Delivering Optimal Wireless in the Glass Manufacturing Plant:

A First Principles Approach

Version 0.1: Initial Draft

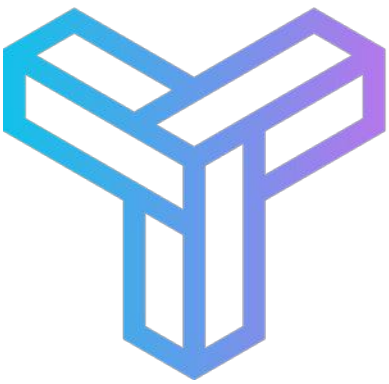
January 2026

By Casey Fahey

Casey.Fahey@NetGoalie.com

in association with

the Toledo Tech Loft



TOLEDO TECH LOFT

Table of Contents

Executive Summary

Wireless connectivity presents a quandary in modern glass manufacturing, one of the most hostile RF (Radio Frequency) environments in industry. Technical challenges notwithstanding, demand is accelerating under Industry 4.0 initiatives, while tolerance for instability and unpredictable behavior continues to shrink.

Thermal gradients, reflective surfaces, movement of materials and equipment, and electromagnetic interference (EMI) destabilize the wireless network. These conditions amplify multipath fading, raise the effective noise floor, and create conditions where conventional wireless designs fail to deliver consistent performance. Traditional remedies such as adding access points, increasing power, and automatic optimization often prove counterproductive.

This paper presents ten first principles and uses them to derive practical design targets. It outlines architectural implications, technology choices, implementation strategies, and validation methods that prioritize predictable delivery, bounded latency, and graceful degradation. Architecture combining multiple technologies, constrained RF design, disciplined spectrum and power management, traffic segmentation, and continuous performance measurement form the foundation of this approach.

The appendix contains supplemental tools to understand failure modes, measure ground truth and to deploy secure solutions.

Performance and reliability design targets come from industrial networking standards (IEEE 3388-2025, IETF DetNet), measurements from analogous industrial facilities, and vendor-reported outcomes from deployments in other challenging environments. Drawing on these standards and research, this paper connects theory to practice and provides a deployment framework to effectively build and manage wireless networks.

Realizing that standards are not solutions, organizations implementing these designs must validate all performance claims through site-specific testing. When designed from first principles, wireless becomes a predictable, scalable enabler. This document provides a framework for achieving that outcome.

The First Principles

Principle 1: Wireless Is a Shared, Finite Medium

Principle
Wireless systems contend for a limited spectrum; capacity does not scale linearly with added devices.

Explanation
Wireless capacity is shared across all transmitters operating in the same domain. As device density increases, contention and interference rise. Increasing transmit power does not create new spectrum and can worsen coexistence by expanding interference domains.

Glass Plant Implication
Deployments must prioritize spectrum governance, channel planning, and segmentation.

Principle 2: The Environment Dominates the Channel

Principle
Physical surroundings shape wireless performance more than protocol features or radio specifications.

Explanation
Reflective surfaces, absorptive materials, obstructions, and electromagnetic noise, overwhelm link budgets and protocol optimizations. Transmission media may not remain stationary or line-of-sight.

Glass Plant Implication
Glass sheets, metal rollers, furnaces, and moving equipment create an RF environment where performance must be engineered for site-specific conditions, not assumed from generic factory models.

Principle 3: Multipath Is the Default State

Principle
Signals arrive primarily via reflected paths rather than direct paths.

Explanation
Multiple delayed signal copies interfere constructively and destructively, producing fading that varies with position, frequency, and time. Signal strength does not guarantee reliable packet delivery.

Glass Plant Implication
Reflective glass and metal surfaces intensify multipath, creating deep fades even at short distances. Designs must assume non-line-of-sight operation and incorporate diversity and redundancy.

Principle 4: Reliability ≠ Throughput

Principle
High data rates do not imply reliable or timely packet delivery.

Explanation
Traffic is often time-sensitive where retransmissions and jitter matter more than bandwidth.

Glass Plant Implication
Systems must be engineered for packet delivery probability and bounded latency.

Principle 5: Mobility Creates Continuous Channel Instability

Principle
Movement transforms wireless links from static problems into dynamic ones.

Explanation
As devices move, transmission media geometry and interference conditions change.

Glass Plant Implication
Changing conditions are amplified by reflections and blockages requiring explicit design treatment.

Principle 6: Much Interference Is Self-Inflicted

Principle
In industrial environments, internal network behavior is often the dominant source of interference.

Explanation
Excessive transmit power and overlapping cells can degrade performance more than external sources. Reflective environments amplify self-generated interference.

Glass Plant Implication
Over-coverage can degrade reliability; constraining is more effective than adding infrastructure.

Principle 7: Determinism Requires Constraint and Control

Principle
Predictable performance requires limiting variability rather than optimizing for average conditions.

Explanation
Adaptive mechanisms can improve throughput but introduce timing variability. Deterministic systems favor scheduled access, fixed parameters, and bounded behavior.

Glass Plant Implication
Static, tightly bounded designs often outperform adaptive schemes in EMI- and multipath-rich zones.

Principle 8: Not All Wireless Traffic Is Equal

Principle
Different applications impose fundamentally different performance requirements.

Explanation
Safety and control traffic demands strict latency and loss bounds, while monitoring and human interfaces better tolerate delay and retries.

Glass Plant Implication
Mission-critical traffic must be isolated from best-effort traffic at the radio and spectrum level.

Principle 9: Failure Is Inevitable - Resilience Is a Design Choice

Principle
Wireless systems destabilize over time and under changing conditions.

Explanation
Environmental changes, equipment drift, added devices, and new interference sources erode performance. Designs must adapt and recover when conditions change.

Glass Plant Implication
Networks must tolerate partial failures through redundancy, path diversity, and graceful degradation.

Principle 10: If It Isn't Measured, It Isn't True

Principle
Wireless performance cannot be validated by design intent alone.

Explanation
Continuous measurement is required to verify assumptions and detect degradation. Models and simulations cannot capture the full complexity of industrial RF environments.

Glass Plant Implication
Site surveys, ongoing monitoring, and stress testing must be treated as core system components.

1. Problem Statement: The Wireless Reality in Glass Manufacturing

1.1 Wireless Demand Is Increasing from All Vectors

Glass manufacturing is evolving from traditional wired networks to wireless, driven by Industry 4.0 initiatives. This increase in wireless demand spans multiple stakeholders and systems, creating a web of competing traffic that strains the finite spectrum. For example:

- Operators, staff, vendors and supervisors: Handheld devices for real-time communication, inventory handling, and tools for on-floor troubleshooting.
- Autonomous and semi-autonomous systems: Automated Guided Vehicles (AGVs), robotic arms, and drone operations require low-latency wireless for navigation.
- Machine interfaces, sensors, and telemetry: IoT sensors monitoring temperatures, vibration and quality via embedded wireless modules (e.g., Wi-Fi or LoRa) drive frequent data streams, prioritizing reliability over throughput.
- Safety, compliance, and monitoring systems: Emergency stops, environmental sensors and regulatory logging require deterministic delivery for safety and compliance.

1.2 Why Glass Manufacturing Is a Special Case

Unlike other industrial settings, glass plants present a hostile RF landscape shaped by material properties and operational dynamics, exacerbating multipath fading and creating dynamic channels.

- High temperatures and thermal gradients: Furnaces operating at 1,500°C+ can cause refractive index gradients in heated air, causing signal bending and phase variations resulting in unpredictable propagation. Electronics and signals must withstand heat, necessitating robust designs with careful antenna placement.
- Reflective and refractive surfaces: Glass sheets and metal rollers cause RF propagation effects through reflection, refraction, and absorption. Conductive surfaces such as metal rollers act as reflectors, while stacked glass sheets create multiple dielectric interfaces that increase attenuation and multipath. Low-emissivity (Low-E) glass incorporates metallic coatings (e.g., silver) intended to reflect infrared radiation; these coatings can also reflect RF energy. This combined dynamic leads to the formation of *RF Shadows*, areas where signals experience deep fades and interference.
- Movement and reconfiguration: Conveyors, cranes, and batch mixers introduce moving blockers/scatterers, altering the broadcast environment in real-time. Plant layouts shift regularly, invalidating wireless maps and demanding adaptive strategies. A moving rack of coated glass can transform a line-of-sight path into an RF Shadow, dropping packets.

- Electromagnetic noise from equipment: Arc furnaces, blowers, and induction heaters generate EMI, adding to self-inflicted and external interference. This noise floor rises with production, clashing with sensitive telemetry.

The extreme thermal environment of a glass plant necessitates focus on infrastructure hardening well beyond standard industrial deployments. Radio components operating in heat zones suffer from an elevated thermal noise floor degrading the Signal-to-Noise Ratio (SNR), resulting in dropped packets and reduced effective range. Hardened enclosures, e.g., IP66-rated with heat exchangers can themselves contribute to interference.

1.3 Bridging to a First Principles Solution

Traditional wireless deployment strategies, such as adding more access points or boosting transmit power can fail in glass manufacturing because of the core physics of the environment. In a landscape defined by thermal gradients, glass and metallic mirrors, and intense EMI, brute force tactics often prove counterproductive, amplifying interference and further destabilizing the channel.

To move from unpredictable connectivity to a deterministic industrial utility, we frame wireless as a constrained, dynamic system. This transition requires moving beyond generic factory models and adopting a first principles framework. This approach does not attempt to overpower; instead, it uses understanding of the environment to ensure designs are stable and resilient.

The following sections translate these realities into a rigorous design methodology. By applying principles of segmentation, diversity, and constraint, we can address the multidimensional demands of modern glass manufacturing. This framework provides a methodology to achieve these objectives:

- **Establish Empirical Baselines:** Moving from design intent to verified performance using tools and standards like NIST research, IETF DetNet/RAW, and IEEE 3388-2025.
- **Decouple Reliability from Throughput:** Prioritizing consistent packet delivery over raw bandwidth for mission-critical control loops.
- **Engineer for Mobility:** Treating movement as a source of continuous channel instability that requires explicit architectural handling.

Key point: When the environment dominates the channel, wireless must adapt to physics rather than attempt to overpower it.

2. Design Requirements Derived From First Principles

> *"Perfection is achieved not when there is nothing more to add, but when there is nothing left to take away,"* - Antoine de Saint-Exupéry

By applying first principles we create tailored strategies emphasizing segmentation, constraint, discipline, and visibility to counter the unique challenges of high-reflectivity, thermal variability, and mobility in glass plants, ensuring scalable, reliable systems.

Key Terms:

- **PDR (Packet Delivery Ratio):** Percentage of packets successfully delivered
- **Latency:** End-to-end delay from source to destination
- **Jitter:** Variation in packet arrival times

2.1 Segmentation by Use Case, Mobility, and Criticality

Effective wireless design begins with dividing the network into logical segments, recognizing that a monolithic approach amplifies interference and fails to address diverse needs. This prevents traffic from degrading critical operations in line with NIST recommendations for industrial zoning, such as those in SP 800-82r2 and AMS 300-4, which emphasize separating zones and conduits to enhance security and reliability.

Drawing from ISA/IEC 62443 and Purdue model best practices, segmentation isolates IT from OT networks, reducing contention in shared ISM bands and enabling deterministic paths per IETF DetNet/RAW. In glass plants, this aligns with Principle 8 by prioritizing safety-critical flows while managing multidimensional growth as set forth in Section 1.1.

Different Problems Require Different Solutions

Segment by application, e.g., dedicated subnets for high criticality applications, isolated from best-efforts traffic. In glass plants for example, isolate control signals from staff Wi-Fi to avoid contention.

- **By Use Case**: Group similar applications e.g., real-time telemetry on dedicated slices or VLANs. This reduces interference from EMI sources like induction heaters, per NIST's emphasis on zoning to limit propagation of disruptions.
- **By Mobility**: High-mobility segments require robust handover with 15-20% overlap and DetNet redundancy, while static segments prioritize low-power, narrowband for efficiency. In reflective environments, mobility segments use directional antennas to constrain RF Shadows.

Prioritize Criticality, Mobility, and Use Case

Define requirements for deterministic paths, ensuring bounded latency for segmented flows.

Example Implementation Table for Glass Plants:

Segment Type	Example Use Cases	Performance Targets	Recommendation
High-Criticality, High-Mobility	AGV navigation, crane control	<20ms latency, >99.99% PDR, redundancy	5G URLLC with network slicing; dedicated slices with deterministic QoS
High-Criticality, Low-Mobility	Furnace telemetry, safety stops	<50ms latency, bounded jitter <5ms	TSCH (Time-Slotted Channel Hopping), WirelessHART / ISA100.11a
Medium-Criticality, Mixed	Quality inspections, sensor monitoring	<100ms latency, >99% PDR (Packet Delivery Ratio)	Wi-Fi 6E with QoS, VLAN isolation
Low-Criticality, Variable	Staff tablets, AR tools	Best-effort, high throughput	Wi-Fi 6 on 6 GHz, wider channels

Key point: Segmentation reduces self-inflicted interference and enables graceful degradation, turning multidimensional growth into manageable zones.

2.2 Cell-Based, Constrained RF Design

To mitigate environmental impacts and multipath, adopt a cell-based architecture with deliberate constraints, favoring smaller zones over blanket coverage. This aligns with NIST guidelines (AMS 300-4, TN 1951) for practical deployments in factories emphasizing reduced overlap.

- **Smaller, intentional coverage zones:** Deploy cells around high-interference areas like metal conveyors, using directional antennas to focus RF energy and avoid unnecessary propagation.
- **Reduced overlap and controlled reuse:** Minimize cell overlap to reduce contention. Implement frequency planning to ensure adequate channel separation with spectrum reuse.
- **Predictable boundaries:** Define cells based on site surveys, ensuring edges align with physical barriers for stable handovers. IETF DetNet use cases highlight this for industrial automation, where predictable RF boundaries support deterministic networking.

2.3 Practical Techniques for Constrained RF

To achieve predictable boundaries and reduced interference required in glass plants, several practical RF techniques shift focus from blanket coverage and adaptive automation to intentional constraint. These include using the lowest effective power, focused antenna patterns, and fixed configurations to limit unwanted propagation and ensure deterministic performance.

- Directional and Dual-polarized Antennas: Deploy patch, panel, or sector antennas focus coverage along specific paths, rather than omnidirectional patterns that scatter energy. This creates predictable boundaries, reduces unnecessary propagation, and combats fading, by limiting reflected paths. To combat multipath fading through polarization diversity and enable MIMO spatial multiplexing, use dual-polarized antennas (Vertical/Horizontal or Slant-45°).
- Deliberate low-power operation: Set transmit power to the minimum required for reliable links as determined by ongoing monitoring and site surveys. Lower power reduces cell overlap, limits reflections, and minimizes self-interference, yielding better reliability than high-power approaches that amplify multipath.
- Fixed channel: Assign static, non-overlapping channels based on spectrum analysis to ensure deterministic behavior, avoiding variability of automatic adaptation in EMI-prone plants.
- Remote Radio Head (RRH) or 'Split-RAN' architecture: Baseband units in climate-controlled electrical rooms connect via fiber to RRHs in protected enclosures near coverage zones, with short RF cable runs to passive antennas in furnace areas. This minimizes heat exposure to sensitive radio components while maintaining signal quality.

Key point: Constrained design outperforms adaptive optimization by providing reliability over throughput; essential where unplanned overlaps could destabilize communications.

2.4 Spectrum Discipline and Traffic Control

Spectrum management and prioritization provide the tools to handle finite resources and unequal traffic, drawing from IETF's focus on deterministic wireless for manufacturing (e.g., DetNet and RAW).

In glass plants, where EMI and multipath amplify contention, spectrum discipline ensures bounded latency for critical flows. Tools like spectrum analyzers map propagation environments, enhancing visibility and reducing variability.

Fixed Channel Plans Where Possible

Avoid dynamic selection in favor of static assignments, especially in unlicensed bands prone to EMI.

- **Static Assignment**: Auto-channel algorithms introduce timing variability from channel changes. Static plans provide predictability, as per IETF RAW's emphasis on reliable paths. Assign non-overlapping channels (e.g., 5 GHz UNII-1/3).
- **Tools for Mapping**: Spectrum analyzers can establish noise floors and EMI patterns during production, identifying clean channels. NIST-recommended monitoring baselines occupancy, reducing interference by selecting optimal ISM bands.

Traffic Prioritization Aligned with Operational Impact

Classify packets at the radio level giving precedence to critical data such as safety telemetry.

- **IETF Deterministic Networking (DetNet):** DetNet applies deterministic resource reservation and per-hop forwarding to protect critical flows from best-effort traffic. DetNet supports low latency control traffic while preventing non-critical applications from impacting critical functions such as controls and telemetry.
- **Enhanced Distributed Channel Access (EDCA):** Provides statistical traffic prioritization in Wi-Fi by replacing uniform contention with differentiated access classes. Higher-priority traffic receives shorter backoff times and more frequent transmission than lower-priority traffic.

2.5 Continuous Measurement as a System Component

Embed monitoring as an integral element, to validate assumptions and detect challenges early. This is critical in evolving glass plants where environmental changes promote instability. Detailed metrics and monitoring frameworks are provided in Section 6.1.

- Wireless performance must be observable: Integrate metrics like SNR, packet loss, and jitter into dashboards for real-time visibility, as well as long term reporting.
- Degradation must be detected early: Employ anomaly detection and periodic RF surveys to identify issues e.g. antenna misalignment from vibrations.
- NIST SP 800-137 outlines continuous monitoring strategies for security and performance in dynamic systems. The industrial wireless guide further emphasizes ongoing assessments for safety-critical applications.

Key point: Measurement enables proactive adjustments, ensuring graceful degradation and aligning with IETF RAW's requirements for reliable services amidst industrial noise.

2.6 Security and Identity as Design Requirements

Security preserves availability and safety and must be designed in from the beginning.

Zero-Trust Identity for All Devices

Glass plants may deploy hundreds of wireless devices, from AGVs and sensors to operator tablets and maintenance tools, each representing a potential entry point.

Design Requirement: Implement zero-trust identity where every device and user must prove identity before network access, regardless of location.

Implementation:

- **For private 5G:** Use SIM or eSIM-based mutual authentication per 3GPP standards. Each device authenticates to the network and vice versa using cryptographic credentials stored in tamper-resistant modules.

- **For Wi-Fi 6/6E:** Deploy WPA3-Enterprise with IEEE 802.1X, using certificate-based authentication tied to Public Key Infrastructure (PKI). This provides per-device identity and prevents credential sharing.
- **Pre-Shared Keys (PSK):** Avoid when possible. PSKs can be single points of compromise and prevent device-level accountability

Individual device identity with non-repudiable logging is essential.

Segmentation as Security Boundary

Section 2.1 established segmentation for performance isolation. Security reinforces this requirement: network segments also function as trust boundaries. Physical or virtual isolation between network segments must prevent lateral movement from potentially compromised devices.

Practical Implementation:

- Network isolation: Separate networks for controls, sensor telemetry, safety systems, and staff access, with firewall enforcement at boundaries.
- 5G network slicing: Dedicated virtual networks with separate authentication, encryption keys, and QoS policies for each use case.
- Segregated management: Wireless management planes should never share infrastructure with production traffic.

