Globalstar™

EBOOK

Innovation on the Industrial and Manufacturing Floor

Robotics Enablement via Resilient Networks

The Robotics Revolution in Manufacturing

Industrial and manufacturing environments are facing rapid transformation. Global competition, fluctuating supply chains, and rising demand for mass customization are reshaping production strategies. At the same time, workforce challenges, from skills gaps to safety regulations, are pushing factories to explore new methods of maintaining throughput without compromising quality or worker well-being.

Robotics is emerging as a cornerstone of this evolution. Once limited to fixed, repetitive tasks behind safety cages, today's industrial robots are more intelligent, collaborative, and adaptable. They handle precision assembly, inspection, material handling, and even complex production steps, operating alongside human teams to deliver speed, accuracy, and consistency.

This surge in robotics adoption has been made possible by several technological leaps. AI-driven machine vision systems now allow robots to detect defects, adjust to variances, and learn from data in near real time. Modular, software-defined control systems make it easier to integrate robotics into existing production lines without massive re-engineering. Most importantly, resilient connectivity solutions are enabling these robots to communicate, coordinate, and update data instantaneously across large factory floors.

Legacy Wi-Fi struggles to penetrate dense machinery, metal structures, and interference-heavy environments, while public cellular networks often lack the guaranteed uptime and low latency required. Modern private networking is filling that gap, delivering the robust, interference-resistant foundation that advanced robotics demands.

Manufacturers that embrace robotics and pair it with resilient networks are positioning themselves to thrive in a new era of industrial innovation where flexibility, speed, and intelligence are the true differentiators.

Common Use Cases for Robotics in Industrial and Manufacturing

On modern production floors, robotics enables smarter, faster, and safer operations.

From precision assembly to predictive maintenance, here are the most common use cases driving the next industrial evolution.

Collaborative Robots (Cobots)

These robots work side by side with human operators on repetitive or hazardous tasks, improving safety and output while freeing employees for more skilled work.

Robotic Assembly Lines

High-speed, high-accuracy robotic arms perform welding, painting, drilling, and assembly, ensuring consistent quality and reducing production bottlenecks.

Material Handling and Movement

Robots handle raw materials and finished goods, feeding production lines and moving parts between stations efficiently without human intervention.

Inspection and Quality Control

Vision-based robotics conducts real-time inspections, identifying defects on the fly and allowing immediate corrective action to reduce waste.

Heavy-Lift and Hazardous Environment Robotics

In sectors like mining or metal processing, specialized robots manage dangerous tasks in extreme environments, improving both worker safety and operational uptime.

In industrial and manufacturing settings, these robotics applications depend on ultra-reliable connectivity that performs flawlessly in such challenging environments and scales effortlessly with production demands. A network that falters under load or interference can derail productivity, making resilient, future-ready connectivity a critical part of the equation.

Why Robotics Needs Resilient Networks

Modern robotics has transformed warehouses, logistics hubs, industrial plants, and factory floors into highly automated ecosystems. But these machines, whether they are autonomous mobile robots (AMRs), automated guided vehicles (AGVs), robotic arms, or inspection drones, are only as effective as the networks that drive them. A resilient network isn't just a convenience; it's the backbone that keeps automation running with precision.

Robotics thrives on data. Every movement, sensor reading, and command is transmitted in real time to ensure that robots avoid collisions, stay on schedule, and adapt dynamically to changes in their environment. For example, an AGV in a warehouse may need to reroute instantly if a pallet blocks its path, while a robotic arm in a manufacturing plant may require split-second updates to keep pace with conveyor lines. If a network drops or slows down, operations grind to a halt, creating bottlenecks and costly downtime.

Resilient networks also enable scalability. As organizations deploy more robots across larger or more complex facilities, their communication needs increase exponentially.

A network must maintain low latency, high throughput, and interference resistance, even when supporting hundreds or thousands of devices simultaneously. This level of robustness allows organizations to deploy robotics confidently, knowing that performance will not degrade as demand grows.

Security is another critical layer. Robotics often handles sensitive operational data, blueprints, production schedules, inventory records, so the network must safeguard this information from unauthorized access or interference. A resilient network is built with strong encryption, clear segmentation, and the ability to isolate traffic for specific use cases, preventing disruption and ensuring compliance.

