Digital Transformation
ACADEMY



Optimizing and securing Wi-Fi in a modern manufacturing facility

Shift your perspective from infrastructure-centric to client-centric visibility, and implement sensors and agents that experience the network exactly as your critical devices do, from the production floor, not the IT closet.

Anil Gupta

What you'll learn:

- Standard network monitoring tools often say everything's fine while production staff report persistent connectivity issues.
- Manufacturing environments are particularly challenging because the RF landscape in them is constantly changing.
- The key to truly optimizing manufacturing Wi-Fi is shifting perspective from infrastructure-centric to client-centric visibility.

Manufacturing facilities are increasingly dependent on Wi-Fi for everything from automated guided vehicles to quality control systems, real-time inventory tracking, and IoT sensors. This connectivity is no longer just convenient. It's absolutely critical to operations.

But here's what many operations leaders are discovering: Standard network monitoring tools often say everything's fine while production staff report persistent connectivity issues. This disconnect isn't just frustrating. It's hurting productivity and potentially introducing security vulnerabilities. What's really happening and what can be done about it?

See also: Nano Dimension wraps acquisition of Desktop Metal

Think of your factory Wi-Fi like a complex highway system with thousands of vehicles. Traditional infrastructure monitoring only shows you traffic from overhead, not what drivers are actually experiencing. When an AGV loses connection for 30 seconds or a quality control tablet keeps dropping packets, your infrastructure tools might not even register the problem.

What makes manufacturing environments particularly challenging is the constantly changing RF landscape. Metal shelving gets moved, inventory levels fluctuate, and machinery creates interference patterns that shift throughout the day. A network that works perfectly during the morning shift might degrade significantly by afternoon.

The security implications are equally concerning. Many manufacturing facilities operate with a mixture of legacy equipment and cutting-edge technology. This creates unique security challenges where outdated devices with minimal encryption capabilities share network space with modern systems. Each intermittent connection disruption doesn't just affect productivity. It creates potential security gaps where unauthorized access could occur.

Client-side intelligence makes the difference

The key to truly optimizing manufacturing Wi-Fi is shifting perspective from infrastructure-centric to client-centric visibility. This means implementing sensors and agents that experience the network exactly as your critical devices do. From the production floor, not the IT closet.

When you monitor from the client perspective, you'll likely discover issues that have been invisible to your traditional tools. Maybe a specific access point performs beautifully for most clients but struggles with certain device types. Perhaps there's interference that only affects a particular frequency at certain times of day. Or most concerning, you might identify suspicious connection attempts or unauthorized devices that your infrastructure tools haven't flagged.

See also: Podcast: Are manufacturers achieving real transformation, or are they just covering up existing inefficiencies?

By collecting and analyzing client-side data with AI-powered tools, you can automatically identify patterns, detect anomalies, and receive specific remediation recommendations. It's like having an expert wireless engineer and security analyst continuously monitoring every corner of your facility.

The cybersecurity imperative

Manufacturing networks face rising cyber threats. The convergence of IT and OT networks creates inherently vulnerable environments where a single compromised device can potentially affect production systems.

Every intermittent wireless connection represents both an operational disruption and a potential security vulnerability. When devices reconnect, they may be susceptible to man-in-the-middle attacks if proper authentication protocols aren't rigorously maintained. Similarly, devices constantly hunting for stronger signals might connect to rogue access points if you lack proper client-side security controls.

See also: Leveraging real-time production data: Q&A with Adam Mullen

Client-side monitoring provides an essential layer of security visibility by identifying several issues. Unauthorized devices attempting to join your network. Unusual device behavior potentially indicating compromise. Anomalous traffic patterns that might indicate data exfiltration. Rogue access points or evil twin attacks targeting your environment. Authentication failures that could signal credential theft attempts.

This visibility becomes even more critical as manufacturing environments adopt increased automation and remote access capabilities. The ability to definitively prove whether issues originate from wireless infrastructure, client devices, or potentially malicious activities is essential for both operational efficiency and security governance.

Strategic optimization without disruption

The good news is that optimizing your manufacturing Wi-Fi doesn't require ripping and replacing your existing infrastructure. By implementing vendor-agnostic client-side monitoring solutions, you can validate network performance across any type of infrastructure.

Start with your most critical production areas or those

experiencing persistent issues. Deploy intelligent sensors that can simultaneously test network performance while monitoring for potential security threats. Establish baseline performance metrics, then leverage AI-powered analytics to identify both immediate issues and emerging trends.

See also: If AI isn't the problem, what is? Maybe trust from frontline teams

Focus on building a comprehensive understanding of your wireless environment that includes several key elements. Where and when performance degrades during normal operations. How different client types experience connectivity across your facility. What security anomalies exist that might indicate vulnerabilities. Which areas are most affected by interference, congestion, or coverage gaps. How your network performs when under peak load conditions.

This approach provides the visibility needed to make targeted improvements rather than costly blanket upgrades. It allows you to prioritize both performance enhancements and security remediations based on actual data rather than assumptions.

The path forward

Manufacturing Wi-Fi will only become more integral to operations as facilities continue their digital transformation journey. The facilities that thrive will be those that implement proactive optimization strategies with security built into their foundation.

See also: How zero-trust data exchange protects manufacturing's private data beyond factory walls

The good news is that you don't need to choose between performance and security. They're inherently connected. By implementing client-side intelligence through a vendor-agnostic platform, you gain the comprehensive visibility needed to support both operational reliability and cybersecurity governance.

The manufacturing facilities that embrace this approach aren't just avoiding downtime and security incidents. They're creating the foundation for continued innovation. When your Wi-Fi infrastructure becomes truly reliable and secure, it opens possibilities for new applications, greater automation, and more efficient operations.

***Anil Gupta** is the co-founder and CTO of Marlborough, Massachusetts-based **Wyebot**, which provides an AI-powered Wireless Intelligence Platform (WIP) that analyzes, optimizes, and identifies problems in Wi-Fi networks. He has over 25 years of experience in the networking industry, over 10 years in wireless, and has held senior technical positions at startup companies as well as large Fortune 500 companies. He has authored 15 patents related to wireless communications.*