Security-Performance Synergy: A compromised staff tablet on the best-effort Wi-Fi segment cannot inject packets into the deterministic 5G slice carrying critical traffic. This serves both security (containment) and performance (prevents best-effort traffic from degrading critical flows).

Encryption Requirements

Where possible implement link-layer (wireless protocol) and application-layer (end-to-end) encryption.

Rationale:

- Link-layer encryption (WPA3, 5G NR encryption) protects against RF eavesdropping and prevents unauthorized devices from joining the network.
- Application-layer encryption (TLS, DTLS, IPsec) protects data even if wireless infrastructure is compromised, providing end-to-end confidentiality.

Glass Plant Consideration: Reflective surfaces can extend signal propagation beyond plant boundaries in unexpected directions. Encryption ensures intercepted signals remain protected. Encryption ensures that if signals are intercepted, data remains protected.

Management Plane Isolation

Wireless infrastructure including access points and base stations are high-value targets. Isolation prevents production incidents from escalating into security incidents and vice versa.

Design Requirement: Management interfaces must be isolated from production networks and protected, ideally with multi-factor authentication.

Practical Implementation:

- Dedicated out-of-band management network or strictly controlled management network.
- Role-based access control (RBAC) with least-privilege principles.
- Multi-factor authentication for all administrative access.
- Centralized logging of all configuration changes with tamper-resistant storage.

Monitoring for Security and Performance

Principle 10 states "If It Isn't Measured, It Isn't True." This applies equally to security.

Design Requirement: Continuous monitoring must correlate RF performance metrics with security indicators.

Practical Implementation:

- Unified dashboards: Monitor SNR, packet loss, jitter, authentication failures, unusual traffic patterns, and spectrum anomalies.
- Behavioral baselines: Establish normal RF behavior (noise floor, device counts, traffic volumes) to detect deviations that may indicate jamming, rogue devices, or misconfiguration.
- Anomaly detection: Identify patterns such as repeated authentication failures, unexpected spectrum occupancy, or correlation between EMI spikes and packet corruption.

Distinguishing Threats from Environment: In glass plants, legitimate EMI from furnaces can mask intentional jamming. Continuous monitoring allows operators to differentiate:

- Expected EMI: Correlates with production schedules, specific equipment operation.
- Anomalous interference: Appears outside normal patterns, lacks correlation with production activity, may indicate malicious RF attack.

Key Point: Security monitoring is not separate from performance monitoring.

Key Concept: Determinism in Glass Plant Wireless Designs

Determinism in wireless networking refers to the ability to guarantee predictable, bounded performance metrics - such as latency, jitter, and packet loss - essential for time-sensitive industrial applications.

Deterministic systems prioritize predictable behavior over optimization. Deterministic systems support continuous monitoring and bounded adjustments within design parameters. However, uncontrolled adaptive algorithms (e.g., automatic channel switching, dynamic power control without bounds) introduce unpredictable variability incompatible with industrial determinism.

In glass manufacturing plants, where processes like furnace control, AGV navigation, and real-time quality monitoring involve precise timing, safety hazards, or downtime, determinism ensures that control loops operate without unpredictable delays.

Unlike best-effort networks (e.g., standard Wi-Fi), deterministic systems prioritize controlled behaviors over adaptive optimizations, aligning with First Principle 7. This is particularly critical in environments characterized by high thermal gradients, reflective surfaces, and electromagnetic interference (EMI).

Performance figures cited represent design targets from NIST factory benchmarks and IETF DetNet standards. Actual performance depends on site-specific conditions and must be verified through IEEE 3388-2025 testing protocols.

Implications for Glass Manufacturing

Determinism transforms wireless from a convenience to a core enabler for Industry 4.0. For instance:

- **High-Mobility Scenarios**: AGVs transporting fragile glass sheets require deterministic handovers with low jitter to avoid collisions; RAW supports this via scheduled transmissions, mitigating multipath.
- **Control and Safety Systems**: Supervisory control demands low latency for telemetry; in harsh EMI, utilize topologies that provide determinism by reducing hopping variability.
- **Measurement Integration**: Continuous monitoring detects deviations from deterministic bounds early, using tools like spectrum analyzers to validate against thermal-induced changes.

Key point: Deriving designs from determinism, segmentation, constrained RF, and traffic control, can help achieve resilient, predictable networks, reducing downtime and enhancing safety.

3. Architectural Implications

Architecture must prioritize physics-driven decisions over technology preferences. This leads to hybrid, segmented frameworks ensuring determinism for critical operations. Emphasize hybrid integration for interoperability in manufacturing, aligning with NIST and IETF guidelines for matching technologies to industrial use cases.

3.1 The Right Tool for the Right Job

Given the diverse constraints in glass plants, ranging from multipath fading to mobility demands, relying on one technology invites instability. Architectures must integrate multiple technologies to leverage their combined strengths.

- **Different access technologies solve different constraints:**
    - Wi-Fi 6/6E excels in high-throughput, human-centric applications but struggles with determinism in EMI-heavy zones.
    - Private 5G/URLLC provides low-latency reliability for automation but at higher costs.
    - LoRaWAN suits low-power sensor telemetry in remote areas.
    - IEEE 802.15.4-based protocols like WirelessHART handle process control in harsh thermal environments.
    - Bluetooth Low Energy (BLE) provides short range, low power consumption, and a simple deployment model.

- **Hybrid approaches emerge from first principles:** Combining technologies (e.g., 5G for core mobility, Wi-Fi for edge access, and wired TSN backhaul) provides resilient connectivity.

Accordingly, IETF's RAW framework provides support by defining hybrid paths for reliable wireless in factories, ensuring bounded performance. For example:

Technology	Range	Target Latency	Target Throughput	Use Case
5G URLLC	100-200m	<10ms	10-100 Mbps	AGV control, mobile robotics
Wi-Fi	30-50m	10-30ms	100-1000 Mbps	Staff devices, AR tools, video inspection
WirelessHART	10-100m (mesh)	10-100ms	<250 kbps	Process sensors, fixed telemetry
LoRaWAN	500m+	1-5s	<50 kbps	Remote sensors, tank levels
BLE	10-30m	10-50ms	1-2 Mbps	Asset tracking, beacons
UWB	10-50m	<1ms	5-10 Mbps	Precision RTLS, positioning

3.2 Matching Wireless Characteristics to Use Cases

Architecture must map technologies to specific use cases, prioritizing reliability over throughput and treating mobility as a distinct challenge. This physics-first matching ensures determinism in non-

stationary environments, as outlined in NIST's factory workcell requirements and IETF DetNet use cases for industrial wireless.

- **Human interaction:** For staff devices like tablets and handhelds, prioritize user-friendly, high-bandwidth technology like Wi-Fi 6E with broad client support. OFDMA enables efficient multi-user access.
- **High-mobility automation:** AGVs, cranes, and robotic arms demand low-jitter, seamless roaming, best served by private 5G with network slicing and path diversity. For lower-bandwidth mobile sensors, mesh-based 802.15.4e TSCH provides reliability. Thermal gradients and moving blockers necessitate redundant routing, as per IETF RAW.

Use Case Selection:

1. Is the application critical (emergency stop, hazard alarm)?
   → Use hardwired per IEC 61511.
   For SIL (Safety Integrity Level) 1/2 or high-availability (not safety-rated)
   → Consider dual-redundant 5G URLLC.

2. Is the application highly mobile (AGV, crane, robot)?
   → Consider private 5G with network slicing

3. Is the application high-bandwidth but latency-tolerant (video, AR)?
   → Consider Wi-Fi 6E on 6 GHz

4. Is the application low-bandwidth, fixed-location telemetry?
   → Consider WirelessHART or ISA100.11a

5. Is the application asset tracking?
   → Consider BLE beacons with fixed gateway infrastructure

Key point: Architecture follows physics; empirical evidence gathered via site surveys and continuous monitoring ensures technologies address instability, fostering ecosystems that scale with demand.

4. Technologies and Architectures

These recommendations are grounded in the first principles, prioritizing determinism, reliability, and environmental resilience. We focus on hybrid solutions that integrate legacy systems with emerging tech like private 5G and TSN-over-wireless, as set forth by NIST and IETF standards. Case studies from analogous industries illustrate practical application.

4.1 Hybrid Wireless Architecture

To achieve segmentation by use case and criticality, adopt hybrid architectures combining multiple Radio Access Technologies (RATs) for optimized coverage. This counters the shared medium limitations by isolating traffic.

- **Multi-RAT integration:** Consider Wi-Fi 6/6E (IEEE 802.11ax/be) for high-throughput staff access, alongside UWB and low-power wide-area networks (LPWAN) like LoRaWAN for static sensors, and private LTE/5G for mobile endpoints. 5G's network slicing enables dedicated virtual networks for safety-critical vs. telemetry traffic, reducing reflective interference.
- **Wired-wireless convergence:** Extend IEEE 802.1 Time-Sensitive Networking (TSN) to wireless via IETF DetNet/RAW, creating deterministic paths for control loops. For example, wire high-reliability zones (e.g., furnace areas) and use wireless extensions for mobility.

The use of Multi-RAT Traffic Steering enables mobile assets to utilize an intelligent connectivity layer such as 3GPP ATSSS[1] or a Policy-Based Connection Manager. This ensures that critical packets are not dropped during a hand-off; instead, traffic is dynamically switched between the 5G and Wi-Fi 6E interfaces based on PDR and jitter metrics, rather than simple signal strength.

Example Scenario	Recommended Band	Rationale
Critical control, navigation, furnace telemetry	Private 5G (CBRS) URLLC	Deterministic latency, network slicing, reduced interference
Real-time sensor telemetry (bounded latency)	5 GHz Wi-Fi 6 with QoS or WirelessHART	Proven propagation, non-DFS channels available, established troubleshooting
AR maintenance tools, video inspection (high throughput, latency-tolerant)	6 GHz Wi-Fi 6E/7 (LPI)	Clean spectrum, high bandwidth, acceptable if brief stalls occur
Staff tablets, office/admin access	5 GHz or 6 GHz Wi-Fi 6E (LPI)	6 GHz preferred if device support and AP density allow
Outdoor campus links, yard operations	5 GHz UNII-3 or 6 GHz Standard Power with AFC	5 GHz default; 6 GHz SP requires AFC complexity

1 Note: ATSSS requires compatible client devices and 5G core network support. As of December 2025, commercial ATSSS implementations are emerging but not yet widespread. Alternative approaches include application-layer path selection or vendor-specific multi-link solutions.

4.2 RF Optimization Tools and Techniques

This section outlines key tools and techniques for precise cell planning, interference management, and performance validation. These enable adherence to first principles such as Principle 3 (multipath as default), Principle 6 (self-inflicted interference), and Principle 10 (measurement as truth) with emphasis is on site-specific modeling. These recommendations align with NIST guidelines (e.g., TN 1951 for factory propagation modeling) and IEEE 3388-2025 for repeatable RF assessment.

Planning and Simulation Tools

RF simulation software can predict coverage before deployment, avoiding over-reliance on theory and automatic optimizations.

- **Site Survey and Modeling Software**: Tools like Ekahau Pro or Cisco DNA Center generate predictive heatmaps for RSSI, SNR, and interference. Input glass-plant specifics: reflective materials, thermal gradients, and dynamic blockers (e.g., moving inventory). Simulate multipath using NIST TN 1951 data. Validate models with on-site passive scans during production to capture real EMI spikes (e.g., from induction heaters).
- **Channel Emulators**: Hardware like Keysight Propsim or Spirent SR5500 replicates glass-plant fading (e.g., Rayleigh/Rician models for severe multipath). Test scenarios: AGV mobility at 5 m/s with 25-30 dB fade margins, or EMI bursts raising noise floors by 5-10 dB.

Advanced Antenna Systems

Antennas are critical for constraining RF footprints and mitigating multipath.

- **MIMO and Beamforming**: Deploy 4x4 or 8x8 MIMO arrays with beamforming to combat fading e.g., MU-MIMO directs beams to AGVs, reducing interference domains by 50-70%. In reflective "RF Shadows," use adaptive beam steering to combat multipath fading (up to 20 dB diversity gain) and null interference sources in glass-reflective environments. Tools like Ansys HFSS simulate antenna patterns, optimizing for orthogonal polarization to exploit diversity.
- **Directional and Smart Antennas**: Prioritize patch/sector antennas for aisle-aligned coverage, limiting overlap to 10-20%. In high-mobility zones, integrate phased arrays for real-time tracking. Recommendation: Low-power settings validated with spectrum analyzers to minimize amplification from reflections.

Interference Management and Validation Tools

Ongoing tools enforce spectrum discipline (Section 2.4) and detect degradation.

- **Spectrum Analyzers**: Devices like AirMagnet Spectrum XT or Rohde & Schwarz FSW identify EMI sources (e.g., arc furnaces at 2.4/3.5 GHz). Capture max-hold traces during peak shifts to baseline noise floors (-85 to -90 dBm typical); alert on >5 dB rises.
- **Performance Analyzers**: Tools like Keysight Hawkeye monitor PDR (>99.9% for control) and latency (<20ms). For glass-specific stress: Simulate thermal effects with environmental chambers, correlating jitter increases with furnace cycles.

In summary, these tools operationalize constrained designs by emphasizing pre-deployment modeling and continuous validation. Per Principle 9, build in resilience tested under production loads.

4.3 Wi-Fi Integration

Wi-Fi 6/6E (IEEE 802.11ax) and Wi-Fi 7 (IEEE 802.11be) are suited for non-critical, high-throughput applications where bounded latency is not required. Wi-Fi excels in prioritizing bandwidth, but requires strict constraints to avoid compromising reliability in reflective, EMI-prone environments.

Wi-Fi 7's Multi-Link Operation (MLO)[2] shows significant promise for glass plants. It allows a device to send data across multiple bands (e.g., 5 GHz and 6 GHz) simultaneously. In a multipath-heavy glass environment where a signal might be "blocked" on one frequency, MLO ensures the packet still arrives via the other band, drastically reducing jitter.

Use Cases for Wi-Fi in Hybrid Deployments

- **Human-Centric Applications**: Ideal for staff tablets, AR/VR maintenance tools, supervisory HMI devices, and video feeds where brief stalls are tolerable. These leverage Wi-Fi's high data rates for bandwidth-intensive, without the overhead of deterministic protocols.
- **Best-Effort Monitoring**: Suitable for non-time-sensitive IoT sensors (e.g., environmental logging) or office/admin zones, freeing spectrum for critical 5G traffic.
- **Glass Plant Considerations**: Wi-Fi should be deployed in segmented SSIDs and VLANs isolated from production loops. Prioritize 5 GHz and 6 GHz bands in production-adjacent zones due to superior interference resistance and capacity.

Deployment Constraints

To mitigate self-inflicted interference and ensure coexistence in hybrid setups:

Channel Selection and Spectrum Discipline:

To achieve the deterministic performance required by Principle 7 (Determinism Requires Control), channel selection must prioritize stability over maximum peak throughput.

- **5 GHz Band (Primary OT Layer):** Use 20 MHz fixed channel widths exclusively to maximize Signal-to-Noise Ratio (SNR) and minimize contention.
    - **Priority Channels (Non-DFS):** Utilize UNII-1 (36–48), UNII-3 (149–161) for critical zones. Avoid the use of UNII-2/2e channels (52–144) in the high EMI areas. EMI can trigger "False DFS" detections, leading to 60-second channel outages that violate safety-critical latency bounds.
- **2.4 GHz Band (Legacy/Secondary):** Deprecate for all mission-critical telemetry. While 2.4 GHz offers superior propagation, it is susceptible to broadband EMI and interference from industrial devices. If required, use a strict Channels 1, 6, 11 plan with 10 MHz-20 MHz widths.

2 As of December 2025, MLO-capable industrial clients are limited. This technology is contemplated for future deployments as client ecosystems mature.

- **6 GHz Band (High-Bandwidth Offload):** Reserved for low-criticality, high-throughput applications (e.g., video). Refer to Appendix G for channel planning and AFC considerations.
- **Static Frequency:** Implement a 4-channel or 7-channel use pattern based on physical site surveys to ensure a 20 dB separation between APs on the same frequency, particularly in reflective zones.

Power and Coverage Management:

- Intentional low-power operation, typically 17-20 dBm conducted power (before antenna gain) with directional antennas to constrain cells and minimize reflections from glass or conveyors.
- Target cell-edge RSSI of -70 to -75 dBm; validate with spectrum analyzers to prevent over-coverage that amplifies multipath fades.
- Calculate Effective Isotropic Radiated Power (EIRP) as: EIRP (dBm) = Transmit Power (dBm) + Antenna Gain (dBi) - Cable Loss (dB).

Bandwidth and QoS:

- Limit to 20-40 MHz channels in dense zones for improved reliability; wider channels increase peak throughput but reduce resilience to interference and multipath.
- Use 802.11e Enhanced Distributed Channel Access (EDCA) QoS to prioritize human interfaces over background traffic.
- In 6 GHz deployments, wider channels (80-160 MHz) can boost throughput, but require careful placement and power management due to propagation characteristics detailed below.

Deployment Recommendations for Glass Plants:

- **Conservative power settings**: Operate at 17-23 dBm conducted transmit power (well below the 30 dBm EIRP regulatory maximum) to constrain cell sizes, minimize reflections, and limit self-interference. Example configuration: 20 dBm transmit power + 6 dBi directional antenna - 2 dB cable loss = 24 dBm EIRP.
- **Directional or sector antennas**: Use patch, panel, or sector antennas (60-90° beamwidth) rather than omnidirectional patterns to focus coverage along aisles or work zones, reducing unwanted propagation into reflective glass storage areas.
- **Selective deployment zones**: Consider 6 GHz for high-throughput, latency-tolerant applications in moderate-temperature zones. Use caution if deploying 6 GHz as in furnace-adjacent hot zones or areas where propagation penalties are highest.
- **Hybrid band strategy**: Deploy dual-band (5 GHz + 6 GHz) or tri-band (2.4 GHz + 5 GHz + 6 GHz) APs to provide client devices with band-steering options. Critical telemetry and control traffic remains on dedicated 5G URLLC or 5 GHz Wi-Fi segments, while 6 GHz handles high-bandwidth best-effort applications.
- **Validate under production loads**: Conduct IEEE 3388-2025 metric stress testing during production to measure actual packet delivery ratios, latency distributions, and roaming stability.

4.4 Deterministic Protocols

To implement spectrum discipline, select protocols that prioritize traffic and ensure bounded performance, essential for unequal packet needs in glass production.

- **Time-slotted protocols:** Adopt IEEE 802.15.4e TSCH or 5G URLLC for scheduled access, minimizing contention in shared bands. IETF RAW extends this for wireless determinism, supporting low jitter for AGV control amid moving reflectors. WirelessHART and ISA100.11a are the primary application-layer frameworks that operationalize TSCH. Ultra-Wideband (UWB) is a short-range wireless technology used for real-time location systems (RTLS) for asset and personnel tracking.
- **QoS and prioritization frameworks:** 802.11e EDCA and DetNet flow management classify traffic e.g., high priority for safety stops, medium for telemetry. In EMI-prone glass plants, this aligns operational impact with radio resources, preventing latency spikes. Deterministic protocols prioritize packets and bound performance, addressing unequal traffic needs. These ensure predictable delivery while allowing best-effort flows for non-urgent data.

