XCOM RAN™ by Globalstar

EBOOK

Why Not Wi-Fi?

The Case for Private 5G Networks

Wi-Fi has been the workhorse of enterprise connectivity for decades. From powering office email to enabling warehouse scanners, it has provided a convenient, low-cost way to connect people and devices. For years, it was considered “good enough.”

But the enterprise environment has changed dramatically. Companies are now running robotics, industrial IoT systems, drones, AR/VR, and AI-enabled automation, all of which demand secure, interference-free, low-latency connectivity that Wi-Fi was never designed to provide.

As organizations look to future-proof operations, a new question has emerged: why not Wi-Fi? The answer lies in its limitations and the rise of private 5G as a fit-for-purpose alternative.

Why Wi-Fi Used to Work

When Wi-Fi first became mainstream in the late 1990s and early 2000s, enterprise demands were modest.

The typical workplace relied on it for:

- Email and basic web browsing
- File sharing and light collaboration tools
- Connecting a limited number of laptops, printers, and handheld scanners

Wi-Fi was inexpensive, easy to deploy, and standardized. IT teams could set up access points quickly and expand coverage by adding more. As Wi-Fi standards advanced, throughput improved enough to keep up with consumer and enterprise expectations.

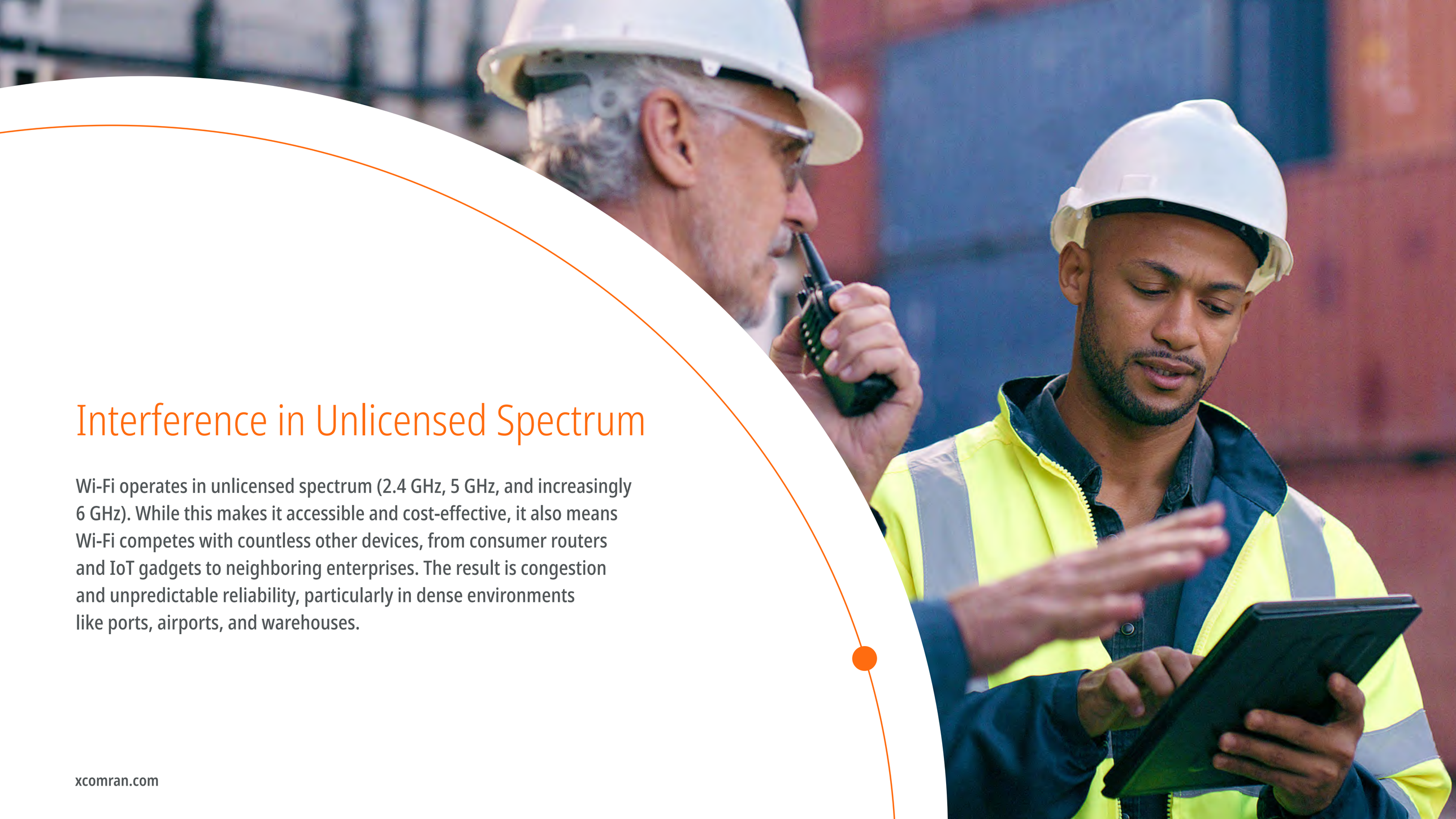
Importantly, most early applications were best effort. If a file download took a few extra seconds or a video call dropped, the consequences were inconvenient but not catastrophic. In this context, Wi-Fi's limitations (unlicensed and shared spectrum, interference, and inconsistent coverage) were tolerable.