Ultimately, robotics delivers on its promise of speed, precision, and cost savings only when its network infrastructure matches that same standard of reliability and intelligence. A resilient network becomes the invisible engine behind higher productivity, improved safety, and optimized workflows.

What Stands in the Way

Industrial and manufacturing environments introduce a different set of barriers to resilient connectivity. Unlike warehouses, which are mainly open, factory floors are often filled with heavy machinery, production lines, thick concrete walls, and equipment that generates significant electromagnetic interference (EMI). This RF-dense environment can scatter or absorb signals, leading to inconsistent coverage and degraded network performance.

The equipment itself poses unique challenges. Industrial robots often require exact, real-time coordination: fractions of a second matter when robotic arms synchronize with conveyor belts or when automated inspection systems relay high-resolution video streams for AI analytics. Any latency, jitter, or packet loss can disrupt production, damage components, or even create safety risks.

The stakes are higher in manufacturing, where downtime translates directly to lost revenue. A single unplanned stop on an assembly line can cost thousands of dollars per minute. Yet legacy Wi-Fi systems, which depend on multiple overlapping access points, are particularly susceptible to interference and signal degradation in these environments, making them ill-suited for critical automation.

Layout changes further complicate connectivity. As production lines reconfigure to accommodate new products or processes, the network must adapt quickly. Traditional systems require extensive engineering and cabling work to keep up, which can slow innovation and hinder agility.

Industrial environments also tend to have stricter compliance and safety requirements. Networks must support isolated traffic for different processes while maintaining robust security to protect intellectual property and prevent cyber threats. Without a purpose-built, resilient solution, the network becomes a liability instead of an enabler, limiting the full potential of robotics on the factory floor.

The Rising Demand for Private Networking

Across industries, a silent transformation is underway: the migration from public, best-effort connectivity to dedicated private networking. Organizations in warehousing, logistics, manufacturing, and beyond are asking more of their networks than ever before. Automation, AI-driven analytics, and real-time visibility into assets and workflows have become cornerstones of operational efficiency. But these technologies only deliver when the underlying network can meet strict performance, security, and scalability requirements.

This is why private networks, wireless systems that an enterprise owns or controls within its footprint, are seeing explosive growth. Unlike public networks, which are built for mass consumer use, private networks are tuned specifically for the needs of a facility, an enterprise campus, or even an entire supply chain. They provide predictable performance, tight security, and the ability to scale without competing with outside users.

Meeting New Needs

Private networks are gaining traction because they address key pain points that traditional public networks or legacy systems simply can't:

Low Latency and High Reliability

Automation systems and robotics need instant, uninterrupted communications. A private network removes the variability that comes with sharing spectrum and infrastructure with others.