Time-Slotted Protocols

Scheduled access mechanisms help eliminate random contention, providing determinism in non-stationary environments.

- **IEEE 802.15.4e TSCH (Time-Slotted Channel Hopping)**: A low-power MAC mode for industrial wireless sensor networks (IWSNs), using time slots and channel hopping to mitigate interference. Slots are synchronized for deterministic access, hopping across 16 channels to evade EMI. Centralized scheduling optimizes for high-mobility zones, reducing collisions in dense deployments.
- **WirelessHART:** A time-slotted protocol providing bounded-latency communication through IEEE 802.15.4e TSCH. Uses configurable time slots and mesh topology for redundancy. Provides backward compatibility with wired HART protocol for process automation.
- **ISA100.11a:** While also utilizing TSCH, ISA100.11a is a more flexible, multi-protocol standard that supports IPv6 and 6LoWPAN. This makes it suited for plant-wide backbone architectures where multiple types of industrial traffic need to coexist on the same wireless infrastructure.
- **5G URLLC (Ultra-Reliable Low-Latency Communications)**: Delivers low latency and high reliability for real-time control, using network slicing to isolate flows. URLLC enables split-second decisions (e.g., collision avoidance) with flexible reconfiguration of production lines. In EMI-prone glass settings, it provides redundant paths and flexible slot configurations (down to mini-slots of ~0.14ms), enabling low bounded jitter.
- **IETF RAW (Reliable and Available Wireless)**: Extends determinism over wireless links, building on DetNet for adaptive reliability, ensuring failover and maintaining end-to-end guarantees. RAW optimizes paths using OAM (Operations, Administration, Maintenance) and PSE (Path Selection Engine) supporting low jitter for AGV control amid moving reflectors.

QoS and Prioritization Frameworks

As set forth in section 2.4, QoS frameworks help classify and manage traffic flows to align radio resources with operational impact, preventing latency spikes in unequal workloads.

- **IETF DetNet:** Provides bounded latency/jitter over IP networks via flow isolation and resource reservation. DetNet classifies traffic (e.g., high priority for emergency stops, medium for telemetry) using PREOF (Packet Replication, Elimination, Ordering Functions) for redundancy. In glass plants, it mitigates multipath, achieving high reliability for critical traffic.
- **802.11e EDCA (Enhanced Distributed Channel Access)**: Wi-Fi QoS mechanism with four access categories (AC): voice (highest priority), video, best-effort, background. EDCA adjusts contention windows and backoff timers to favor critical packets e.g., shorter waits for safety stops vs. telemetry. In EMI-prone zones, prioritize control traffic to reduce retry rates, ensuring <100ms latency for human interfaces amid interference.

4.5 Security Architecture and Implementation

Authentication Mechanisms by Technology

Wireless technologies provide various authentication capabilities to align with security requirements.

Technology	Authentication Method	Strength	Glass Plant Use Case
Private 5G	SIM/eSIM-based mutual authentication (3GPP)	Highest - Hardware-backed, mutual authentication	AGVs, mobile robotics, safety systems
Wi-Fi 6/6E	WPA3-Enterprise + 802.1X (EAP-TLS)	High - Certificate-based, per-device identity	Staff devices, maintenance tools, supervisory systems
Wi-Fi (Legacy)	WPA3-Personal (SAE)	Medium - Improved over WPA2 but still shared secret	Guest/visitor access only (isolated segment)
LoRaWAN	Device-specific keys + join procedures	Medium - Suitable for low-rate sensors	Remote sensor telemetry (non-critical)

Wi-Fi Security Requirements

Mandatory Security Controls:

1. **WPA3-Enterprise** with certificate-based authentication (EAP-TLS)
    - Ties identity to device, not shared password
    - Enables per-device revocation
    - Supports non-repudiable logging
2. **Protected Management Frames (PMF / 802.11w)**
    - Prevents deauthentication/disassociation attacks
    - Required for WPA3, should be enabled for WPA2 where still deployed
    - Protects against RF-based denial-of-service
3. **Management VLAN Isolation**
    - AP management interfaces on dedicated VLAN

    - No routing to production networks
    - Multi-factor authentication for controller access
4. **Rogue AP Detection**
    - Continuous scanning for unauthorized access points
    - Automated alerting and optional containment
    - Critical in reflective environments where signal leakage is amplified

6 GHz Security Considerations:

- Cleaner spectrum reduces interference but also reduces unintentional signal attenuation
- Shorter range results in reduced eavesdropping distance, though reflections can still extend propagation unpredictably.
- Requires full encryption as a design requirement

Private 5G Security Architecture

While private 5G provides certain boundaries, proper implementation is critical.

Core Security Features:

- **SIM-based authentication:** Cryptographic device identity stored in tamper-resistant modules
- **Mutual authentication:** Network authenticates to device, device authenticates to network
- **Per-user encryption keys:** Unique keys derived per device per session
- **Network slicing isolation:** Separate virtual networks with independent security domains

Implementation Requirements:

1. **Secure boot and firmware signing** on all 5G radios and user equipment
2. **Core network hardening:**
    - User Plane Function (UPF) and Control Plane Function separated
    - Zero-trust policies between network functions
    - Regular security patching and vulnerability management
3. **SIM lifecycle management:**
    - Secure provisioning and distribution
    - Remote SIM locking for lost/stolen devices
    - Certificate expiration monitoring and rotation

CBRS-Specific Security:

- SAS connectivity uses TLS with certificate validation
- SAS spoofing (validate SAS FQDN and certificates)

IT/OT Boundary Controls

Wireless architectures can create new pathways between IT and OT domains so explicit boundary controls are required.

Architecture Requirements:

- **Demilitarized Zone (DMZ):** Data historians, HMI, etc in DMZ, not directly on OT network
- **Unidirectional gateways:** For truly critical systems (furnace control, safety PLCs), consider data diodes that allow monitoring data out but no commands in
- **Protocol inspection:** Deep packet inspection at IT/OT boundary to validate industrial protocol traffic and block malicious payloads

Wireless-Specific Controls:

- Staff devices (IT domain) never directly access OT wireless segments
- Separate SSIDs/APNs for IT vs. OT traffic
- Remote access to wireless management requires VPN + MFA, with session recording

Thermal Environment and Cryptographic Hardware

Particular to high-heat industrial environments: sustained temperatures can affect security hardware.

Design Considerations:

- **Hardware Security Modules (HSM)** and Trusted Platform Modules (TPM) have temperature ratings, verify devices are rated for ambient temperatures in deployment zones
- **Cryptographic performance degradation:** High temperatures may slow cryptographic operations or increase error rates
- **Hardware Random Number Generators (RNG):** Heat can affect entropy sources; monitor for RNG health

Mitigation:

- Deploy wireless infrastructure with active cooling in high-heat zones
- Remote Radio Heads (split-RAN) in climate-controlled electrical rooms
- Regular cryptographic validation testing as part of continuous monitoring
- Environmental sensors co-located with critical security hardware

Incident Response and Recovery

Assume breaches will occur; design for detection, containment, and recovery. Incident response playbooks should include:

1. **RF Jamming Detected:**
    - Distinguish from EMI using correlation with production schedules
    - Activate backup communication paths
    - Physical security team investigates for rogue transmitters
    - Notify regulatory authorities
2. **Rogue Device/AP Detected:**
    - Automated containment
    - Forensic capture of device characteristics
    - Review authentication logs for compromise indicators

    - Physical investigation and removal
3. **Authentication Storm / Mass Failures:**
    - May indicate credential compromise or certificate expiration
    - Isolate affected segment, validate certificate infrastructure
    - Review for correlation with recent configuration changes
4. **CBRS Spectrum Preemption (DPA Event):**
    - Treated as availability incident
    - Automatic failover to backup spectrum
    - Validate safety systems remain operational
    - Log event for compliance and analysis

Recovery Validation:

- Secure backup of all configurations, certificates, and cryptographic material
- Regular restoration testing in lab environment
- Validation that restored systems meet security baselines (encryption enabled, certificates valid, isolation enforced)

4.6 Case Studies

Case Study: Celanese Chemical Plant Private 5G

Celanese, in collaboration with NTT DATA, deployed a CBRS-based private network at its Texas chemical facility in 2025, focusing on process automation in EMI-heavy environments.

Key details:

- Supports real-time sensor telemetry, robotic process control, and safety systems amid welding/arc sources (analogous to glass furnace heaters).
- Achieved reliable packet delivery for critical telemetry using URLLC slicing and TSN extensions.
- Benefits: Reduced latency spikes from EMI, prevented safety delays, and enabled predictive maintenance without production interruptions.
- Analogy to glass plants: Mitigates electromagnetic noise from heavy equipment, similar to arc furnaces and induction heaters, while maintaining reliability for small-packet control traffic.

Case Study: John Deere Private 5G Deployment

John Deere emerged as a leader in private 5G for large-scale manufacturing, with extensive deployments across U.S. facilities (e.g., Davenport Works in Iowa-named 2025 Assembly Plant of the Year-and Waterloo Works). Using CBRS spectrum and Nokia radios, the company operates its own private networks to support high-density connectivity in metal-heavy factories.

Key details:

- Over 100 AGVs rely on private 5G for seamless transport of engines, drive trains, and parts, enabling low latency and smooth handovers-critical for mobility in interference-prone environments.
- Supports industrial robotics (e.g., over 55 robotic arms in paint shops), smart torque tools, real-time quality control, asset tracking, and digital twins.
- "80-10-10" model: Targeting 80% private 5G coverage, 10% Wi-Fi, 10% wired Ethernet.
- Benefits: Handles up to 800 devices per radio (vs. ~50 on Wi-Fi), reduces manual intervention, improves safety, and scales for 20x device growth, reconfigure assembly lines in hours vs. days.
- Analogy to glass plants: Large metal machinery creates multipath and EMI similar to reflective glass sheets/conveyors; private 5G provides deterministic performance for AGVs amid dynamic blockers.

This deployment (ongoing since ~2020, scaled significantly in 2024-2025) counters self-inflicted interference and mobility challenges, aligning with constrained RF design and hybrid architectures.

Case Study: Airbus/Ericsson Private 5G Deployment

The Airbus/Ericsson private 5G deployment (announced October 2025) is an excellent analogy for glass manufacturing due to the reflective metal environments in aerospace assembly; aircraft fuselages, wings, and components cause issues similar to glass sheets and metal conveyors.

Key details:

- Fully operational private 5G Standalone (SA) network at Airbus' Hamburg (Germany) production site.
- Deployment underway in Toulouse (France), expected completion by 2026.
- Powered by Ericsson Private 5G (modular, API-driven, with automated infrastructure for rapid rollout).
- Use cases: IoT integration, real-time quality control, collaborative robotics, augmented reality, 3D simulation, predictive maintenance, asset traceability, and mobility for operators/equipment.
- Benefits: Seamless full-site coverage, reliable low-latency connectivity from workstation to aircraft cabin, enhanced security, and scalability for Industry 4.0.
- Broader road map: Expansion to sites in Spain, UK, US, and Canada.

This deployment demonstrates how private 5G overcomes reflective/multipath challenges in large-scale metal-heavy factories, providing deterministic performance for AGVs, robotics, and control systems-directly transferable to glass plants handling fragile sheets amid conveyors and thermal zones.

Case Study: Celona Private 5G Deployment

A Celona private 5G deployment at a major U.S. steel manufacturer is a strong analogy for glass manufacturing due to the highly reflective metal environments and heavy EMI from machinery, furnaces, and conveyors create multipath and interference challenges comparable to glass sheets, metal rollers, and arc furnaces.

Key details:

- Deployed Celona 5G LAN on CBRS spectrum, with network slicing for prioritized traffic across indoor/outdoor transitional areas.
- Focused on automated material handling, AGVs, and telemetry in interference-prone zones (e.g., scrap yards with poor legacy Wi-Fi coverage).
- Use cases: Real-time logistics, production monitoring, asset tracking, and connectivity for mobile equipment/operators.
- Benefits: Reduced unplanned downtime from frequent interruptions to near-zero in the reported deployment context, streamlined operations, lowered maintenance costs, and improved productivity without halting production.
- Analogy to glass plants: Reflective metal surfaces and EMI from heavy equipment mirror glass sheet reflections and furnace noise; private 5G provides seamless coverage and bounded latency for AGVs amid dynamic blockers and thermal zones.

5. Implementation Guidelines

> *"Improve constantly and forever the system of production and service, to improve quality and productivity, and thus constantly decrease costs."* - W. Edwards Deming

This section outlines a phased, risk-mitigated approach to deploying wireless systems, grounded in first principles such as measurement over assumption, graceful degradation, and controlled determinism.

By prioritizing incremental adoption and empirical validation, deployments can evolve from pilot use cases to full-scale integration, minimizing disruptions in glass plants' dynamic, EMI-heavy environments. This aligns with NIST guidelines for industrial wireless testbeds and IEEE 3388-2025 for performance assessment under aggressors like multipath and thermal variations.

Graceful degradation in glass plant wireless systems means that, under fault conditions (e.g., EMI spikes, spectrum preemption, mobility failures), the system:

- Preserves safety-critical communications
- Maintains bounded failure modes (detectable, logged, recoverable)
- Degrades non-critical services first

5.1 Incremental Deployment Over Big-Bang Rollouts

Avoid large-scale overhauls; instead, phase in deployments to build confidence and gather empirical data. Start with bounded, high-value use cases, isolated applications where reliability gains justify investment, emphasizing early wins without overextending resources.

- **Pilot Selection**: Focus on areas with low-risk, high ROI. Begin with non-disruptive zones, using hybrid architectures to test. This mitigates risks from multipath or EMI, allowing data collection before expansion.
- **Phased Rollout**: Increment by zone, validating each phase with site surveys and continuous monitoring. Scale based on metrics like jitter, incorporating feedback to refine constrained RF.
- **Risk Mitigation**: Redundant paths during transitions; monitoring for graceful degradation.

5.2 Design for Evolution, Not Final State

Design systems for adaptability, not static final states. Industrial wireless architectures should support incremental adoption and modular integration of emerging technologies. Standards like IETF RAW guide upgrades to deterministic networks, ensuring new systems do not compromise reliability. Anticipate growing demand and plan for scalable, multidimensional expansion.

- **Modular Architecture**: Build with open standards (e.g., IEEE 1451 for sensor interoperability) to integrate future tech like 6G or enhanced URLLC without full redesigns. RAW's OAM functions enable seamless upgrades, maintaining bounded latency amid evolving EMI patterns.

- **Scalability Planning**: Forecast device growth (e.g., from 100 sensors to 500+); use DetNet/RAW for flow isolation, ensuring additions don't exceed airtime targets (<40% for deterministic traffic). Plan for spectrum expansion, e.g., adding 6 GHz for high-throughput AR.
- **Future-Proofing**: Incorporate APIs for over-the-air updates; design for hybrid evolution (e.g., Wi-Fi to 5G migration) with minimal downtime.

5.3 Testing, Validation, and Collaboration

Robust testing bridges design intent and real-world performance, using standards to identify aggressors.

Testing Phase	Methods and Tools	Target Metrics	Glass Plant Focus
Lab/Pilot	Channel emulators with simulations integrating real PLCs/sensors. Emulate multipath using NIST TN 1951 data for reflective environments.	Latency <10ms (TSN-over-wireless); PDR >99.99%; jitter <10ms. Target NIST benchmarks for mobile scenarios.	Simulate thermal gradients, moving blockers, and EMI bursts; validate per IETF DetNet/RAW.
Site Surveys	Spectrum analysis and surveys; use NIST TN models for pre-deployment emulation.	SNR >25 dB; retry rates <2%; interference correlation with production.	Address reflections and DPA preemption; conduct surveys during production.
Stress/ Production	Incremental rollout with continuous monitoring (SNR, retry rates); hardware-in-the-loop for failover tests.	Recovery <100ms; throughput under load matching IEEE 3388 aggressors.	Test under production (e.g., furnace EMI); detect degradation early.
Collaboration	Engage vendors for knowledge transfer and domain expertise; maintain open-standard independence. (e.g., IEEE 3388-2025)	Protocol-agnostic evaluation; benchmarks like <5ms TSN latency	Multi-vendor pilots ensure resilience; align with standards.

No wireless system can eliminate failure entirely, particularly in harsh industrial environments where RF conditions, physical layouts, and operational demands evolve. The objective of implementation is bounded and predictable behavior: failures that are detectable, recoverable, and operationally safe. Achieving this requires continuous measurement and validation as part of normal operations.

Similarly, no deployment plan survives first contact with a manufacturing plant unchanged. Thermal behavior shifts, production layouts evolve, and interference sources appear over time. Observe, constrain, validate, and adapt within bounded limits.

6. Performance Validation and Success Metrics

Success is measured by how reliably the network supports production in harsh, reflective, and dynamic environments. As emphasized in IEEE 3388-2025, key metrics must account for real-world aggressors like multipath fading, EMI and mobility-induced variability. These align with NIST guidelines and IETF RAW/DetNet requirements for bounded latency and high packet delivery.

6.1 Metrics That Matter

Prioritize metrics that directly reflect reliability and determinism over raw throughput, as high bandwidth can mask underlying issues in glass plants. IEEE 3388-2025 defines standardized evaluation of these under simulated aggressors (e.g., multipath fading, EMI bursts, thermal refraction), ensuring repeatable, comparable results across deployments. Focus on end-to-end indicators that validate bounded latency for control loops amid reflections and EMI.