For offices, schools, and retail shops, Wi-Fi became the de facto connectivity solution, but it was never engineered for industrial-grade, mission-critical operations.

Why Wi-Fi Falls Short Today

As enterprises digitize, their connectivity requirements have shifted dramatically. Applications that once could tolerate jitter, interference, or downtime now require deterministic performance.

This is where Wi-Fi begins to break down.



Interference in Unlicensed Spectrum

Wi-Fi operates in unlicensed spectrum (2.4 GHz, 5 GHz, and increasingly 6 GHz). While this makes it accessible and cost-effective, it also means Wi-Fi competes with countless other devices, from consumer routers and IoT gadgets to neighboring enterprises. The result is congestion and unpredictable reliability, particularly in dense environments like ports, airports, and warehouses.

Limited Coverage and Range

Wi-Fi signals degrade quickly with distance, obstacles, and environmental conditions. To cover large areas, enterprises must deploy dozens — even hundreds — of access points, each of which requires power, backhaul, and ongoing management. The result is a patchwork network where device performance varies depending on location.

Contention-Based Access

Wi-Fi's "listen before talk" protocol creates collisions and retries when multiple devices attempt to communicate at once. With thousands of sensors, robots, and connected workers vying for bandwidth, contention leads to latency spikes and lost packets. This makes Wi-Fi unsuitable for automation that requires split-second decision-making.

Mobility Challenges

For mobile assets like drones, AGVs (automated guided vehicles), and handheld devices, Wi-Fi handovers between access points are often inconsistent. This leads to dropped connections or disrupted application performance: unacceptable in logistics, safety, or real-time control environments.

Scaling Costs

In theory, scaling Wi-Fi is as simple as adding access points. In practice, dense deployments create more interference, higher management overhead, and diminishing returns. Enterprises end up spending heavily on infrastructure without achieving reliable performance.

Security Gaps

While Wi-Fi security has improved, private 5G introduces SIM-based authentication, stronger encryption, and centralized management. For industries handling sensitive data or critical infrastructure, Wi-Fi remains a weaker link.

Bottom Line

Wi-Fi was designed for convenience, not mission-critical reliability. In environments demanding consistent performance, safety, and control, it simply cannot keep up.

The Case for Private 5G

Private 5G addresses the very gaps Wi-Fi leaves behind. Built on licensed spectrum and 3GPP standards, private 5G is designed for predictable, scalable, and secure connectivity across diverse enterprise environments. Private 5G addresses the very gaps Wi-Fi leaves behind. Built on licensed spectrum and 3GPP standards, private 5G is designed for predictable, scalable, and secure connectivity across diverse enterprise environments.

Licensed Spectrum Advantage

With dedicated licensed spectrum such as Globalstar's Band n53, private 5G eliminates the interference and unpredictability of unlicensed Wi-Fi. Enterprises gain exclusive access to channels that guarantee consistent performance and security.

Wide-Area Coverage

Private 5G can cover large facilities, ports, airports, industrial plants, and energy fields, with far fewer radios than Wi-Fi. This reduces infrastructure costs, simplifies management, and ensures seamless coverage for moving assets.

Deterministic Latency

Private 5G consistently delivers sub-20 millisecond response times, enabling time-sensitive applications like:

- Robotics coordination in warehouses
- Machine vision quality control in factories
- Real-time video feeds from drones in public safety
- AR/VR applications for training and remote assistance

Seamless Mobility

Unlike Wi-Fi, private 5G is engineered for mobility. Devices move across wide areas without handover failures, supporting autonomous vehicles, forklifts, and drones without connectivity interruptions.

Scalability for Massive IoT

Private 5G networks can reliably support thousands of devices per cell — far beyond Wi-Fi's practical limits. This scalability is crucial as enterprises deploy sensors, cameras, and connected assets at an industrial scale.

