercise, organizations should build the processes and capabilities needed to scale efficiently without compromising network resilience, security or production continuity.

With these foundations in place, manufacturers can move beyond managing connectivity reactively towards using consistent network information to anticipate issues, optimize performance and support more intelligent operations. The next challenge is ensuring that AI and automation build on reliable data and established operational controls.



Expereo perspective:

“No two factories are the same, and they shouldn’t have to be. What should be consistent is how connectivity is designed, delivered, supported and measured, wherever a site is and whichever local providers it relies on. Standardize the operating model, not every detail, and each new site becomes a repeatable step rather than a fresh start.”

Matthew Lea

Product Development Director, Expereo



Theme 5:

From automation ambition to intelligent manufacturing operations

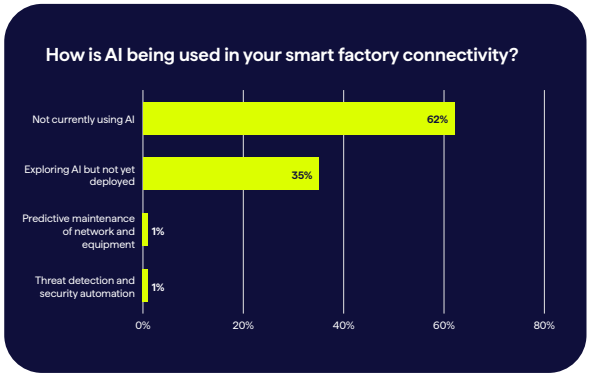
Why AI can support more proactive networks, but reliable data and governed action come first.

AI is frequently discussed as part of the future factory, from quality analysis to predictive maintenance and production scheduling. Network operations present a narrower, but potentially valuable, application: recognizing changing conditions, identifying likely causes of service degradation and helping teams act before incidents affect important workflows.

However, the existence of an AI initiative elsewhere in a manufacturing business does not demonstrate that the network itself is managed intelligently. A machine-learning quality model and an AI-assisted network troubleshooting process use different information, operate under different constraints and should be assessed against different outcomes.

Separate ambition from deployment

62% of our audience indicated no current AI use within smart factory connectivity operations, with 35% exploring AI but not deploying it. Only 1% were associated with predictive maintenance of network and equipment and a further 1% with threat detection and security automation. The categories are specific to connectivity operations, not all uses of AI in manufacturing.



AI hasn't quite reached the factory floor.

For context, Deloitte's 2025 Smart Manufacturing and Operations Survey found that 29% of surveyed large manufacturers were using AI or machine learning at the facility or manufacturing-network level, while 24% had deployed generative AI at that scale. A further 38% reported piloting generative AI.

These findings illustrate the growing interest in AI across manufacturing, but they measure broader technology adoption rather than AI specifically applied to connectivity operations.

They should not be interpreted as directly comparable with our findings.

The distinction is important. Experimenting with AI using existing business or production data is different from introducing AI into the systems responsible for managing factory connectivity. Legacy equipment, fragmented network information and the need to protect production continuity can complicate deployment, particularly where automated decisions might influence critical infrastructure.

For manufacturing network leaders, the opportunity lies in carefully targeted applications, such as identifying early signs of network degradation, accelerating incident diagnosis and improving visibility across distributed facilities. Realizing these benefits requires reliable performance data, clearly defined operational responsibilities and appropriate safeguards.

The strategic implication is therefore not that manufacturers are failing to adopt AI, but that **AI-enabled network operations represent a distinct capability that must be developed, governed and measured against operational outcomes.**

Operational intelligence depends on trustworthy information

Before introducing automated diagnosis or path changes, network teams need accurate inventories, usable telemetry, consistent incident records and an understanding of how individual services support applications and processes. If these foundations are incomplete, AI can generate plausible but misleading explanations or recommend an intervention that addresses the wrong component.

The CISA-led asset inventory guidance provides a practical basis for documenting OT assets and their communications. This matters because a plant with several generations of equipment may have hidden dependencies or proprietary protocols that are not obvious from general-purpose network monitoring. Visibility into external connectivity and managed services should complement, not replace, what local OT specialists know about production behavior.

A controlled use case might correlate repeated interruptions at several sites with a common upstream network path, helping a human operator investigate sooner. Another might prioritize alerts based on the criticality of affected applications. The value should be measured through faster diagnosis, fewer avoidable escalations and demonstrable improvements in service quality, rather than the volume of automated decisions.



Expereo perspective:

“AI will make networks more proactive, but only if it’s built on data people can trust. Start with AI that helps engineers diagnose faster, prove it works, then expand with clear guardrails. In production environments, earned confidence beats bold autonomy every time.”