Performance Metrics

Metric	Description	Target (Glass Plant)	Warning/ Critical Thresholds	Action
Packet Delivery Ratio (PDR)	Percentage of packets successfully delivered	>99.99% for control; >99% for telemetry	Warning: <99.9%; Critical: <99%	Correlate with EMI spikes; investigate multipath if uncorrelated to production
First-Attempt Packet Success Rate (PSR)	Ratio of packets succeeding on first transmission (no retries)	>95% for safety-critical	Warning: <90%; Critical: <80%	Check for self-interference; adjust power if over-coverage suspected
Latency Consistency (Standard Deviation of Delay)	Variability in end-to-end latency	<5ms for control; <20ms for monitoring	Warning: >10ms; Critical: >50ms	Analyze for thermal gradients; optimize scheduling if jitter correlates with mobility
Latency Variance (Jitter)	Peak-to-peak delay variation	<10ms for AGVs; <50ms for sensors	Warning: >20ms; Critical: >100ms	Validate under peak load; implement DetNet if exceeds bounds
Recovery Behavior Under Failure (Time to State Restoration)	Duration to restore normal operation post-disruption (e.g., EMI burst)	<100ms for critical; <1s for others	Warning: >500ms; Critical: >2s	Test failover; log for trend analysis

Authentication and Access Control Metrics

Metric	Description	Target	Warning/Critical Thresholds	Action
Failed Authentication Attempts	Count by device/zone/time	<5/day per device	Warning: >10/day; Critical: >50/day	Investigate spikes; correlate with RF anomalies for jamming attacks
Certificate Expiration Tracking	Rotation rates and expires	100% rotated on schedule	Warning: <90% compliance; Critical: Any expired	Automate alerts; tie to resilience planning
Unauthorized Device Detection Events	New/rogue devices attempting access	0	Warning: 1-5/week; Critical: >5/week	Quarantine and scan; map to geographic heat maps
MFA Bypass Attempts or Failures	Bypasses or failed multi-factor authentication	0	Any event critical	Incident response; review logs for insider and external threats

Network Behavior Metrics

Metric	Description	Target	Warning/Critical Thresholds	Action
Unexpected Traffic Patterns	Deviations in volume/timing/destination	Matches baseline	Warning: ±20% deviation; Critical: ±50%	Correlate with production schedules; investigate if uncorrelated
Frame Retry Rates	MAC-layer retransmissions	<2%	Warning: 2-5%; Critical: >5%	Check for over-coverage; adjust antennas if multipath suspected
Rogue AP Detection Events	Unauthorized access points	0	Any event critical	Isolate and remove; scan spectrum for sources
MAC Address Spoofing Indicators	Duplicated or anomalous MAC addresses	0	Any event critical	Enforce 802.1X; log for forensic analysis
Protocol Anomalies	Malformed packets/unusual flags	0	Warning: 1-10/day; Critical: >10/day	Block sources; correlate with PDR drops for EMI vs. attack

RF Security Indicators

Metric	Description	Target	Warning/Critical Thresholds	Action
Spectrum Occupancy Outside Normal Patterns	Unusual band usage	Matches baseline	Warning: ±10% deviation; Critical: ±20%	Scan for jamming; compare to baseline EMI

Metric	Description	Target	Warning/Critical Thresholds	Action
Interference Detected Outside Production Correlation	Non-correlated noise spikes	0	Any event critical	Investigate external sources; alert if persistent
Signal Strength from Unexpected Directions/Locations	Anomalous RSSI patterns	Matches design	Warning: > -60 dBm unexpected; Critical: > -50 dBm	Map to heat maps; check for rogue devices
Channel Switching Events	Distinguish DFS vs. attacks	Legitimate DFS	Any unexplained critical	Log and analyze; tie to CBRS preemption

Availability and Resilience Metrics

Metric	Description	Target	Warning/Critical Thresholds	Action
CBRS DPA Preemption Events	Frequency and recovery times	<1/month	Warning: >2/month; Critical: >5/month	Minimize footprint, optimize failover, diversify spectrum
Failover Activation Frequency	Redundancy triggers	<5/year	Warning: >10/year; Critical: >20/year	Root-cause analysis; enhance diversity
Time to Detect and Contain Security Incidents	From alert to resolution	<5min	Warning: >15min; Critical: >30min	Drill simulations; integrate with dashboards
Recovery Time Objectives (RTO) for Security Events	Post-incident restoration	<1min for critical	Warning: >5min; Critical: >10min	Test under aggressors; refine resilience plans

Correlation Metrics

Critical: Monitor for correlations that indicate security vs. environmental issues, using unified platforms to avoid false positives in EMI-heavy settings.

- Authentication failures + unusual RF activity = potential attack (e.g., jamming to force reconnects).
- PDR drops + production schedule correlation = likely EMI (normal; monitor trends).
- PDR drops + no production correlation = investigate jamming or external interference.
- Management access + configuration change + immediate degradation = insider threat or misconfiguration.

Apply IEEE 3388-2025 aggressor models to simulate and differentiate.

Visualization and Dashboards

Dashboards must present a unified view, correlating RF, performance, and security data.

- **Single-Pane Overview**: Display RF health (noise floors, occupancy), performance (PDR/latency), and security (authorization failures, anomalies) in one interface.

- **Time-Series Correlation**: Overlay production schedules, authentication events, and RF metrics to spot patterns (e.g., EMI spikes during furnace peaks).
- **Geographic Heat Maps**: Show coverage quality and security event density by zone (e.g., rogue detections near glass storage).
- **Trend Analysis**: Distinguish gradual environmental degradation (e.g., antenna drift from heat) from acute security events.

Tools: Integrate with platforms like Cisco DNA Center or Splunk for real-time alerts, ensuring glass-specific thresholds (e.g., >5 dB noise rise triggers EMI check).

Key point: Security and performance are inseparable and continuous monitoring provides the data needed to remain performant and secure.

6.2 Aligning Wireless Performance with Production Impact

Technical metrics gain meaning when linked to operational outcomes, turning wireless data into business value. This section bridges RF performance (Section 6.1) to factory KPIs like Overall Equipment Effectiveness (OEE) and downtime costs, demonstrating how first principles designs (e.g., resilience per Principle 9) translate to tangible ROI.

By correlating PDR drops with scrap rates or jitter with cycle times, stakeholders can quantify wireless contributions to efficiency, reducing the hidden costs of instability (Section 1.3). Integrated platforms enable this alignment, justifying investments in constrained RF for Industry 4.0 initiatives.

Technical Metrics Tied to Operational Outcomes

Map wireless indicators to production KPIs, using correlations to prioritize fixes and measure improvements. For example, NIST and IEEE studies show reliable IIoT wireless can boost OEE by 10-20% through reduced downtime and real-time data.

Wireless Metric	Operational Impact	Example in Glass Production	Potential Improvement
PDR and PSR	Influences OEE (availability/quality)	Packet loss in telemetry, reducing yield and increasing scrap from misalignment. A 1% PDR drop can cut OEE by 2-5%.	Reliable wireless enables real-time monitoring, boosting OEE by 10-20% via predictive maintenance.
Jitter and Latency Consistency	Affects cycle times and throughput	Variable delays in AGV commands cause bottlenecks in sheet transport, extending lead times by 5-15% and raising defect rates.	Minimized jitter shortens cycles, improving throughput by 5-10%; e.g., sub-20ms latency for control loops.
Recovery Behavior and Failover Time	Impacts downtime and resilience	A 1-minute outage halts lines, costing $100-16,000/min in lost melt/production; correlates to safety incidents from missed alerts.	Fast recovery (<100ms) prevents halts, reducing annual downtime costs ($129M/facility average) by 20-30%.

Wireless Metric	Operational Impact	Example in Glass Production	Potential Improvement
Broader Correlations (e.g., RF Anomalies)	Ties to production volume, defects, safety	EMI-correlated PDR drops increase defects (e.g., from unadjusted forming); non-correlated signal unusual activity flags security risks affecting uptime.	Integrated logging quantifies ROI: e.g., 5% higher throughput from reduced jitter, or 15% lower scrap via reliable inspections.

Implementation Recommendations

- **Integrated Platforms**: Use tools (Section 4.5) to correlate wireless logs with PLC/SCADA data, e.g., overlay PDR trends with furnace cycles to isolate EMI vs. design flaws.
- **ROI Quantification**: Calculate benefits like OEE gains (10-20% from IIoT wireless) or downtime savings ($9K/min average across manufacturing; higher in high-volume glass lines). Track pre/post-deployment KPIs to justify costs.

Key point: Use integrated platforms (e.g., correlating wireless logs with PLC data) to quantify ROI, e.g., reduced jitter yielding 5% higher throughput or 20% lower downtime costs. This turns principles into measurable business outcomes.

7. Conclusion

Wireless reliability in glass manufacturing is not a mystery problem. The challenges include multipath reflections from glass sheets, thermal gradients distorting propagation, EMI from furnaces and heavy machinery, and the demands of mobile automation; these are all well-understood consequences of physics in a uniquely hostile environment. Standards bodies like NIST and IETF, with emerging benchmarks such as IEEE 3388-2025, have mapped these impairments and provided the tools to measure and mitigate them systematically.

By returning to first principles, recognizing wireless as a shared, finite medium shaped more by the environment than by protocol features, we can move beyond reactive fixes (more access points, higher power) to intentional designs built on segmentation, constrained RF planning, traffic discipline, and continuous empirical validation. These principles, applied consistently, transform wireless from a source of frustration into a predictable enabler of operational excellence.

When designed from first principles, scalable and reliable wireless is achievable even under extreme conditions. Glass plants, with a combination of high-heat processes, reflective surfaces, and dynamic material flows, represent one of the most demanding industrial settings. As demonstrated in analogous manufacturing deployments and validated through NIST testbeds and IETF deterministic frameworks, hybrid architectures, deterministic protocols, and measurement-driven iteration deliver bounded latency, consistent packet delivery, and graceful degradation.

Accepting that demand will continue to increase is the starting point. The proliferation of sensors, mobile robots, AR tools, and data-driven processes is inevitable in the journey toward smarter, more efficient glass manufacturing. The true risk lies in treating wireless as an afterthought, assuming consumer-grade solutions will suffice, or failing to implement wireless use cases under the assumption of futility. By embracing incremental deployment, evolutionary design, and rigorous validation from the outset, we can build networks that meet today's needs and grow confidently into tomorrow's.

In the end, optimal wireless in the glass plant is not about chasing perfect conditions-it is about engineering resilience into an imperfect medium. With disciplined application of first principles, the glass industry can lead in demonstrating that reliable, high-performance wireless is fully attainable, even where the environment fights hardest against it.

A Word on Standards and Practices

> *"No plan survives contact with the enemy."* - Helmuth von Moltke the Elder

Standards provide essential frameworks, common vocabularies, and validated methodologies. They enable interoperability, establish performance benchmarks, and codify lessons learned across industries. This document relies heavily on standards from IEEE, IETF, NIST, 3GPP, and IEC because these represent the best available foundation for industrial wireless design.

However, standards are not solutions; they are tools.

The Standards Landscape as of December 2025

Mature and Validated:

- **IEEE 802.11 (Wi-Fi)**: Decades of deployment data, extensive vendor ecosystem, well-understood performance characteristics.
- **3GPP LTE/5G specifications**: Mature radio specifications with growing private network implementations.
- **IEC 62443**: Established cybersecurity framework with proven application in industrial control systems.
- **NIST SP 800-82**: Comprehensive OT security guidance refined through multiple revisions.

Recently Published:

- **IEEE 3388-2025** (July 2025): Provides rigorous methodology for industrial wireless performance assessment. Protocol-agnostic framework is sound, but practical application requires developing sector-specific test profiles. Glass manufacturing facilities implementing this standard will be among the first to establish best practices for this methodology in reflective, high-heat environments.

Emerging:

- **IETF RAW (Reliable and Available Wireless)**: Architecture remains Internet-Draft as of December 2025, with RFC publication expected in 2025-2026. Conceptual framework is solid and grounded in DetNet principles, but commercial implementations are limited. Early adopters should verify vendor roadmaps and conduct interoperability testing.

Adapted from Adjacent Domains:

- **NIST TN 1951** provides industrial RF propagation measurements from automotive, machine shop, and steam plant facilities. This document adapts these findings to glass manufacturing by adding environment-specific factors (glass reflectivity, extreme thermal gradients, Low-E coatings). These adaptations represent informed engineering judgment, not empirical validation in glass plants.

What This Means for Glass Manufacturing

The performance figures, design parameters, and validation methodologies presented in this document represent:

- **Design targets** derived from standards and research, not guaranteed outcomes
- **Engineering principles** that must be validated through site-specific testing
- **Framework approaches** that require adaptation to each facility's unique conditions

When this document states "target latency <10ms" or "PDR >99.99%," these are specifications from IETF DetNet and NIST factory testbeds - they are what deterministic systems *should* achieve, not what all systems *will* achieve without proper design and validation.

When vendor case studies report "800 devices per base station" or "near-zero downtime," these represent outcomes in specific deployment contexts with baseline conditions that may differ substantially in practice.

The First Principles Approach to Standards

This is precisely why a first principles methodology matters. Rather than accepting standards-based designs at face value, the approach outlined in this document emphasizes:

1. **Measure, don't assume** (Principle 10): Standards provide targets; measurement provides truth. Site surveys, spectrum analysis, stress testing, and continuous monitoring validate whether standards-based designs actually deliver required performance in your specific environment.
2. **Design for failure, not perfection** (Principle 9): First principles acknowledge that multipath, EMI, thermal effects, and hardware degradation will challenge any design. Resilience comes from redundancy, diversity, and graceful degradation, not from assuming standards compliance guarantees performance.
3. **Environment dominates** (Principle 2): IEEE 802.11 specifications define Wi-Fi capabilities in controlled test environments. Your glass plant has 1,500°C furnaces, moving sheets of glass, and arc welders generating broadband EMI. Standards cannot predict how these interact. Empirical validation is non-negotiable.

Looking Forward

As IEEE 3388-2025 gains adoption, as IETF RAW transitions from draft to RFC, and as DetNet/TSN integration matures in commercial products, the industrial wireless ecosystem will strengthen. Glass manufacturing facilities implementing these approaches in 2026 will develop invaluable operational data that will, in turn, inform future standards and practices.

The first principles outlined in this document will remain valid regardless of how standards evolve. Physics - multipath propagation, thermal refraction, electromagnetic interference - does not change with publication dates. What changes is our collective understanding of how to measure, manage, and mitigate these effects systematically. Standards are the foundation, validate through measurement, design for resilience, and trust physics not promises.

Appendix A: Failure Modes and Anti-Patterns

Glass manufacturing facilities represent one of the most hostile RF environments found in industry. Extreme temperatures, reflective and refractive surfaces, moving glass inventory, dense metallic machinery, and high-energy electrical systems destabilize wireless behavior.

In this context, many widely accepted enterprise and “smart factory” wireless design practices fail – predictably. This can be addressed through first principles, remembering the dominance of the environment, multipath as the default propagation mode, self-inflicted interference, and inevitable performance degradation over time.

Each section describes the underlying cause, observable symptoms, and operational implications, drawing on measurements and findings from NIST studies in analogous industrial environments.

A.1 Multipath Fading

Aspect	Description
Cause	Reflective surfaces create multiple signal paths, leading to interference.
Symptoms	Rapid signal fluctuations (e.g., 20-30 dB fades), high packet error rates, and intermittent connectivity despite strong average RSSI.
Operational Implications	Disrupted control loops for AGVs or sensors, causing instability; e.g., a 10% packet loss can delay emergency stops by 200-500 ms.
Glass-Specific Aggravation	Glass and metal rollers amplify reflections, turning short-distance links into "RF Shadows" with non-stationary channels due to thermal refraction.
Mitigation	Incorporate MIMO diversity and frequency redundancy (e.g., 802.11ax beamforming). Use directional antennas; simulate with tools like iBwave for site-specific modeling. Cross-reference Section 2.3 for constrained RF techniques.

A.2 Electromagnetic Interference (EMI) from Equipment

Aspect	Description
Cause	Furnaces, heaters, and blowers generate broadband noise, elevating noise floor.
Symptoms	Increased bit error rates, reduced effective range, and sporadic disconnects.
Operational Implications	Unreliable telemetry from vibration sensors, leading to undetected equipment failures; in one metal plant case, EMI caused 15% downtime spikes.
Glass-Specific Aggravation	High-heat zones (1,500°C+) intensify EMI, clashing with sensitive IoT bands; moving mixers create time-varying noise profiles.
Mitigation	Isolate critical traffic via spectrum segmentation (e.g., 5G private networks in 3.5 GHz). Deploy EMI shielding on enclosures and continuous SNR monitoring per IEEE 3388-2025. Reference Section 2.4 for traffic control.

A.3 Over-Coverage and Uncontrolled Cell Overlap

Aspect	Description
Cause	Excessive access point density or high transmit power exacerbates interference.
Symptoms	Hidden node problems, co-channel contention, and reduced throughput.
Operational Implications	Systemic latency for mobility use cases like AGVs and cranes, risking collisions; amplifies contention in dense device areas.
Glass-Specific Aggravation	Reflective surfaces propagate signals farther, turning minor overlaps into plant-wide interference; e.g., a single AP can affect 2-3 zones in glass "mirrors."
Mitigation	Cell-based designs controlled overlap and power capping. RF planning tools like Ekahau facilitate site surveys.

A.4 Treating All Traffic Equally

Aspect	Description
Cause	Lack of QoS and segmentation permits contention between critical and best-effort traffic.
Symptoms	Jitter and packet drops in mixed-use networks (e.g., admin Wi-Fi delaying sensor data).
Operational Implications	Compromised critical systems, delayed signals, cascading failures.
Glass-Specific Aggravation	Multidimensional demand exacerbates contention in shared ISM bands.
Mitigation	Implement criticality-based segmentation per Section 2.1.

A.5 Adaptive Optimization in Deterministic Environments

Aspect	Description
Cause	Reliance on auto-tuning (e.g., dynamic channel selection, automatic power control) introduces timing variability.
Symptoms	Unpredictable latency spikes (e.g., 100-300 ms during channel switches), inconsistent packet delivery timing.
Operational Implications	Undermines control loops requiring bounded jitter; e.g., collision avoidance or coordinated robot motion leading to quality defects or safety incidents.
Glass-Specific Aggravation	Dynamic channels selected based on shifting patterns quickly invalidate optimizations; suboptimal adaptations create variability.
Mitigation	Use fixed, bounded parameters per IETF DetNet principles (e.g., scheduled TDMA, static channel assignments, fixed transmit power). Consider disabling automatic RF optimization features. Stress-test with IEEE 3388-2025 metrics under production loads.

A.6 Inadequate Resilience to Environmental Changes

Aspect	Description
Cause	Designs fail to account for drift from equipment additions, layout shifts, or seasonal variations.
Symptoms	Gradual performance erosion, unexplained coverage gaps.
Operational Implications	Unplanned outages affecting production scalability; "death by a thousand cuts" degradation.
Glass-Specific Aggravation	Process changes and crane movement patterns create RF Shadows; seasonal thermal cycling (summer cooling loads vs. winter heating) shifts propagation characteristics; new equipment installations invalidate original RF maps.
Mitigation	Build in redundancy through path diversity and graceful degradation per Principle 9. Implement continuous monitoring per Section 2.5 with baseline drift detection. Schedule periodic re-surveys to validate assumptions. Maintain RF documentation updated with facility changes.

A.7 Inadequate Measurement and Validation

Aspect	Description
Cause	Reliance on simulations or initial surveys without continuous verification and production-load testing.
Symptoms	Degradation (e.g., hidden interference buildup), performance that diverges from design predictions, failures that occur only under specific production conditions.
Operational Implications	False assumptions lead to systemic unreliability; e.g., EMI from a rarely-used backup furnace causes sensor failures when activated.
Glass-Specific Aggravation	Complex environments with thermal gradients, moving inventory, and variable EMI defy predictive models; surveys conducted during maintenance shutdowns miss production-time interference patterns.
Mitigation	Integrate continuous measurement as a core system component per Principle 10 and Section 2.5. Conduct stress testing during peak production shifts. Implement IEEE 3388-2025 validation protocols with glass-plant-specific test profiles. Correlate wireless metrics with production schedules to identify cause-effect relationships.

A.8 Hardware Degradation from Environmental Factors

Aspect	Description
Cause	Silica dust, humidity, thermal cycling, and vibration destabilize antennas, connectors, and enclosures.
Symptoms	Signal attenuation, intermittent faults, connector oxidation, antenna detuning.
Operational	"Flaky" connections that work intermittently, confounding troubleshooting efforts.