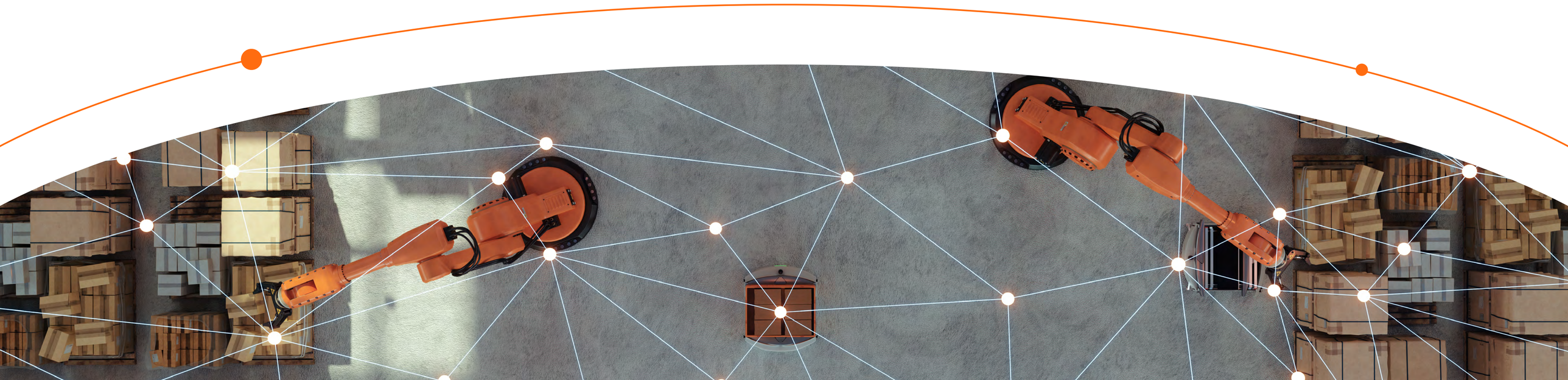
Dedicated Capacity

When a facility runs on its own network, bandwidth can be allocated based on operational priorities. High throughput video streams, edge AI applications, and massive device fleets no longer fight for airtime.

Security and Control

With sensitive operational data flowing constantly, organizations need airtight control over who accesses their network and how. A private network enables segmentation, encryption, and strict governance.

These needs are not niche. From warehouses fulfilling orders in minutes to industrial floors with robots welding alongside humans, reliable connectivity is becoming mission-critical.



Wi-Fi vs. Cellular Private Networking

In most facilities today, Wi-Fi is the default wireless technology. It is inexpensive, widely available, and well understood. But as operations scale and automation increases, Wi-Fi starts to show its limits:

Coverage Gaps

Wi-Fi access points have relatively short range, so large sites require dense deployments. Every access point adds cost, complexity, and potential points of failure.

Interference and Handoffs

In environments with moving robots, high shelving, or dense machinery, Wi-Fi signals can scatter, creating dead zones and forcing constant handoffs between access points. These micro-interruptions may go unnoticed for casual use but are catastrophic for automation.

Lack of Quality of Service (QoS)

Wi-Fi is a shared medium with no guaranteed performance. When multiple devices compete, latency spikes and throughput drops.

Cellular private networks, especially 5G, were designed from the ground up to overcome these issues. A single private cellular radio can cover a much larger area than Wi-Fi, reducing deployment costs and complexity. Handoff issues are eliminated or minimized, as the network can be architected as a “supercell” with seamless roaming across the site. And because private cellular networks can operate on licensed spectrum, they offer interference-free performance and guaranteed QoS, even under heavy load.

Scalability is another differentiator. Private 5G networks are built to support dense device ecosystems with low latency, ideal for environments where automation is growing year over year. Unlike Wi-Fi, which often requires “forklift” upgrades (ripping and replacing hardware) to scale, cellular private networks can grow through software updates and modular expansion.

Use Case Highlight

On a factory floor producing high-value components, robotic arms synchronize with conveyor belts while AI-enabled inspection cameras stream high-definition video for defect detection. Human workers collaborate side-by-side with machines, requiring the utmost in network reliability to avoid errors or safety incidents.

Wi-Fi often buckles under these conditions. Heavy machinery creates RF noise, while concrete walls and equipment racks block signals. Every new production line or machine requires site surveys and new cabling. Performance is unpredictable at best.

A private cellular network transforms the experience. Its larger coverage radius minimizes infrastructure complexity, while licensed spectrum cuts through interference for stable, low-latency performance. The factory can add new robots or reconfigure workflows without a costly network redesign. Real-time video inspection, remote monitoring, and edge AI processes run concurrently with precision control signals, creating a smarter, safer, and more productive environment.

Why Traditional Private Networks Fall Short...

and Why a New Approach is Needed

For years, Wi-Fi has been the default choice for private networks inside warehouses, factories, and logistics hubs. It is familiar, relatively inexpensive, and easy to deploy on a small scale. Yet, as automation accelerates and mission-critical processes move from human control to interconnected systems, these legacy private networks are increasingly showing their limitations.

Coverage and Scalability Challenges

Traditional private networks built on Wi-Fi often struggle in large or complex environments. Their limited range means a dense mesh of access points is required to cover even a moderately sized facility, driving up both initial costs and ongoing maintenance. Every new robot, camera, or sensor adds additional load. When sites expand or workflows shift, the network must often be redesigned or “retuned,” consuming engineering resources and increasing downtime.