Jean-Philippe Avelange

Chief Information Officer, Expereo

Keep engineering and governance in the loop

An intervention that is appropriate for ordinary enterprise traffic may be unsafe or disruptive for industrial control systems. Network automation affecting production-critical traffic should operate within defined change limits, approved maintenance windows where relevant, clear decision-making authority and established rollback procedures. Teams should also be able to determine which data informed an action and whether the result achieved its intended objective.

The **NIST Guide to Operational Technology Security, SP 800-82 Revision 3** emphasizes the importance of protecting the reliability, performance and safety of industrial systems when introducing security controls or operational changes.

These principles also have implications for AI-assisted network operations. The **NIST AI Risk Management Framework** provides a complementary foundation, reinforcing the importance of defined oversight responsibilities, appropriate testing and ongoing risk management.

For manufacturers, this means establishing clear boundaries around what can be automated, which decisions require human approval and how potential impacts on production-critical systems should be assessed before wider deployment.

A mature approach can begin with AI-assisted decision support rather than full autonomy. This allows teams to improve data quality, validate recommendations and build confidence before introducing progressively more consequential automated actions. It also recognizes that industrial engineers, network specialists and security professionals bring different forms of expertise that must work together within a coordinated operating model.



Strategic insight

Intelligent factory networking should be measured by the quality of operational decisions, the reliability of production-critical services and the value delivered to the business, not by the number of AI tools deployed.

For manufacturing leaders, the priority is to ensure that AI-assisted network operations build on accurate data, consistent performance measurement and clearly defined responsibilities across IT, OT and external service providers. Automation should be introduced progressively, with appropriate engineering oversight, tested safeguards and evidence that it can improve incident response, reduce disruption and support more predictable network performance.

Across the five themes, the central requirement remains consistent: connected manufacturing depends on networks that are designed around production outcomes, made visible and measurable, secured for industrial environments and managed effectively as operations scale.

The next step is translating these principles into practical priorities that help manufacturers strengthen network assurance, improve operational resilience and realize greater value from their connectivity investments.

Summary:

Five priorities for the next era of smart factory connectivity

Turning connected manufacturing ambition into secure, measurable and scalable operations.

The research points to a practical conclusion: technology adoption can expand what factories are capable of doing, but the reliability of the supporting network operating model determines how confidently those capabilities can be used across sites.

Five connected priorities emerge from the research, highlighting the capabilities manufacturers need to translate smart factory ambition into secure, measurable and scalable network operations.

- **Translate digital strategy into network requirements:** Industry 4.0 and AI are influential investment priorities, but business value depends on knowing which production processes and data flows require connectivity, which can operate locally and what constitutes acceptable degradation.
- **Make connectivity performance accountable to production:** Monitoring needs to progress from service and device status to consistent evidence about critical applications, fault domains, incident restoration and operational impact. Reported visibility should be supported by agreed measurement definitions.
- **Treat IT/OT security and continuity as one design challenge:** Industrial security requires equipment-aware controls and shared accountability across IT, OT and providers.
- **Coordinate global operations while respecting local requirements:** Diverse factory sites need coordinated deployment, supplier management and incident ownership, not one mandated technology.
- **Introduce automation through evidence and governance:** AI-assisted networking needs dependable data, engineering oversight and measurable results before greater autonomy.

These priorities inform the practical readiness assessment that follows.



Smart Factory Network Readiness Scorecard

A practical assessment of the capabilities behind connected production

The six-dimension scorecard assesses how manufacturers manage connectivity across sites, applications and operations. It is a qualitative discussion tool drawn from the evidence, not a statistically validated benchmark.

Dimension	Developing	Established	Advanced
1. Production-critical performance	Success is measured mainly through circuit uptime; production impact is hard to identify.	Critical paths and applications have defined baselines, alerts and named owners.	End-to-end service evidence links network health to production impact and recurring improvement.
2. Asset and dependency visibility	Inventories and monitoring are fragmented by site, supplier or technical domain.	Critical OT assets, routes, external services and dependencies are documented and reviewed.	Cross-site visibility and dependency maps support coordinated diagnosis and proactive planning.
3. Industrial security and continuity	Controls and recovery responsibilities vary; industrial change implications are unclear.	IT/OT boundaries, access policies and incident escalation are defined and tested for priority processes.	Risk controls, recovery tests and accountable decisions are embedded in ongoing operations.
4. Cross-site service coordination	Carrier services and incident processes are managed separately across facilities.	Central teams can see key services, providers and support owners through consistent processes.	Diverse suppliers operate within a coordinated performance, change and assurance model.
5. Deployment and scalability	Each site launch needs substantial bespoke planning and post-launch correction.	Reference designs and acceptance checks reduce avoidable variation in priority sites.	Repeatable rollout processes flex to local constraints and demonstrate predictable service readiness.
6. Intelligent operations and value	Alert handling is reactive; automation lacks reliable data or clear measures of success.	Teams use consistent telemetry and selected governed automation to improve resolution.	Intelligent actions are evaluated for safety, service performance and business value.