Aspect	Description
Implications	
Glass-Specific Aggravation	Fine silica dust penetrates IP66 enclosures through cooling vents; thermal expansion cycles (daily furnace on/off, seasonal ambient variation) stress antenna mounts causing mechanical misalignment; condensation from temperature differentials (cold outdoor air meeting hot indoor zones) corrodes electronics.
Mitigation	Deploy hardened components (IP67-rated minimum; IP68 for severe zones) with active cooling or heat exchangers rather than passive venting. Use sealed enclosures in dust-heavy zones. Implement predictive maintenance via environmental sensors co-located with wireless infrastructure. Schedule regular physical inspections of antenna mounting integrity, connector corrosion, and enclosure seal condition.

A.9 Security Vulnerabilities in Shared Spectrum

Aspect	Description
Cause	Unsecured IoT devices, rogue APs, authentication exploits.
Symptoms	Unauthorized device associations, interference-based DoS attacks, data exfiltration, spoofed telemetry.
Operational Implications	Compromised systems, intellectual property theft, compliance violations.
Glass-Specific Aggravation	High-reflectivity environment inadvertently extends signal range beyond facility perimeter, exposing networks to external attackers; truck drivers, contractors, or visitors with personal devices introduce rogue endpoints.
Mitigation	Enforce zero-trust identity models per Section 2.6. Implement network access control with device profiling and automated quarantine. Deploy wireless intrusion detection/prevention systems with continuous rogue AP scanning. Use directional antennas to minimize signal leakage outside facility boundaries. Segment guest/contractor access on isolated VLANs with no path to OT networks. Monitor for anomalies via SIEM correlation of RF metrics and authentication events.

A.10 Spectrum Revocation in Regulated Bands

Aspect	Description
Cause	Dynamic Protection Area (DPA)[3] activations in CBRS/5G prioritize federal

3 For manufacturers in the Greater Toledo area deploying private 5G on CBRS spectrum, availability is subject to federal Dynamic Protection Areas (DPAs). These zones protect Tier 1 incumbents e.g., US Government and consequently, the Spectrum Access System (SAS) is mandated to immediately suspend or reallocate certain grants of bandwidth on demand. This creates potential for external preemption so designs must integrate failover, diverse frequency strategies, and minimize antenna power and height to reduce the neighborhood interference footprint.

Aspect	Description
	incumbents (e.g., naval radar), immediately revoking spectrum grants.
Symptoms	Sudden bandwidth loss (50-100 MHz), complete connectivity blackouts in affected sectors, SAS-initiated channel evacuation.
Operational Implications	Abrupt halts, loss of telemetry during DPA events; production disruptions, potential safety incidents.
Glass-Specific Aggravation	Proximity to naval installations (e.g., Toledo area near Great Lakes) increases DPA activation potential; glass plants operate 24/7 so can disrupt continuous processes.
Mitigation	Design hybrid architectures with automatic failover. Use CBRS extended heartbeat mechanism to maintain local operations during temporary SAS connectivity loss. Minimize CBRS antenna height and EIRP to reduce interference footprint and potential coordination zone conflicts. Implement operational playbooks for DPA events with pre-defined communication paths and production hold procedures. Monitor SAS grant status in real-time with alerting to operations teams.

A.11 Mobility Handover Failures

Aspect	Description
Cause	Insufficient cell overlap, rapid environmental changes from moving inventory, protocol mismatches, or poorly tuned roaming triggers prevent seamless transitions between access points or base stations.
Symptoms	Connection drops during roaming, elevated latency spikes (100-500 ms), increased packet loss, frequent device reassociations, "sticky client" behavior.
Operational Implications	Disruptions to mobile operations resulting in temporary halts or reduced throughput; operators experience inconsistent HMI.
Glass-Specific Aggravation	Dynamic blockers can create intermittent RF Shadows and multipath pattern shifts, triggering premature or delayed handover decisions; high-reflectivity amplifies cell-edge instability; NIST SP 1500-204 data from metal-heavy factories suggests up to 30% higher handover failure rates in reflective environments compared to open warehouses.
Mitigation	Ensure 15-20% controlled cell overlap. Deploy fast-roaming protocols for network-directed roaming. For 5G, leverage 3GPP handover optimization features including measurement reporting and conditional handovers. Incorporate IETF DetNet/RAW packet replication and elimination during handover windows to maintain zero packet loss. Validate with mobility stress tests. Implement Multi-RAT traffic steering to maintain parallel paths.

A.12 Antenna Physical Degradation and Misalignment

Aspect	Description
Cause	Thermal expansion/contraction cycles, vibration from nearby equipment, improper

Aspect	Description
	mounting, or physical damage cause antenna elements to detune or mounting hardware to shift orientation.
Symptoms	Gradual coverage pattern distortion, reduced gain, shifted null points creating unexpected dead zones, polarization skew reducing MIMO effectiveness, increased VSWR (Voltage Standing Wave Ratio) indicating impedance mismatch.
Operational Implications	Coverage holes appear in previously reliable zones; devices experience intermittent connectivity issues that shift over time.
Glass-Specific Aggravation	Daily thermal cycling from furnace operation (ambient swings of 20-40°C) causes metal antenna mounts to expand/contract, loosening hardware; vibration from equipment transmits through mounting structures; airborne silica dust clogs antenna radomes, affecting pattern shape.
Mitigation	Use vibration-isolating mounts, elastomeric dampers rated for industrial environments. Install stainless steel or aluminum mounting hardware with thread-locking compound and spring washers to prevent loosening. Select antennas with sealed radomes (IP67 minimum) to prevent dust ingress. Incorporate thermal expansion joints in long antenna mounting poles. Conduct regular physical inspections including visual checks for loose hardware, corrosion, and VSWR measurements with handheld RF meters. Implement automated antenna health monitoring via return loss measurements from infrastructure radios where supported. Document antenna orientation during installation re-verify during inspections. Replace antennas showing >2 dB gain degradation or VSWR >1.5:1.

A.13 Cable and Connector Degradation

Aspect	Description
Cause	Cable breakdown from sustained high temperatures, connector corrosion from moisture/condensation, mechanical stress on cables routed through moving equipment zones, improper cable bending radius, UV degradation on outdoor runs.
Symptoms	Increasing insertion loss, intermittent connectivity correlating with temperature or humidity changes, RF arcing at connectors creating broadband noise, complete signal loss from internal conductor fracture.
Operational Implications	Degraded link budgets forcing lower modulation rates and reduced throughput; intermittent failures that pass initial deployment testing but fail months later; connector arcing introduces EMI affecting adjacent systems; complete outages requiring emergency replacements during production.
Glass-Specific Aggravation	Cables routed near furnaces or heated zones experience accelerated dielectric breakdown; temperature cycling causes expansion/contraction stress on connectors; condensation forms when cables transition from hot to cold zones, entering connectors through capillary action; silica dust combined with condensation creates paste on connector threads, causing shorts or impedance changes.
Mitigation	Specify high-temperature rated cables for zones exceeding 70°C ambient. Maintain minimum bend radius per manufacturer specifications. Use sealed, compression-style

Aspect	Description
	connectors with gaskets; apply dielectric grease to threads. Route cables through protective conduit in high-dust or high-traffic areas. Implement drip loops and cable glands to prevent moisture ingress at enclosure entry points. Test cables during installation and document baseline insertion loss per segment; re-test during periodic inspections and replace any showing degradation. Avoid routing RF cables parallel to high-current AC power lines to prevent EMI coupling. Color-code or label cable runs for easy identification. Maintain spare cable assemblies on-site.

A.14 Thermal Noise Floor Elevation

Aspect	Description
Cause	Radio receiver front-ends operating in sustained high-temperature environments experience elevated thermal noise due to increased molecular motion in semiconductor junctions and resistive components.
Symptoms	Reduced receiver sensitivity, decreased effective range, higher bit error rates, reduced maximum achievable modulation order, increased packet retries.
Operational Implications	Coverage zones shrink compared to design predictions based on room-temperature receiver specifications; systems designed with marginal link budgets fail to achieve target PDR in hot zones; seasonal variation (summer vs. winter ambient temperatures) creates inconsistent performance that frustrates troubleshooting.
Glass-Specific Aggravation	Furnace radiant heat creates localized ambient temperatures of 60-85°C within 3-5 meters; sustained operation at elevated temperature accelerates component aging, further degrading noise figures over time.
Mitigation	Deploy industrial-grade radios rated for extended temperature operation. Use actively cooled enclosures in high-heat zones; target internal enclosure temperature ≤50°C. Increase link budget margins in hot zones by 3-5 dB to compensate for thermal effects. Monitor radio module temperatures in real-time via SNMP/management. Avoid deploying consumer or standard enterprise-grade equipment in hot zones.

A.15 Time Synchronization Failures

Aspect	Description
Cause	Time synchronization failures due to network congestion, packet delay, asymmetric routing paths, or GPS antenna failures.
Symptoms	Time stamp errors in sensor data logs, TDMA slot misalignment causing collisions in scheduled wireless protocols, coordinated motion failures, security certificate validation failures due to clock skew, data correlation failures in analytics systems.
Operational Implications	Deterministic networking guarantees violated; TSN frame scheduling breaks down; DetNet packet ordering fails; safety-critical systems with time-dependent logic produce false alarms or fail to trigger; forensic analysis and troubleshooting compromised by unreliable timestamps.
Glass-Specific	EMI from furnaces and heavy machinery can affect GPS antenna reception; cable

Aspect	Description
Aggravation	runs from GPS antennas to equipment rooms introduce delay; the non-deterministic nature of contention-based protocols can undermine synchronization accuracy.
Mitigation	Deploy dedicated PTP clocks with GPS disciplined oscillators providing stratum-1 accuracy; ensure GPS antennas have clear sky view and lightning protection. Use boundary clocks at network boundaries to prevent error accumulation across domains. Distribute PTP over wired backbone rather than wireless segments where possible. Implement redundant time sources with automatic failover. Monitor clock offset, path delay, and synchronization state continuously. Test time-sensitive applications under simulated synchronization loss to validate graceful degradation behavior.

A.16 Cryptographic Hardware Stress in High-Temperature Environments

Aspect	Description
Cause	Hardware Security Modules (HSM), Trusted Platform Modules (TPM), and secure elements in SIM/eSIM cards experience accelerated aging, increased error rates, or functional degradation when operated beyond rated temperature specifications; cryptographic operations (key generation, signing, encryption) may slow or produce errors at elevated temperatures.
Symptoms	Authentication failures during production that succeed during cooler periods; increased latency in TLS handshakes or 5G authentication procedures; key generation failures producing weak or duplicate keys; intermittent WPA3 association failures; device certificates failing validation due to signature verification errors.
Operational Implications	Security controls become unreliable precisely when production is most active; troubleshooting falsely implicates network configuration rather than temperature-dependent hardware; compromised cryptographic operations may create undetected security vulnerabilities (weak keys, failed integrity checks); devices repeatedly failing authentication create operational disruptions and support burden.
Glass-Specific Aggravation	Secure elements in modems or sensor nodes operate in ambient temperatures exceeding component specifications; thermal cycling causes solder joint fatigue in surface-mount secure elements; Hardware Random Number Generators may produce degraded entropy at temperature, potentially weakening cryptographic strength.
Mitigation	Specify industrial-grade secure elements and SIM cards rated for extended temperature operation. Deploy cryptographic operations in climate-controlled infrastructure rather than field devices where possible. Use device certificates issued centrally rather than generating keys in-field. For devices that must operate in hot zones, use actively cooled enclosures. Implement cryptographic operation monitoring: track authentication success rates, key generation rates, and latency. Conduct periodic cryptographic health validation. Maintain hardware spares for rapid replacement.

A.17 Frequency Drift and Oscillator Instability

Aspect	Description
Cause	Radio transceivers drift outside specification due to temperature variation, aging, or vibration and exceed compensation range.
Symptoms	Frequency error causing receiver desensitization; adjacent channel interference; receiver unable to lock onto signals due to frequency offset; increased bit error rates from carrier frequency offset; intermittent connectivity as frequency drifts.
Operational Implications	Radios fail to associate or maintain connections despite adequate signal strength; troubleshooting implicates interference or coverage when root cause is local oscillator drift; regulatory compliance violations if transmit frequency error exceeds limits; asymmetric connectivity issues.
Glass-Specific Aggravation	Rapid temperature swings cause transient frequency drift; sustained elevated temperatures shift oscillator frequency outside TCXO correction range; mechanical vibration couples into oscillator mounting, creating phase noise and instability.
Mitigation	Specify radios with OCXO (Oven-Controlled Crystal Oscillators) or high-quality TCXO for infrastructure and mission-critical mobile devices operating in extreme environments. Thermally stabilize radio enclosures to minimize temperature variation rates. Use vibration-isolating mounts for radios in high-vibration zones. Implement frequency error monitoring. Replace radios showing frequency drift.

A.18 DFS False Positives and Radar Detection Issues

Aspect	Description
Cause	Wi-Fi Dynamic Frequency Selection (DFS) radar detection algorithms falsely identify non-radar signals (EMI, multipath reflections, other Wi-Fi devices) as radar, forcing unnecessary channel evacuation; or fail to detect actual radar (false negatives), causing interference to protected services.
Symptoms	Unexpected channel outages when DFS channels are vacated; clients forced to roam or disconnect during channel change; repeated channel switches creating network instability; equipment blacklisting DFS channels exhausting available spectrum.
Operational Implications	Unpredictable network availability violating deterministic performance requirements; clients experience outages during DFS channel changes; time-sensitive application disruptions; administrative burden from investigating repeated DFS events; potential regulatory violation if radars are not detected.
Glass-Specific Aggravation	Broadband EMI from furnaces, heaters, or switching power supplies mimics radar chirp patterns, triggering false DFS detections; multipath reflections in reflective environments create signal copies that DFS algorithms misinterpret as radar.
Mitigation	Avoid DFS-required 5 GHz channels (UNII-2 / UNII-2e) in OT networks; restrict 5 GHz operation to non-DFS bands (UNII-1 and UNII-3) to eliminate radar-induced

Aspect	Description
	channel evacuation. Deploy access points with high-quality, field-tested DFS implementations. Use spectrum analysis to identify and mitigate EMI. Configure backup channels to minimize disruption during DFS events.

A.19 Backup Battery and UPS Failures in Harsh Environments

Aspect	Description
Cause	Uninterruptible Power Supplies (UPS) and backup battery systems experience accelerated aging, capacity loss, or failure when operated outside rated temperature specification reducing battery lifespan and available capacity.
Symptoms	Backup runtime significantly less than rated specifications; UPS systems failing during power events; battery health indicators showing degradation; thermal runaway events; corroded terminals and electrolyte leakage in lead-acid batteries.
Operational Implications	Wireless infrastructure loses power during utility disturbances, creating network-wide outages precisely when reliable communication is most critical (e.g., coordinating procedures during power failures); false sense of backup protection leads to inadequate disaster preparedness; battery replacements during production outages.
Glass-Specific Aggravation	UPS and battery systems located adjacent to furnaces experience sustained elevated temperatures, reducing battery life; thermal cycling from daily furnace operation stresses battery chemistry; dust infiltration into battery compartments increases self-discharge rates and internal resistance.
Mitigation	Locate UPS and battery systems in climate-controlled electrical rooms; avoid co-locating with heat-generating equipment. Specify high-temperature batteries. Derate battery capacity specifications by 30-50% when operating above 25°C ambient. Implement battery temperature monitoring with automated alerts. Conduct load testing regularly. Replace batteries proactively on manufacturer-recommended schedules, adjusted for actual operating temperature. Deploy redundant UPS systems with automatic failover. Consider centralized DC power distribution with battery strings in climate-control rather than distributed UPS systems in harsh locations. Size UPS systems to support graceful shutdown procedures for wireless controllers and servers. Monitor UPS input power quality (sags, surges, harmonics) and install upstream power conditioning as required.

Appendix B: Glossary

AFC (Automated Frequency Coordination)
A cloud-based system for coordinating spectrum sharing in the 6 GHz band. AFC allows Wi-Fi 6E/7 access points to operate at Standard Power (up to 36 dBm EIRP) by dynamically determining channel availability at specific locations to avoid interference with licensed incumbent services (fixed microwave, satellite). Required for outdoor 6 GHz operation and optional for indoor Standard Power operation in the United States and Canada.

AGV (Automated Guided Vehicle)
A mobile industrial vehicle used to transport materials within manufacturing or warehousing environments. AGVs depend on continuous, low-latency, and reliable wireless connectivity for navigation, coordination, and safety functions, particularly in dynamic and interference-rich facilities.

CBRS (Citizens Broadband Radio Service)
A 3.5 GHz spectrum band in the U.S. (Band n48) that allows enterprises to deploy private cellular (LTE/5G) networks without a traditional carrier license. It is managed by a cloud-based Spectrum Access System (SAS).

Determinism
The ability of a network to provide predictable, bounded performance (e.g., latency, jitter, packet delivery) regardless of load or interference. Essential for time-sensitive industrial control; achieved through scheduling and prioritization rather than adaptive algorithms.

DetNet (Deterministic Networking)
IETF framework for extending deterministic capabilities to Layer 3 networks, ensuring end-to-end bounded latency and reliability, often integrated with wireless extensions like RAW.

DFS (Dynamic Frequency Selection)
Regulatory mechanism requiring Wi-Fi devices to vacate channels when radar is detected, introducing unpredictable channel changes.

DPA (Dynamic Protection Area)

Geographic zones where CBRS spectrum can be temporarily revoked to protect federal incumbent users (primarily military radar). Common along U.S. coastlines and near military installations. SAS immediately suspends GAA and PAL grants when DPA is activated. Architectures in DPA regions require spectrum failover strategies.

ESC (Environmental Sensing Capability)

Sensor network that detects federal incumbent radar signals in the CBRS band, triggering SAS to activate Dynamic Protection Areas (DPA). Part of the three-tier CBRS protection architecture. ESC sensor tampering is a security concern as it could cause false DPA activations.

EIRP (Effective Isotropic Radiated Power)

Total power that a theoretical isotropic antenna which radiates equally in all directions would need to emit to produce the same signal strength as a real antenna in its strongest direction.

EMI (Electromagnetic Interference)
Electrical "noise" generated by heavy industrial equipment (e.g., arc furnaces or induction heaters). In glass plants, high EMI can drown out sensitive telemetry data, particularly in unlicensed bands.

Fading
Reduction in signal strength due to multipath interference or environmental factors. In factories, often Rayleigh fading from non-line-of-sight reflections.

GAA (General Authorized Access)

Tier 3 access in CBRS (3.5 GHz band), providing opportunistic, no-cost spectrum access managed by SAS. GAA users have lowest priority and must immediately vacate channels when needed by Incumbents or PAL holders. Suitable for most enterprise private 5G deployments not requiring guaranteed spectrum.

Graceful Degradation
The principle that systems should maintain partial functionality during failures or overloads, rather than complete collapse - critical for safety in glass plants.

Handover / Roaming

Process by which a mobile device transitions connectivity between cells or radios; failure or delay is a dominant reliability risk in mobile industrial systems.

HMI (Human Machine Interface)

The display and control system that allows operators to interact with industrial equipment and processes. Provides visualization of system status, alarms, and control inputs.