Performance Bottlenecks

Wi-Fi was never designed for latency-sensitive applications. In environments where machines communicate hundreds of times per second, even momentary drops or handoff delays can have a significant impact. Robots pause mid-route, video feeds buffer, and time-sensitive control commands are delayed, all of which are small inefficiencies that compound into measurable operational costs.

Interference and RF Noise

Warehouses, industrial floors, and ports are filled with physical barriers and sources of RF noise, metal shelving, heavy equipment, dense fleets of devices, that degrade Wi-Fi signals. The result is unpredictable performance and dead zones that require constant troubleshooting. While public cellular offers broader coverage, it lacks the control, security, and guaranteed capacity that many industries require.

Security and Control Gaps

Traditional private networks can also struggle to meet today’s cybersecurity demands. Shared spectrum environments are more susceptible to interference and eavesdropping, and legacy network designs were not built with granular segmentation and zero-trust principles in mind.

Why a New Approach is Needed

As industries demand real-time data, automation, and advanced analytics, a more resilient and scalable network foundation is critical. Private 5G and other next-generation architectures are purpose-built to address these gaps, offering licensed or interference-free spectrum, ultra-low latency, broader coverage with fewer radios, and software-defined flexibility to evolve as operations grow.

In short, traditional private networks were never engineered for the scale and intensity of today's industrial applications. To unlock the full potential of robotics, AI, and IoT, organizations need a new approach: one that treats connectivity not as an afterthought, but as the foundation of their operational future.

XCOM RAN: Powering Intelligent Connectivity for Industrial and Manufacturing Floors

Industrial and manufacturing environments are undergoing a fundamental shift. Once dominated by isolated machinery and manual oversight, today's factory floors are dynamic ecosystems of robotics, edge-driven analytics, and AI-powered processes. From robotic arms executing micro-precise tasks to real-time vision systems inspecting product quality, these operations depend on networks that are as advanced as the systems they support.

Traditional connectivity solutions fall short in these settings. RF interference from heavy equipment, reflective surfaces, and dense machine clusters creates coverage gaps and latency spikes. Wi-Fi's frequent handoffs disrupt time-critical commands, while public cellular cannot offer the private control or guaranteed quality required in regulated industrial environments.

XCOM RAN provides the backbone needed for this new industrial era. A software-defined radio access network designed for private 5G, XCOM RAN delivers a level of resilience and flexibility that conventional private networks can't match. Instead of relying on fragmented cells with frequent handoffs, XCOM RAN's unique architecture creates a single supercell across the facility. Robots, sensors, and analytics systems experience consistent connectivity everywhere they operate — no interruptions, no dips in throughput.

In manufacturing, this means a robotic welder receives continuous guidance without latency lags. A high-definition inspection camera uploads real-time analytics without clogging the network. Edge AI can process data locally and issue immediate adjustments without waiting on backhaul systems. Because XCOM RAN is software-defined, these capabilities evolve with your needs. Adding new production lines or upgrading analytics software doesn't require ripping out hardware or redesigning coverage maps; updates roll out through the network itself.

Industrial floors are also susceptible to downtime. Even a few minutes of interruption can cost thousands of dollars in lost production. XCOM RAN's interference management, high availability, and native support for critical IoT devices safeguard against these costly pauses, ensuring operations remain fluid and predictable.

Topline Benefits of XCOM RAN in Industrial and Manufacturing

- Single Supercell coverage eliminates handoffs and keeps robotics online
- High throughput supports data-intensive applications like machine vision
- Ultra low latency ensures split-second responsiveness for automated systems
- Software-defined platform future proofs operations without forklift upgrades
- Robust interference mitigation for RF-dense, equipment-heavy environments
- Seamless integration with private 5G cores for custom deployments

Globalstar™

Tap Into the Full Potential of Your Network

Robotics, automation, and mission-critical applications demand more than a basic private network. To truly scale, streamline operations, and stay competitive, you need a solution designed to handle high-density environments, heavy data loads, and zero-downtime expectations. XCOM RAN delivers that edge as a software-defined, future-proof platform that turns your private 5G network into a supercharged foundation for growth.

Take the next step toward seamless connectivity and operational excellence.

Ready to transform your network?

Contact our team of experts to learn how XCOM RAN can support your automation journey.

© 2025 All rights reserved.