Security by Design

Private 5G offers SIM-based authentication and end-to-end encryption, providing stronger defenses against intrusion. For industries like defense, energy, and healthcare, this is not optional; it's mandatory.

In short

Private 5G provides the performance, reliability, and control that enterprises now require, and Wi-Fi cannot deliver.

Coexistence, Not Replacement

It’s important to recognize that Wi-Fi isn’t going away. For many environments, it will remain a cost-effective and convenient option. Employees don’t need private 5G to check email, stream a training video, or connect to guest Wi-Fi in a conference room.

The reality is that enterprises need both, but for very different reasons. Wi-Fi continues to serve well in low-stakes, best-effort scenarios where interference or occasional downtime has limited consequences. Private 5G, on the other hand, is engineered for mission-critical operations where performance, reliability, and control cannot be compromised.

Forward-looking enterprises are adopting a hybrid approach, assigning Wi-Fi to its natural role and overlaying private 5G where higher performance is required. This strategic coexistence ensures that organizations optimize cost without sacrificing reliability where it matters most.

USE CASES

Private Wi-Fi vs. Private 5G

Here are real-world examples that highlight how the two technologies perform when applied to the same challenges:

Warehousing & Logistics

Private Wi-Fi

Can support handheld scanners and basic inventory applications, but suffers from interference and inconsistent handoffs when AGVs or drones move across access points. Dropped connections slow automation and increase downtime.

Private 5G

Provides seamless mobility across large facilities, ensuring continuous connectivity for AGVs, drones, and connected workers. Deterministic latency enables real-time coordination and higher throughput.

Manufacturing

Private Wi-Fi

Handles office productivity and light IoT sensors, but struggles with the density and precision required for robotics, machine vision, and predictive maintenance. Congestion leads to jitter and unreliable performance.

Private 5G

Delivers sub-20 ms latency for robotic control, reliable uplink for machine vision, and scalability for thousands of IoT devices. Offers SIM-based security to safeguard sensitive production data.

Ports & Airports

Private Wi-Fi

Fragmented deployments create coverage gaps, while interference from competing signals leads to dropped links for moving assets like cranes, vehicles, and luggage-handling equipment.

Private 5G

Covers the entire area with fewer radios, ensuring consistent connectivity across high-traffic zones. Licensed spectrum guarantees interference-free performance for mission-critical logistics and safety communications.

Public Safety & Emergency Response

Private Wi-Fi

Often unavailable or unreliable in outdoor and disaster environments. Vulnerable to congestion, making it unsuitable for drones, bodycams, or emergency communications.

Private 5G

Provides resilient, wide-area coverage independent of public infrastructure. Supports Drones as First Responders (DFR), real-time video streaming, and secure communications under crisis conditions.

Energy & Utilities

Private Wi-Fi

Challenging to deploy across wide geographies; coverage fades quickly in remote or outdoor environments. Not designed for hazardous area certification.

Private 5G

Scales across onshore and nearshore environments with certified devices (ATEX/CI/DI). Provides continuous visibility into assets, pipelines, and grids, ensuring uptime and worker safety.

Wi-Fi vs. Private 5G

At a Glance

Capability	Private Wi-Fi	Private 5G
Spectrum	Unlicensed (shared, interference-prone)	Licensed (exclusive, interference-free, predictable)
Coverage	Limited range, requires many APs for large areas	Wide-area coverage with fewer radios
Latency	Variable, contention-based, unpredictable	Deterministic, <20 ms, consistent across environments
Mobility	Weak handovers; dropped connections for moving assets	Seamless mobility; designed for AGVs, drones, vehicles
Scalability	Struggles beyond hundreds of devices; congestion common	Thousands of devices per cell with reliable performance
Security	WPA2/WPA3 improvements but still vulnerable	SIM-based authentication + end-to-end encryption
Use Cases	Office productivity, guest access, non-critical IoT	Robotics, automation, ports, energy, public safety
Cost Profile	Low-cost entry, but expensive to scale/manage	Higher upfront investment, but scalable and lower TCO

XCOM RAN™ by Globalstar

Enabling the Next-Generation Demands for Private Wireless

Wi-Fi helped enterprises take their first steps into wireless connectivity. It remains useful for best-effort tasks, but it was never designed for mission-critical operations. Today's demands — automation, safety, scalability, resilience — require a new foundation.

Private 5G networks built on licensed spectrum deliver that foundation, enabling enterprises to innovate and scale without being constrained by interference, downtime, or security risks.

Why not Wi-Fi? Because mission-critical operations demand private 5G.

Learn more at xcomran.com.