IEEE (Institute of Electrical and Electronics Engineers) 3388-2025
The international standard for the "Performance Assessment of Industrial Wireless Systems," providing the framework for measuring network success in factory environments.

IoT (Internet of Things)
The network of physical objects such as sensors, for the purpose of connecting and exchanging data.

ISM (Industrial, Scientific, and Medical) Bands
Unlicensed radio bands including ISM bands (2.4 GHz, 5.8 GHz) and UNII bands (5 GHz, 6 GHz) shared by Wi-Fi, Bluetooth, and industrial devices; prone to interference and in factories.

Jitter
Variation in packet delay; low jitter is vital for synchronized control loops in automation.

Latency
End-to-end delay for packet delivery; bounded latency is a core requirement for deterministic industrial networks.

LPI (Low Power Indoor)

A 6 GHz Wi-Fi device class with 30 dBm EIRP maximum and 5 dBm/MHz power spectral density. LPI operation is restricted to indoor use only and does not require AFC coordination. The default operating mode for most Wi-Fi 6E indoor access points.

MCS (Modulation and Coding Scheme)

A parameter set defining how data is transmitted over a wireless link, combining a specific modulation method and forward error correction coding rate.

Multipath Propagation
Phenomenon where signals arrive via multiple paths (direct and reflected), causing phase interference, fading, or reinforcement. Dominant in glass plants due to highly reflective surfaces like glass sheets and metal structures.

Network Slicing
A 5G feature allowing the logical creation of virtual dedicated networks on shared physical infrastructure, enabling isolation for different use cases (e.g., a reliable slice for safety systems vs. a high-bandwidth slice for staff devices).

OAM (Operations, Administration, Maintenance)

The functions and mechanisms used to monitor, manage, verify, and maintain the health and performance of a network or system throughout its operational lifecycle.

OEE (Overall Equipment Effectiveness)

A manufacturing KPI measuring the percentage of planned production time that is truly productive, calculated from availability, performance, and quality metrics. Used to quantify the operational impact of network reliability.

OFDMA (Orthogonal Frequency-Division Multiple Access)

Multi-user access technique allowing simultaneous transmissions by subdividing channels, improving efficiency under load but not determinism.

OODA (Observe-Orient-Decide-Act)

A decision-making framework that models how systems and operators sense conditions, interpret meaning, choose actions, and execute responses in dynamic environments.

PAL (Priority Access License)

Tier 2 access in CBRS providing county-based, 10-year licensed spectrum (70 MHz total in 10 MHz blocks). PAL holders have priority over GAA but must defer to Incumbents. Provides more predictable spectrum access than GAA for mission-critical applications. Obtained through FCC auction.

PDR (Packet Delivery Ratio)
Percentage of packets successfully delivered without loss.

PKI (Public Key Infrastructure)

A framework of policies and technologies used to manage digital identities, using a public key (shared with everyone) and a private key (kept secret by the owner).

PREOF (Packet Replication, Elimination, and Ordering Functions)

Mechanism in Deterministic Networking (DetNet) used to ensure high reliability and zero packet loss.

PSK (Pre-Shared Keys)

PSK is a method where both communicating parties already know a "shared secret" or password.

PSD (Power Spectral Density)

Power per unit of frequency bandwidth, typically expressed in dBm/MHz. Used in 6 GHz regulations to limit power across channel widths. For example, LPI devices are limited to 5 dBm/MHz, meaning wider channels (80/160 MHz) can use more total power while staying within spectral density limits.

QoS (Quality of Service)

A set of mechanisms used to classify, prioritize, and manage network traffic to meet specific performance objectives such as latency, jitter, and packet loss. In industrial wireless systems, QoS is essential for ensuring time-sensitive and safety-critical traffic is delivered predictably under contention.

RAW (Reliable and Available Wireless)
IETF working group and emerging framework extending DetNet principles to wireless links, addressing challenges like fading, mobility, and interference to achieve high availability in industrial settings.

RBAC (Role-based Access Control)
A security framework that regulates access to computer or network resources based on the roles of individual users within an organization.
RF (Radio Frequency) Shadows
Narrow aisles or zones between large metal machinery and stacked glass inventory that trap and reflect RF energy, intensifying self-interference and multipath distortions.

RSSI (Received Signal Strength Indicator)
Measure of received signal power; frequently misleading in multipath-rich environments, as strong RSSI can coexist with poor reliability due to fading.

SAS (Spectrum Access System)

Cloud-based system that manages CBRS spectrum allocation in the 3.5 GHz band, coordinating access among three tiers (Incumbents, PAL, GAA). SAS dynamically grants and revokes spectrum authorizations based on incumbent protection requirements and interference management. Required for all CBRS deployments.

SCADA (Supervisory Control and Data Acquisition)

An industrial control system architecture used for monitoring, supervisory control, and data collection across distributed assets and processes.

SIL (Safety Integrity Level)

A discrete level (SIL 1 through SIL 4) defined by IEC functional safety standards that specifies the required risk reduction for safety-related systems. Higher SIL levels correspond to more stringent requirements for reliability, availability, and fault tolerance in safety-critical industrial processes.

SNR (Signal to Noise Ratio)
Ratio of received signal power to noise power; more predictive of link reliability than RSSI in interference- and multipath-rich environments

Thermal Gradient
Variations in air temperature that can refract or bend wireless signals, causing unpredictable propagation and signal "shimmering".

TSCH (Time-Slotted Channel Hopping)
Mechanism in IEEE 802.15.4e for low-power deterministic wireless: time is slotted and transmissions hop across channels to avoid interference and ensure collision-free delivery.

TSN (Time-Sensitive Networking)
Suite of IEEE 802.1 standards providing deterministic Ethernet through time synchronization, traffic shaping, and scheduling; serves as the foundation for converged IT/OT networks.

URLLC (Ultra-Reliable Low-Latency Communication)
5G service category designed for mission-critical applications, targeting extremely high reliability (99.99%+) and very low latency with strong guarantees.

VLAN (Virtual Local Area Network)

A logical network segmentation mechanism that partitions a physical network into isolated broadcast domains. VLANs are used to separate traffic by function, criticality, or security domain, reducing contention and limiting fault propagation in converged IT/OT environments.

VLP (Very Low Power)

A 6 GHz Wi-Fi device class with 14 dBm EIRP maximum and -5 dBm/MHz power spectral density. VLP devices can operate both indoors and outdoors without AFC coordination but at significantly reduced range compared to LPI or Standard Power.

Appendix C: References and Research

NIST Publications and Resources

NIST Technical Note (TN) 1951

- **Title:** *Industrial Wireless Systems: Radio Propagation Measurements*
- **Authors:** Candell, R., Remley, C., Quimby, J., Novotny, D., Curtin, A., Papazian, P., Koepke, G., Diener, J., and Hany, M. (2017)
- **Publisher:** National Institute of Standards and Technology, Gaithersburg, MD
- **DOI:** https://doi.org/10.6028/NIST.TN.1951
- **URL:** https://nvlpubs.nist.gov/nistpubs/TechnicalNotes/NIST.TN.1951.pdf
- **Key Content:** Empirical RF channel measurements from three industrial facilities (automotive assembly plant, machine shop, steam plant). Provides path loss models, delay spread, K-factor, and multipath characterization for metal-heavy and thermally variable environments.
- **Used For:** Glass plant environmental loss factors (10-30 dB additional attenuation beyond free space), fade margin requirements (25-30 dB), multipath severity estimates, and baseline propagation models adapted for glass manufacturing.
- **Data Availability:** Raw measurement data publicly available at https://www.nist.gov/ctl/smart-connected-systems-division/networked-control-systems-group/project-data-wireless-systems

NIST Advanced Manufacturing Series (AMS) 300-4

- **Title:** *Guide to Industrial Wireless Systems Deployments*
- **Authors:** Montgomery, K., Candell, R., Liu, Y., Hany, M. (2018)
- **Publisher:** National Institute of Standards and Technology, Gaithersburg, MD
- **DOI:** https://doi.org/10.6028/NIST.AMS.300-4
- **URL:** https://nvlpubs.nist.gov/nistpubs/ams/NIST.AMS.300-4.pdf
- **Key Content:** Comprehensive best practices for industrial wireless deployment, site surveys, technology selection frameworks, and incremental deployment strategies. Covers Wi-Fi, CBRS, and low-power wireless technologies.
- **Used For:** Site survey methodologies, technology selection criteria (Section 3.2), deployment strategies, testing protocols, and deployment guidance.

NIST Wireless Systems for Industrial Environments Project

- **Program:** Ongoing NIST research program focused on industrial wireless testbeds, channel emulation, and non-stationary RF environments
- **Last Updated:** March 26, 2025
- **URL:** https://www.nist.gov/programs-projects/wireless-systems-industrial-environments
- **Key Content:** Current research on deterministic wireless, IEEE 3388 testing frameworks, factory workcell performance benchmarks, AI-assisted testing in reverberation chambers.
- **Used For:** Validation of performance targets, testbed methodologies, continuous research updates on industrial wireless reliability.

NIST-Led Industrial Wireless Standard IEEE 3388 Passes Important Review Steps

- **Type:** News announcement (March 2025)

- **URL:** https://www.nist.gov/news-events/news/2025/02/nist-led-industrial-wireless-standard-ieee-3388-passes-important-review
- **Key Content:** Details on IEEE 3388-2025 approval process, NIST's leadership role, scope of the standard.
- **Used For:** Context on IEEE 3388 development and NIST's involvement in industrial wireless standardization.

Shaping the Future of Connectivity: NIST CTL Builds on IEEE 3388

- **Type:** Feature article (July 2025)
- **URL:** https://www.nist.gov/news-events/news/2025/07/shaping-future-connectivity-nist-ctl-builds-ieee-3388
- **Key Content:** Overview of NIST Communications Technology Laboratory (CTL) activities related to IEEE 3388, testing methodologies, and cross-sector collaboration for industrial wireless evaluation.
- **Used For:** Understanding NIST's ongoing work extending IEEE 3388 frameworks, future directions in industrial wireless research.

NIST Special Publication (SP) 800-137

- **Title:** *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*
- **Authors:** Dempsey, K., Chawla, N., Johnson, A., et al. (2011)
- **Publisher:** National Institute of Standards and Technology, Gaithersburg, MD
- **URL:** https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-137.pdf
- **Key Content:** Continuous monitoring strategies for security and performance in dynamic systems, applicable to industrial wireless.
- **Used For:** Continuous measurement philosophy (Principle 10), monitoring framework (Section 2.5), integration of security and performance monitoring.

NIST Special Publication (SP) 800-82 Revision 3

- Title: Guide to Operational Technology (OT) Security
- Authors: Stouffer, K., Pease, M., Tang, C., et al. (2023)
- Publisher: National Institute of Standards and Technology, Gaithersburg, MD
- URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf
- Key Content: Provides a comprehensive cybersecurity framework for Operational Technology (OT), including risk management for industrial control systems, IT/OT convergence security, and specific wireless security considerations in industrial environments.
- Used For: OT security architecture (Section 2.6, 4.6), establishing security zones and conduits (Section 2.1), and aligning wireless performance with safety-critical security requirements.

IEEE Standards

Industrial Wireless Performance

IEEE 3388-2025

- **Title:** *IEEE Standard for the Performance Assessment of Industrial Wireless Systems*
- **Published:** July 3, 2025

- **Sponsorship:** IEEE Instrumentation and Measurement Society (TC9), Industrial Electronics Society (IES)
- **URL:** https://standards.ieee.org/ieee/3388/11516/
- **Key Content:** Protocol-agnostic framework for evaluating wireless performance in industrial and mission-critical environments. Defines reference RF environment model, aggressor types (interference, multipath, jamming), test profiles, and standardized methodology for measuring latency, jitter, PDR, and throughput under stress.
- **Used For:** Testing protocols (Section 5.3), validation methodology, performance metric definitions (Section 6.1), glass plant test profile development (Appendix D).
- **Note:** This standard was developed with significant NIST leadership and represents current best practice for industrial wireless validation as of 2025.

Wi-Fi Standards

IEEE 802.11-2020

- **Title:** *IEEE Standard for Information Technology-Telecommunications and Information Exchange between Systems-Local and Metropolitan Area Networks-Specific Requirements-Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*
- **Published:** 2020 (consolidates amendments through 2020)
- **URL:** https://standards.ieee.org/ieee/802.11/7028/
- **Key Content:** Complete Wi-Fi specifications including modulation schemes, receiver sensitivity, channel definitions, power limits, MAC protocols.
- **Used For:** Receiver sensitivity reference table, Wi-Fi technical parameters, channel planning, link budget calculations.

IEEE 802.11ax-2021 (Wi-Fi 6)

- **Title:** *IEEE Standard for Information Technology-Telecommunications and Information Exchange between Systems Local and Metropolitan Area Networks-Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 1: Enhancements for High-Efficiency WLAN*
- **Published:** 2021
- **URL:** https://standards.ieee.org/ieee/802.11ax/7536/
- **Key Content:** OFDMA specifications, spatial stream configurations, updated MCS tables for Wi-Fi 6, target wake time (TWT), BSS coloring.
- **Used For:** Wi-Fi 6/6E capacity planning, performance thresholds, integration constraints (Section 4.3).

IEEE 802.11be (Wi-Fi 7) (Informational)

- **Title:** *Extremely High Throughput (EHT) Amendment*
- **Status:** Published 2024
- **Key Content:** Multi-link operation (MLO), 320 MHz channels, 4K-QAM, enhanced features for deterministic latency.
- **Used For:** Future evolution discussions, multi-band strategies mentioned as emerging capability.

Industrial Networking

IEEE 802.15.4-2020

- **Title:** *IEEE Standard for Low-Rate Wireless Personal Area Networks (LR-WPANs)*
- **Published:** 2020
- **URL:** https://standards.ieee.org/ieee/802.15.4/7029/
- **Key Content:** Physical and MAC layer specifications for low-rate wireless. Includes Time-Slotted Channel Hopping (TSCH) for deterministic low-power industrial wireless, forming the basis for WirelessHART, ISA100.11a, and 6TiSCH.
- **Used For:** Deterministic protocol examples (Section 4.4), TSCH for low-power sensor networks, industrial wireless technology options.

IEEE 802.1 Time-Sensitive Networking (TSN) Standards Family

- **Key Standards:** IEEE 802.1Qbv (time-aware scheduling), 802.1AS (timing and synchronization), 802.1Qbu (frame preemption), 802.1Qca (path control), 802.1CB (frame replication and elimination)
- **URL:** https://1.ieee802.org/tsn/
- **Key Content:** Suite of standards enabling deterministic Ethernet through time synchronization, traffic shaping, scheduled access, and bounded latency.
- **Used For:** Wired-wireless convergence architecture (Section 4.1), deterministic networking foundation, integration with IETF DetNet for end-to-end bounded latency.

IEEE Std 145-2013

- **Title:** *IEEE Standard for Definitions of Terms for Antennas*
- **Published:** 2013 (reaffirmed 2020)
- **Key Content:** Antenna gain, EIRP calculations, beamwidth definitions, polarization terminology.
- **Used For:** Antenna selection guidance, EIRP calculations, gain specifications.

IETF Documents

RFC 8655

- **Title:** *Deterministic Networking Architecture*
- **Authors:** Finn, N., Thubert, P., Varga, B., Farkas, J. (2019)
- **URL:** https://www.rfc-editor.org/rfc/rfc8655.html
- **Key Content:** Architectural framework for deterministic networking over IP networks, defining bounded latency and high reliability for time-sensitive applications.
- **Used For:** Deterministic networking concepts (Key Concept box), architectural principles for industrial wireless, bounded latency requirements.

RFC 9320

- **Title:** *Deterministic Networking (DetNet) Bounded Latency*
- **Authors:** Varga, B., Farkas, J., Mirsky, G., Thubert, P. (2022)
- **URL:** https://www.rfc-editor.org/rfc/rfc9320.html
- **Key Content:** Methods for verifying bounded end-to-end latency in DetNet networks.

- **Used For:** Latency calculations, deterministic performance requirements, validation criteria.

RFC 9450

- **Title:** *Reliable and Available Wireless (RAW) Use Cases*
- **Authors:** Thubert, P., Ed. (2023)
- **URL:** https://www.rfc-editor.org/rfc/rfc9450.html
- **Key Content:** Industrial wireless scenarios including factory automation, mobile robots, mining, building automation. Describes reliability and availability requirements for wireless in deterministic networking.
- **Used For:** Use case validation (Section 1.1), requirements for AGV mobility and control systems, wireless-specific challenges in deterministic networks.

IETF RAW Architecture (Work in Progress)

- **Title:** *Reliable and Available Wireless Architecture*
- **Document:** draft-ietf-raw-architecture-30 (July 2025)
- **URL:** https://datatracker.ietf.org/doc/draft-ietf-raw-architecture-30/
- **Status:** Internet-Draft (work in progress, expected RFC publication 2025-2026)
- **Key Content:** Extending DetNet to wireless segments with path diversity, replication, elimination, and scheduling mechanisms to achieve bounded latency and high reliability despite wireless channel variability.
- **Used For:** Wireless deterministic architecture (Section 4.4), path diversity strategies, reliability mechanisms for non-stationary channels.

IETF DetNet Working Group

- **URL:** https://datatracker.ietf.org/wg/detnet/documents/
- **Key Content:** Collection of RFCs and drafts defining bounded-latency networking over IP for time-sensitive applications, including flow management, service layer, and data plane specifications.
- **Used For:** Deterministic networking framework throughout document, traffic management principles, integration with TSN.

Regulatory and Standards Bodies

FCC Regulations (United States)

FCC Part 15 (Unlicensed Spectrum - Wi-Fi)

- **Title:** Code of Federal Regulations, Title 47, Part 15 - Radio Frequency Devices
- **URL:** https://www.ecfr.gov/current/title-47/chapter-I/subchapter-A/part-15
- **Key Content:** Rules for unlicensed operation in ISM bands (2.4 GHz, 5 GHz, 6 GHz). Defines EIRP limits, indoor/outdoor restrictions, power spectral density, DFS requirements, and prohibited channels.

- **Used For:** Regulatory compliance limits in power level tables (Section 3.5.1), channel planning constraints, 6 GHz Low Power Indoor (LPI) rules.

FCC Part 96 (Citizens Broadband Radio Service)

- **Title:** Code of Federal Regulations, Title 47, Part 96 - Citizens Broadband Radio Service
- **URL:** https://www.ecfr.gov/current/title-47/chapter-I/subchapter-B/part-96
- **Key Content:** CBRS band plan (3550-3700 MHz), three-tier access model (Incumbents/PAL/GAA), Spectrum Access System (SAS) requirements, Environmental Sensing Capability (ESC), Dynamic Protection Areas (DPA), power limits by device class.
- **Used For:** CBRS channel planning, DPA considerations for Toledo area (Section 1.1, Appendix F), power level specifications, spectrum coordination requirements.