How to use the scorecard

Organizations should use the scorecard to identify material gaps, not to maximize scores indiscriminately. The most valuable improvement may be better visibility for a high-risk plant, improved accountability across carriers or a clearer process for approving network changes that affect production.

1. **Start with business impact.** Prioritize locations, workloads and dependencies where performance or disruption would have the most important operational consequences.
2. **Establish evidence and targets.** Agree measurable baselines for service performance, restoration, deployment lead times and supplier coordination, using definitions shared by operations and IT.
3. **Assign ownership and review progress.** Identify what site teams, central IT, security specialists, integrators and managed network partners are each responsible for delivering.

Closing Summary

For manufacturers, the next phase of digital transformation will depend on making connected operations dependable at scale. More sensors, more applications and more automation can expand insight and capacity, but they also increase the importance of understanding service dependencies, managing risk and responding consistently when conditions change.

There is no single architecture for every factory. Local production environments require different technologies and safeguards, while enterprise leaders need a common approach to cross-site connectivity, performance evidence and operational accountability. The organizations best positioned to progress will define outcomes clearly, measure them consistently and coordinate the different teams and partners on which production relies.

The future of smart factory connectivity is not just about connecting more production assets. It is about knowing that the network can support the business when it matters.

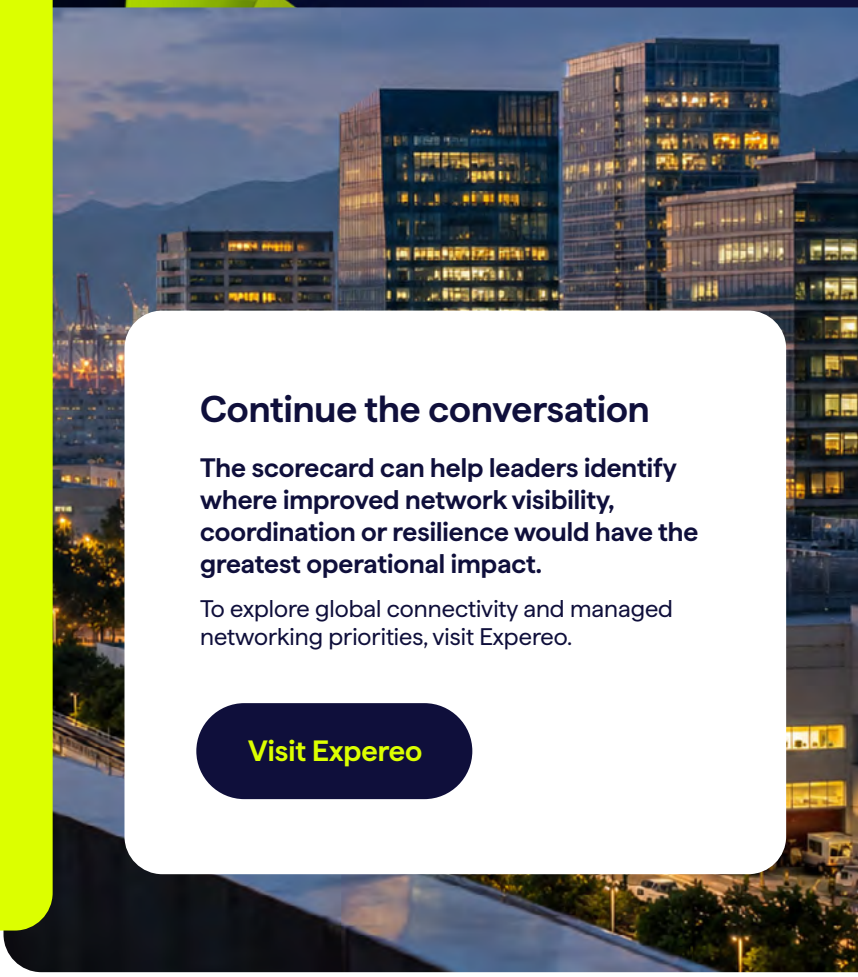
expereo

Closing Perspective:

“The next generation of smart factories won’t be defined by who connects the most machines. It will be defined by who can trust their network when a line is running, a new site goes live, or something fails on a night shift. That trust comes from clear outcomes, consistent evidence and shared accountability. Find your biggest gap, and let’s close it together.”

Julian Skeels

Chief Digital Officer, Expereo



Continue the conversation

The scorecard can help leaders identify where improved network visibility, coordination or resilience would have the greatest operational impact.

To explore global connectivity and managed networking priorities, visit Expereo.

Visit Expereo