3GPP Specifications (5G/LTE)

3GPP TS 38.104

- **Title:** *NR; Base Station (BS) radio transmission and reception (Release 16)*
- **Organization:** 3rd Generation Partnership Project
- **URL:** https://www.3gpp.org/ftp/Specs/archive/38_series/38.104/
- **Key Content:** 5G NR base station specifications including power classes, EIRP limits, channel bandwidths, frequency bands (including Band n48 for CBRS), receiver characteristics, spurious emissions.
- **Used For:** CBRS/5G power level specifications, link budget parameters, receiver sensitivity for 5G, capacity estimates.

3GPP TS 23.501

- **Title:** *System architecture for the 5G System (5GS) (Release 16)*
- **Organization:** 3rd Generation Partnership Project
- **URL:** https://www.3gpp.org/ftp/Specs/archive/23_series/23.501/
- **Key Content:** 5G system architecture including network slicing, quality of service (QoS), service-based architecture, user plane/control plane separation.
- **Used For:** Network slicing for segmentation (Section 2.1), 5G architecture concepts, URLLC service definitions.

3GPP Access Traffic Steering, Switching and Splitting (ATSSS)

- **Specification Series:** TS 23.501, TS 24.193
- **Key Content:** Multi-RAT traffic steering mechanisms allowing simultaneous or switched use of 5G and Wi-Fi interfaces for reliability and performance.
- **Used For:** Multi-RAT traffic steering strategy (Section 4.1), hybrid architecture resilience, deterministic mobility.

Industry Alliances and Certification Bodies

Wi-Fi Alliance

- **Organization:** Industry alliance for Wi-Fi certification and interoperability
- **Programs:** Wi-Fi 6/6E Certification, WPA3 Security Certification
- **URL:** https://www.wi-fi.org/
- **Key Content:** Practical device capabilities, interoperability requirements, real-world performance benchmarks, security certification requirements.
- **Used For:** Device density recommendations, WPA3-Enterprise requirements, practical throughput estimates, interoperability validation.

CBRS Alliance (OnGo)

- **Organization:** Industry alliance for CBRS ecosystem development
- **Program:** OnGo Certification Program
- **URL:** https://www.cbrsalliance.org/
- **Key Content:** CBRS device certification requirements, SAS operational specifications, coexistence testing, deployment best practices.
- **Used For:** CBRS deployment guidance (Section 3.5.3), GAA vs. PAL recommendations, device certification requirements, SAS provider selection.

Global mobile Suppliers Association (GSA)

- **Organization:** Industry association representing mobile infrastructure ecosystem.
- **Publications:** Market reports on private mobile networks, 5G deployment statistics.
- **Key Content:** Private network deployment tracking, manufacturing sector adoption data.
- **Used For:** Market context and industry trends (Section 5), private 5G adoption statistics.

Research Papers and Technical References

Path Loss and Propagation

Friis Transmission Equation

- **Source:** Friis, H.T. (1946), "A Note on a Simple Transmission Formula," *Proceedings of the IRE*, 34(5), 254-256
- **DOI:** 10.1109/JRPROC.1946.234568
- **Key Content:** Fundamental equation for free-space path loss: FSPL (dB) = 20 $\log_{10}$(d) + 20 $\log_{10}$(f) + 32.45 (with d in km, f in MHz)
- **Used For:** Baseline path loss calculations before environmental factors are added.

Glass Plant-Specific Adaptations (Methodological Note)

The glass manufacturing-specific environmental penalties and design parameters represent engineering applications of the above research to the unique conditions of glass plants:

Methodology:

1. **Start with NIST TN 1951 industrial baseline:** Path loss, multipath, and interference measurements from metal-heavy industrial facilities (automotive, machine shop, steam plant)
2. **Add glass-specific environmental factors:**
    - **Glass reflection penalty (+5-10 dB):** Based on material properties of glass (high dielectric constant, smooth surface causing specular reflection) and RF behavior at 2.4-6 GHz frequencies
    - **Metal scattering from conveyors (+3-8 dB):** From NIST measurements in metal-heavy factory environments, adjusted for glass plant conveyor density
    - **Thermal refraction near furnaces (+2-5 dB):** Based on atmospheric physics of RF propagation through temperature gradients >1000°C, causing signal bending and additional path loss
3. **Increase fade margins:** 25-30 dB for glass plants vs. 15-20 dB for standard factories, representing conservative engineering practice for harsh, non-stationary environments with extreme multipath
4. **Constrain cell sizes:** 20-40m radius cells vs. 50-100m typical, derived from link budget analysis with increased path loss and required fade margins

Validation Approach: All glass plant-specific parameters must be validated through:

- Site-specific RF surveys per NIST AMS 300-4 methodology
- IEEE 3388-2025 testing protocols with glass plant test profiles
- Empirical measurement during pilot deployment (Section 5.2)
- Continuous monitoring and correlation analysis (Section 2.5)

These adaptations represent informed engineering judgment applied to established research, not arbitrary values. The conservative approach prioritizes reliability over optimistic coverage predictions.

Industry Reports and Market Data (Contextual / Non-Normative)

These sources provide market context and deployment examples but are not normative references:

GSA Private Mobile Networks Report (June 2025)

- **Organization:** Global Mobile Suppliers Association
- **URL:** https://gsacom.com/paper/private-mobile-networks-june-2025/
- **Key Content:** Tracks 1,772 private mobile network deployments globally; manufacturing represents leading sector.
- **Used For:** Industry context (Section 5), adoption trends, market sizing.

Ericsson State of Enterprise Connectivity Report - USA Edition (June 2025)

- **Organization:** Ericsson
- **URL:** https://www.ericsson.com/en/news/2025/6/state-of-enterprise-connectivity-report---usa-edition---june-2025
- **Key Content:** Enterprise adoption of private cellular technologies, manufacturing use cases, deployment drivers.
- **Used For:** Industry trends, enterprise perspectives on private 5G.

\

Private 5G Market 2025-2030

- **Source:** Research and Markets
- **URL:** https://www.researchandmarkets.com/reports/6161605/private-5g-market-opportunities-challenges
- **Key Content:** Market analysis, investment projections, manufacturing-related private 5G use cases.
- **Used For:** Market context, ROI considerations (Section 5.4.3), future outlook.

Global Spectrum Regulatory Reports

GSA Private Mobile Networks - Global Update (December 2025)

- Organization: Global mobile Suppliers Association
- URL: https://gsacom.com/paper/private-mobile-networks-december-2025/
- Key Content: Comprehensive tracking of private mobile network deployments worldwide, with specific focus on CBRS, dedicated local licensing models, and manufacturing sector adoption patterns as of December 2025.
- Used For: International spectrum comparison, validation of licensing model trends, global deployment statistics.

FCC/WInnForum CBRS 2.0 Operational Standards and Exclusion Zone Updates (June 2025)

- Organization**:** Federal Communications Commission / Wireless Innovation Forum
- URL: https://www.fcc.gov/ and https://www.winnforum.org/
- Key Content: Updated CBRS 2.0 specifications including enhanced heartbeat intervals, revised Dynamic Protection Area (DPA) boundaries and enhanced SAS coordination protocols.
- Used For: CBRS deployment guidance (Section 1.1, Appendix F), DPA mitigation strategies, spectrum availability calculations for Toledo region.

BNetzA Status of Local 5G Licenses in Germany (November 2025)

- Organization: Bundesnetzagentur (Federal Network Agency, Germany)
- URL: https://www.bundesnetzagentur.de/
- Key Content: Registry of 550+ issued local 5G licenses in 3.7-3.8 GHz band for industrial/campus networks; licensing procedures, technical requirements, and deployment patterns in German manufacturing sector.
- Used For: International licensing model comparison (Appendix F), European regulatory approach to private spectrum, benchmark for dedicated vs. shared access models.

ARCEP New Framework for 3.8-4.2 GHz Industrial Spectrum (July 2025)

- Organization: Autorité de Régulation des Communications Électroniques, des Postes et de la Distribution de la Presse (France)
- URL: https://www.arcep.fr/
- Key Content: France's regulatory framework for private 5G in 3.8-4.2 GHz and 2.6 GHz TDD bands; local industrial assignment procedures, coexistence rules, and harmonization with EU-wide 3.8-4.2 GHz mandate.
- Used For: European spectrum policy comparison (Appendix F), regulatory harmonization trends, alternative licensing models for industrial wireless.

Vendor-Published Case Studies (Reported Outcomes)

The following case studies provide real-world deployment examples. Performance claims are vendor-reported and represent specific deployment contexts. Readers should validate applicability to their own environments.

Airbus and Ericsson - Hamburg and Toulouse Plants (October 2025)

- **Source:** Ericsson press release and case study
- **URL:** https://www.ericsson.com/en/news/2025/10/airbus-and-ericsson-accelerate-industrial-digitalization-with-private-5g-deployment-at-hamburg-and-toulouse-plants
- **Key Content:** Private 5G Standalone deployment in highly reflective metal aerospace assembly environments (analogous to glass plants). Use cases: IoT integration, real-time quality control, collaborative robotics, AR, predictive maintenance, asset traceability.
- **Used For:** Case study (Section 4, main document), demonstration of 5G overcoming reflective/multipath challenges, large-scale industrial deployment patterns.

John Deere Private 5G - Davenport and Waterloo Works

- **Deployments:** Multiple U.S. manufacturing facilities (Davenport, IA; Waterloo, IA; others)
- **Partners:** Nokia (radio equipment), various systems integrators
- **Key Content:** CBRS-based private 5G supporting 100+ AGVs, 55+ robotic arms, smart tools, asset tracking. Achieved 800 devices per base station vs. ~50 on Wi-Fi. "80-10-10" model: 80% private 5G, 10% Wi-Fi, 10% wired.
- **Used For:** Case study (Section 4), capacity planning reference (800 devices/base station), AGV mobility reliability, manufacturing digital transformation example.
- **Note:** Davenport Works named 2025 Assembly Plant of the Year; deployment scaled significantly 2024-2025.

Celanese Chemical Plant Private 5G (2025)

- **Partners:** NTT DATA, private 5G providers
- **Location:** Texas chemical facility

- **Key Content:** CBRS-based deployment for process automation in EMI-heavy environment (analogous to glass plant furnace zones). Real-time sensor telemetry, robotic process control, safety systems. URLLC slicing and TSN extensions for deterministic control.
- **Used For:** Case study (Section 4), EMI mitigation strategies, chemical process control parallels to glass manufacturing.

Celona - US Steel Manufacturer (2022, updated 2025)

- **Partner:** Celona 5G LAN on CBRS
- **Key Content:** Steel manufacturing deployment (highly reflective metal environment, heavy EMI). Network slicing for prioritized traffic, automated material handling, AGVs, telemetry in interference-prone zones (scrap yards). Reported: reduced unplanned downtime from frequent interruptions to near-zero.
- **URL:** https://www.celona.io/community-stories/us-steel-manufacturer-streamlines-operations-reduces-costs-and-improves-productivity-with-celona-5g-lan
- **Used For:** Case study (Section 4), steel manufacturing parallels to glass plants (reflective surfaces, EMI, AGV mobility), private 5G effectiveness in harsh RF environments.

Note on Case Study Performance Claims: Vendor-reported results (e.g., "near-zero downtime," "80% reduction in handover failures") represent outcomes in specific deployment contexts with baseline conditions that may differ from other facilities. Glass plant engineers should:

- Use case studies as proof points of technical feasibility
- Validate performance expectations through pilot testing (Section 5.2)
- Not assume identical results without site-specific testing per IEEE 3388-2025 protocols

Standards for Security and Compliance

IEC 62443 Series

- **Title:** Industrial communication networks – Network and system security
- **Organization:** International Electrotechnical Commission
- **Key Standards:** IEC 62443-3-3 (system security requirements), IEC 62443-4-2 (component security requirements)
- **Key Content:** Cybersecurity framework for industrial automation and control systems (IACS), security levels, zone and conduit models, component hardening requirements.
- **Used For:** Security architecture (Section 2.6, 4.6), threat modeling (Appendix E), compliance framework, IT/OT security boundaries.

IEC 61511

- **Title:** Functional safety – Safety instrumented systems for the process industry sector
- **Organization:** International Electrotechnical Commission
- **Key Content:** Safety integrity level (SIL) requirements, functional safety lifecycle, safety-instrumented systems design.

- **Used For:** safety-critical wireless requirements, understanding when security failures could induce safety failures, SIL considerations for glass plant control systems.

ISA-95 (IEC 62264)

- **Title:** Enterprise-Control System Integration
- **Organization:** International Society of Automation / IEC
- **Key Content:** Models and terminology for enterprise-manufacturing system integration, control loop timing requirements, IT/OT hierarchy.
- **Used For:** Control loop latency requirements, IT/OT integration architecture, operational context for deterministic networking.

Equipment and Component Specifications

Antenna Manufacturer Technical Data:

- Cisco Aironet antenna series datasheets (gain, beamwidth, mounting specifications)
- CommScope (Ruckus) industrial antenna portfolio
- Laird Connectivity industrial wireless antennas
- Poynting MIMO antennas for harsh environments
- **Used For:** Antenna selection guidance (Section 3.3), gain ranges (2-24 dBi), beamwidth specifications, practical antenna recommendations.

Cable Loss Specifications:

- Times Microwave Systems LMR-series cable specifications
- Andrew Corporation (CommScope) cable loss tables
- **Used For:** Cable loss budgets (Section 3.3), link budget calculation, attenuation values at 5 GHz for common cable types.

Testing Equipment Specifications:

- Manufacturer published specifications and list pricing (Keysight, Rohde & Schwarz, Tektronix, NetAlly, Ekahau)
- **Used For:** Testing equipment recommendations and budget, practical tool selection guidance.

Data Availability and Reproducibility

Researchers and engineers seeking to validate or extend this work can access:

Publicly Available Data:

- **NIST TN 1951 raw RF measurement data:** https://www.nist.gov/ctl/smart-connected-systems-division/networked-control-systems-group/project-data-wireless-systems
- **3GPP specifications:** https://www.3gpp.org/specifications (free download)
- **IETF RFCs and drafts:** https://www.rfc-editor.org/ and https://datatracker.ietf.org/ (free access)

- **FCC regulations:** https://www.fcc.gov/ (free access)

Vendor Resources:

- Case studies and whitepapers: Available from vendor websites (Ericsson, Nokia, Celona, etc.)
- Equipment datasheets: Available from manufacturer websites

How to Cite This Document

Full Citation: Fahey, C. (2025). *Delivering Optimal Wireless in the Glass Manufacturing Plant*. Toledo Tech Loft. NetGoalie

Section-Specific Citation (Example for Section 3.3): Fahey, C. (2025). "Detailed RF Engineering Guidelines," in *Delivering Optimal Wireless in the Glass Manufacturing Plant*, Section 3.5. Design parameters derived from NIST TN 1951, IEEE 3388-2025, IEEE 802.11 standards, and 3GPP TS 38.104, with adaptations for glass manufacturing environments.

Appendix D: IEEE 3388-2025: Standard for the Performance Assessment of Industrial Wireless Systems

IEEE 3388-2025 is an active IEEE standard, published on July 3, 2025. It was developed under the sponsorship of the IEEE Instrumentation and Measurement Society's TC9 (Sensor Technology Committee), with joint sponsorship from the Industrial Electronics Society (IES).

Purpose and Scope

The standard provides a protocol-agnostic framework for evaluating the performance of wireless networks in industrial and mission-critical environments, where reliability, latency, and packet delivery are crucial for sensing, control, optimization, and safety applications. It applies to all wireless protocols (e.g., Wi-Fi, 5G, IEEE 802.15.4-based systems like WirelessHART, Bluetooth) used in factories, automation systems, and operational settings where wireless failures impact safety or functionality.

Key goals:

- Enhance adoption of wireless technologies by providing standardized, repeatable testing methods.
- Address uncertainties in harsh RF environments (e.g., multipath fading, interference from machinery, electromagnetic noise).
- Focus on reliability over ideal conditions, supporting real-world industrial scenarios.

The standard does not specify hardware implementations, underlying algorithms for generating test environments, or operational details of the wireless systems themselves.

Core Components

1. RF Reference Environment Model:
    - Introduces a functional model of radio impairments known as "aggressors" - factors that degrade performance, such as:
        - Interference (e.g., co-channel, adjacent-channel, EMI from equipment).
        - Multipath propagation and fading.
        - Jamming or external noise.
        - Physical blockers and mobility effects.
    - This model simulates RF channels, including physical and electromagnetic degradation.
2. Reference Test Architecture:
    - Defines a standardized setup for testing, including over-the-air (OTA) methods using tools like reverberation chambers or channel emulators.
    - Supports lab-based reproduction of factory-like conditions without on-site disruption.

3. Test Methodology and Evaluation Process:
    - Outlines a transparent, step-by-step process for:
        - Test planning.
        - Execution (e.g., stressing systems with aggressors).
        - Reporting results.
    - Key performance metrics include:
        - Latency and jitter.
        - Packet delivery ratio (PDR) and error rates.
        - Throughput under stress.
        - Reliability probabilities (e.g., for bounded latency in control loops).
4. Standardized Test Profiles:
    - Provides a framework to create tailored profiles for specific industries (e.g., manufacturing, process control), applications (e.g., AGV mobility, sensor telemetry), or severity levels.
    - Profiles allow customization while maintaining comparability across tests.

Development and Impact

- Originated as IEEE P3388 (project authorization in prior years), with significant contributions from NIST's Industrial Wireless Systems team.
- Milestones included balloting in 2024-2025, RevCom review, and final Standards Board approval in early 2025.
- NIST has integrated it with ongoing research, such as AI-assisted testing in reverberation chambers (presented at ISIE 2025).
- It advances wireless reliability in Industry 4.0, complementing standards like IETF DetNet/RAW and NIST guidelines.

This standard is particularly valuable for environments like glass manufacturing, enabling empirical validation of wireless designs against reflective surfaces, thermal effects, and EMI - aligning with measurement-driven approaches for deterministic performance.

Appendix E: Security and Integrity for High-Heat Industrial Wireless

Purpose, Scope, and Threat Model Assumptions

The main document (Sections 2.6 and 4.6) established security as a design requirement integrated with performance, mobility, and determinism. This appendix provides the detailed threat model, formal STRIDE analysis, and compliance mapping for security architects, IT/OT security teams, and auditors.

Intended Audience:

- Chief Information Security Officers (CISOs)
- IT/OT security architects
- Compliance and audit teams
- Security vendors evaluating industrial wireless solutions

Relationship to Main Document:

- **Sections 2.6 and 4.6** provide security requirements for all readers involved in design and implementation
- **This appendix** provides the formal security analysis and compliance details for specialized security roles

What Follows:

- Formal threat model assumptions and attack surface analysis
- Complete STRIDE threat categorization with glass plant context
- Detailed controls mapped to IEC 62443, NIST SP 800-82, and 3GPP standards
- Advanced topics: thermal effects on cryptographic hardware, RF-based attacks, supply chain security

Wireless networks in glass manufacturing plants operate in extreme environments characterized by sustained high temperatures, electromagnetic interference (EMI), reflective surfaces, vibration, and airborne particulates. These physical stressors distort RF propagation, accelerate hardware degradation, and materially increase both cyber and physical security risk.

This appendix defines a threat-modeled security framework for high-heat industrial wireless systems, extending the first principles established in the main document, particularly Principle 9 (Failure Is Inevitable - Resilience Is a Design Choice) and Principle 10 (If It Isn’t Measured, It Isn’t True).

The guidance aligns with IEC 62443, NIST SP 800-82 Revision 3, and applicable wireless standards. It addresses cyber threats, physical integrity risks, and regulatory-induced denial-of-service conditions, with specific emphasis on hybrid architectures such as private 5G combined with Wi-Fi supporting deterministic OT workloads including AGV control, furnace telemetry, and safety-relevant signaling.

Threat Model Assumptions

This appendix assumes:

- An adversary with RF access to the plant perimeter and non-restricted zones.
- Limited or intermittent physical access to edge devices and enclosures.
- The ability to exploit environmental stressors such as EMI and heat to amplify attacks.
- Potential compromise paths through IT/OT convergence points, gateways, and management planes.
- Regulatory spectrum preemption risk, including CBRS Dynamic Protection Areas (DPAs), treated as a non-malicious but impactful denial-of-service condition.

The security objective is to preserve confidentiality, integrity, and availability (CIA) without compromising operational determinism or functional safety.

STRIDE Threat Analysis for High-Heat Industrial Wireless

Spoofing Identity

Unauthorized devices may impersonate legitimate sensors, AGVs, controllers, or access points if identity mechanisms are weak or improperly managed. High-multipath environments can unintentionally extend RF reach, increasing exposure to rogue endpoints.

Impacts include false AGV navigation commands, forged telemetry influencing control logic, and unauthorized access to OT networks.

Mitigations include:

- **Zero-trust identity enforcement** for all devices and users.
- **Certificate-based authentication** for Wi-Fi using WPA3-Enterprise.
- **SIM or eSIM-based mutual authentication** for private 5G per 3GPP standards.
- **Cryptographic device attestation**, where supported, to validate firmware integrity and hardware identity before network admission.
- Prohibition of shared credentials and pre-shared keys in production environments.

Tampering with Data or Systems

Telemetry manipulation, control command alteration, or firmware modification can occur through man-in-the-middle attacks or compromised gateways. In glass manufacturing, manipulated thermal or chemical sensor data can directly induce unsafe operating conditions.

High temperatures also introduce a form of tampering where thermal stress degrades connectors, secure elements, or cryptographic modules, resulting in silent data corruption or explicit failure.

Mitigations include:

- **End-to-end, application-layer encryption** for all control and telemetry data, independent of link-layer security.
- **Secure boot and signed firmware** on all wireless devices.
- Continuous validation of **cryptographic module reliability**, including awareness that prolonged heat exposure may impact hardware random number generators.
- Isolation of management planes from production traffic.

Where telemetry influences safety-instrumented systems, security controls must align with **IEC 61511** and applicable **Safety Integrity Level (SIL)** requirements to prevent security-induced unsafe states.

Repudiation

Without strong identity binding and logging, operators or adversaries may deny responsibility for actions such as configuration changes, device associations, or spectrum modifications.

Mitigations include:

- Strong, non-repudiable identity mechanisms tied to devices and users.
- Centralized, tamper-resistant logging across wireless, RF, and OT management systems.
- Time-synchronized logs suitable for forensic analysis and audit.

Information Disclosure

Wireless eavesdropping is amplified in reflective, high-heat environments due to multipath propagation extending signal reach.

Mitigations include:

- Mandatory encryption for all data in transit and at rest.
- Strict segmentation preventing best-effort or IT traffic from accessing sensitive OT data.
- Shielded enclosures and directional antenna design to minimize unintended RF leakage.

Denial of Service (DoS)

Denial-of-service in glass plants can arise from multiple vectors:

- Intentional RF jamming.
- EMI from arc furnaces, induction heaters, or large motors.
- Regulatory spectrum preemption, such as CBRS DPA events.
- Thermal-induced hardware throttling or failure.

Mitigations include:

- Deterministic segmentation, isolating life-safety and real-time control traffic from best-effort systems using VLANs, firewalls, 5G network slicing, or Wi-Fi 7 Multi-Link Operation.
- Explicit prohibition of shared control planes between safety-critical and non-critical networks.
- CBRS 2.0 extended heartbeat capability to sustain operations during SAS connectivity loss.
- Multi-band and multi-path communication strategies for redundancy.
- Continuous RF monitoring to distinguish between inherent EMI, gray-zone interference, and malicious jamming.

Elevation of Privilege

Attackers may exploit weak segmentation, misconfigured gateways, or shared management infrastructure to move laterally from IT networks into OT wireless systems.

Most malware propagation in wireless OT environments occurs through management systems, controllers, or gateways, rather than constrained field radios.

Mitigations include:

- Strict enforcement of IT/OT boundary controls with continuous verification.
- Role-based access control and multi-factor authentication for all wireless management interfaces.
- Least-privilege configuration of controllers, orchestration platforms, and spectrum managers.

Environment-Specific Security Considerations

Private 5G and CBRS Resilience

CBRS deployments in DPA regions must treat spectrum revocation as a regulatory denial-of-service condition. Architectures should provide:

- Local survivability through CBRS heartbeat mechanism with extended intervals.
- Failover paths to alternate spectrum or technologies.
- Operational playbooks for spectrum loss scenarios.

Wi-Fi 7 Integrity

Wi-Fi 7 deployments should enforce:

- Protected Management Frames (PMF) to prevent deauthentication attacks.
- Multi-band operation and Multi-Link Operation for interference resilience.
- Isolation and hardening of Wi-Fi management planes.

RF Aggressors and EMI Validation

The IEEE 3388-2025 reference architecture enables RF baseline characterization under multipath and EMI stress. These baselines should be treated as forensic artifacts, supporting detection, attribution, and corrective action following RF security events.

Dynamic Protection Areas (DPA) as an Integrity Consideration

Section 1.1 introduced CBRS Dynamic Protection Areas as a spectrum management challenge. From an integrity perspective, DPA preemption is a form of regulatory denial-of-service.

Design Requirement: Architectures deployed in DPA regions must treat spectrum revocation as a security-relevant availability threat.

Mitigation Strategies:

- CBRS heartbeat mechanism: Maintains local operation during temporary SAS connectivity loss.
- Multi-band failover: Automatic failover to alternative spectrum or Wi-Fi when preempted.

- Operational playbooks: Pre-defined procedures for spectrum loss scenarios, including notification chains and fallback communication paths.

Toledo-Specific Implication: Glass plants along the Maumee River and Lake Erie are in Tier 1 protection zones. While DPA events are infrequent, they are non-negotiable as military radar takes precedence. Treating this as a security consideration ensures continuity of safety-critical communications during spectrum loss.

Alignment with Standards and Frameworks

- **IEC 62443**, defining component and system security requirements for industrial automation and control systems.
- **NIST SP 800-82 Revision 3**, guiding OT risk management, zero-trust adoption, and continuous monitoring.
- **3GPP standards** for SIM-based authentication and encryption in private 5G.
- **IEEE 3388-2025**, integrating RF performance assessment with security validation under harsh industrial conditions.

Appendix F: Summary of Global 5G Implementation Practices

This appendix summarizes key approaches to private 5G spectrum allocation worldwide as of December 2025, with a focus on mid-band spectrum suitable for industrial deployments (e.g., manufacturing plants). The primary distinction lies in licensing models: many international markets reserve dedicated mid-band spectrum for local/private use via direct enterprise licensing, whereas the United States utilizes a shared, dynamic access framework.

United States: Shared Spectrum via CBRS (Three-Tiered Access)

- **Band:** 3.55-3.7 GHz (150 MHz, Band n48).
- **Model:** Citizens Broadband Radio Service (CBRS), by automated **Spectrum Access Systems (SAS)**.
- **Tier 1: Incumbents** (e.g., U.S. Navy radar) - Full priority and protection.
- **Tier 2: Priority Access Licenses (PALs)** - Auctioned county-based licenses (70 MHz total) providing 10-year protected access.
- **Tier 3: General Authorized Access (GAA)** - "License-by-rule" (no-cost, no application required). Offers open access but is subject to SAS coordination to mitigate interference.
- **Key Differences:** The U.S. does not currently offer a direct-to-enterprise "site license" similar to Germany. Instead, enterprises access shared spectrum. This lowers entry costs and has made CBRS the dominant band for U.S. private networks, supporting over 1,500 commercial deployments in manufacturing, logistics, and healthcare as of late 2025.
- **2025 Updates:** Implementation of **CBRS 2.0** has reduced coastal exclusion zones by 30%, increasing spectrum availability in industrial port regions.
- **Implication for Glass Plants:** Highly cost-effective for Toledo facilities. GAA is suitable for internal factory use, though PAL leases are recommended for mission-critical robotics to ensure higher protection from interference.

Europe

European regulators have prioritized "Industry 4.0" by granting enterprises direct access to spectrum, bypassing traditional mobile network operators.

- **Germany (Market Leader):**
- **Band:** 3.7-3.8 GHz (100 MHz reserved exclusively for private/campus networks).
- **Model:** BNetzA direct site-licensing. Over 550 licenses issued by December 2025.
- **Key:** Guaranteed exclusive use per site; highly predictable for heavy industrial automation.
- **United Kingdom:**
- **Bands:** 3.8-4.2 GHz (Shared Access) and 26 GHz (mmWave).
- **Model:** Ofcom’s "Shared Access Licenses."
- **Key:** A hybrid approach using low-power indoor licenses that are coordinated to prevent overlap.

- **France:**
- **Band:** 3.8-4.2 GHz (newly opened in 2025) and 2.6 GHz TDD.
- **Model:** ARCEP local industrial assignments.
- **EU Harmonization:** By late 2025, the European Commission has mandated the **3.8-4.2 GHz** band be harmonized for local, low-power industrial use across all member states to reduce equipment fragmentation.

Asia-Pacific

- **Japan:**
- **Bands:** 4.6-4.9 GHz (Local 5G) and 28 GHz.
- **Model:** MIC Local 5G licensing. Japan emphasizes high-frequency mmWave for ultra-low latency in smart factories.
- **South Korea:**
- **Bands:** 4.7 GHz and 28 GHz ("e-Um 5G").
- **Model:** Dedicated spectrum for non-telecom companies (e.g., Samsung, Naver) to run their own private industrial networks.
- **China:**
- **Bands:** 3.3-3.6 GHz and 4.8-5.0 GHz.
- **Model:** Primarily MNO-led (Mobile Network Operator) private "slices," though direct 5.0 GHz licensing for industrial campuses has expanded in 2025.

Summary Comparison Table (2025)

Aspect	United States (CBRS)	Europe / Asia-Pacific
Licensing Type	Shared/Dynamic (No direct site license)	Dedicated Local/Exclusive License
Cost / Barrier	GAA is free; SAS fees are minimal.	Small application fees.
Protection	GAA is "best effort" sharing.	Exclusive rights to the site frequency.
Operational Control	Managed by automated SAS cloud.	Managed by the enterprise/regulator.

Appendix G: Wi-Fi 2.4, 5, 6 GHz Spectrum: Regulatory Classes, Advantages, and Limitations

This appendix summarizes characteristics, regulatory constraints, and practical deployment considerations of the 2.4 GHz, 5 GHz, and 6 GHz Wi-Fi bands in industrial environments, with specific emphasis on glass manufacturing facilities. Each band presents distinct tradeoffs in coverage, capacity, interference susceptibility, and determinism that must be explicitly accounted for during RF design.

G.1 Wi-Fi 2.4 GHz Band

Frequency Range: 2.400–2.4835 GHz (ISM band, globally harmonized)
Regulatory Model: Unlicensed, no coordination requirements

Advantages

- **Broad device compatibility:** Supported by virtually all Wi-Fi clients, including legacy and industrial embedded devices.
- **Resilience in marginal RF conditions:** Often the only band that remains usable in high-attenuation zones or deep plant interiors.

Limitations

- **Severely limited spectrum:** Only three non-overlapping 20 MHz channels, resulting in chronic co-channel contention.
- **High interference density:** Coexists with Bluetooth, Zigbee, proprietary ISM radios, microwave leakage, and industrial control systems.
- **Poor determinism under load:** CSMA contention and airtime starvation make 2.4 GHz unsuitable for latency-sensitive or high-reliability OT traffic.

2.4 GHz should be treated as a coverage and compatibility band of last resort, reserved for low-rate sensors, legacy devices, and fault-tolerant applications. It should not be relied upon for primary plant connectivity or real-time control traffic.

G.2 Wi-Fi 5 GHz Band

Frequency Range: 5.150–5.850 GHz (UNII-1/2/2e/3; regional variations apply)
Regulatory Model: Unlicensed, with DFS requirements in radar-sharing sub-bands

Advantages

- **Expanded channel availability:** Significantly more spectrum than 2.4 GHz, enabling channel reuse and reduced contention.
- **Balanced propagation vs. capacity:** Offers materially higher throughput than 2.4 GHz while maintaining workable indoor range.

- **Mature ecosystem:** Broad enterprise support, extensive tooling, and predictable behavior across client classes.

Limitations

- **DFS operational risk:** Channels subject to radar detection can force disruptive channel changes, impacting availability.
- **Moderate penetration loss:** Attenuation through dense machinery, stacked glass, and metal infrastructure is materially higher than 2.4 GHz.
- **Legacy coexistence:** Presence of older 802.11a/n/ac devices increases airtime overhead.

5 GHz remains the primary workhorse band for most industrial Wi-Fi deployments. In glass plants, it is best suited for controlled micro-cell designs with conservative channel widths (20–40 MHz) and explicit fade margins.

G.3 Wi-Fi 6 GHz Band (Wi-Fi 6E / Wi-Fi 7)

Frequency Range: 5.925–7.125 GHz (United States; international allocations vary)
Regulatory Model: Unlicensed, class-based power limits; AFC required for Standard Power devices

Advantages

- **Clean spectrum:** 1.2 GHz of new unlicensed bandwidth with no legacy Wi-Fi, Bluetooth, or Zigbee devices.
- **High channel density:** Up to 59 non-overlapping 20 MHz channels, 14 × 80 MHz, or 7 × 160 MHz channels.
- **Mandatory modern PHY:** All devices support OFDMA, MU-MIMO, and Target Wake Time without backward-compatibility penalties.

Limitations in Glass Manufacturing Environments

Propagation Characteristics

- **Higher free-space path loss:** Approximately +2.5 dB versus 5 GHz and +7.5 dB versus 2.4 GHz at equal distance, yielding ~30–40% shorter effective range indoors.
- **Thermal and material absorption:** Elevated attenuation in high-temperature air masses near furnaces and increased reflection/absorption from coated glass surfaces. Empirical industrial measurements show an additional 3–6 dB loss relative to 5 GHz in high-heat zones.
- **Severe multipath sensitivity:** Shorter wavelength increases the density of destructive interference nulls in reflective environments, requiring higher fade margins (≥30 dB) and strong MIMO spatial diversity.

G.4 6 GHz Regulatory Device Classes (United States – FCC Part 15)

Device Class	Max EIRP	PSD Limit	Indoor / Outdoor	AFC Required	Typical Range	Primary Use
Low Power Indoor (LPI)	30 dBm	5 dBm/MHz	Indoor only	No	30–50 m	Enterprise APs
Standard Power (SP)	36 dBm	8 dBm/MHz	Indoor & outdoor	Yes	100–200 m	Outdoor / campus
Very Low Power (VLP)	14 dBm	–5 dBm/MHz	Indoor & outdoor	No	5–15 m	Client devices

G.5 Operational Considerations by 6 GHz Device Class

Low Power Indoor (LPI)

- No AFC dependency simplifies deployment and avoids external availability risks.
- Well-aligned with indoor glass plant use cases.
- PSD limits favor wider channels for efficiency, improving link budgets without exceeding EIRP caps.

Standard Power (SP)

- AFC dependency introduces operational risk (internet outages, geolocation errors, AFC system failures).
- Best suited for non-critical IT connectivity or outdoor backhaul, not mission-critical OT traffic.

Very Low Power (VLP)

- Intended exclusively for client devices.
- Severely limited range necessitates dense AP placement when VLP clients dominate.

G.6 Integration with Hybrid Wireless Architectures

When deploying multiple Wi-Fi bands alongside private LTE/5G:

- Use **2.4 GHz for compatibility**, not performance
- Use **5 GHz for primary plant connectivity**
- Use **6 GHz for best-effort, high-throughput offload**, not baseline coverage
- Maintain band-specific SSIDs and VLANs
- Apply band-steering policies that prioritize determinism over peak throughput
- Keep 6 GHz airtime utilization below ~40% to preserve latency and contention advantages

Appendix H - RF Site Survey Methodology

This appendix defines a standardized, repeatable methodology for RF site surveys in glass manufacturing facilities. The scope is limited to RF characterization, validation, and documentation activities used to inform or verify industrial wireless designs. This methodology is aligned with NIST SP 1900-5 for industrial wireless testing and IEEE 3388-2025 for performance assessment, with emphasis on measurement over assumption and validation under representative operating conditions.

Commercial RF planning and survey platforms (e.g., Ekahau, AirMagnet, MetaGeek, or equivalent tools) are assumed for floor plan management, measurement capture, visualization, and reporting.

Pre-Survey Planning

Prior to on-site measurements, the following information shall be collected and documented to ensure surveys are safe, repeatable, and representative of production conditions.

Facility Overview:

- Facility name and location
- Total floor area and ceiling heights by zone
- Number and type of production lines
- Shift schedules and peak production periods
- Planned shutdown or maintenance windows

Critical Operational Zones:

- Furnaces and hot-end processes
- Glass handling, storage, and inspection areas
- Metal conveyor systems and large equipment
- AGV routes, intersections, and charging stations
- Control rooms, PLC cabinets, and MCCs
- Maintenance and QA areas
- Office and administrative spaces

Existing Infrastructure:

- Wireless systems currently in use and operating bands
- Wired backbone and fiber locations
- Power distribution and PoE switch locations
- Candidate antenna or access point mounting points
- Cable pathway availability and constraints

Environmental Factors:

- Furnace duty cycles and thermal profiles (e.g., temperatures up to 1,500°C in hot zones)
- EMI-generating equipment (e.g., induction heaters, VFDs, large motors)
- Glass composition and coatings, including Low-E prevalence
- Material motion patterns affecting multipath behavior (e.g., conveyor speeds of 5 m/s)
- Shift-based or seasonal environmental variation

Safety and Access:

- PPE requirements by zone (hot work, confined space, elevated work)
- Permit requirements
- Escort and restricted-area requirements
- Emergency procedures and evacuation routes

Stakeholders:

- Operations and production management
- Facilities and safety leadership
- IT/OT network owners
- Area supervisors by zone

Equipment Preparation

All measurement equipment shall be verified as operational, calibrated, and suitable for high-temperature industrial environments.

Spectrum Analysis Equipment:

- Coverage of 2.4 GHz, 5 GHz, 6 GHz, and 3.5 GHz (CBRS where applicable)
- Real-time bandwidth sufficient for interference detection (e.g., 100 MHz capture)
- Calibration within manufacturer specifications
- Omnidirectional antennas for general surveys
- Adequate power, storage, and heat-resistant cases (e.g., rated for 60°C operation)

RF Survey Platform:

- Valid software licenses
- Correctly scaled and verified floor plans
- Calibrated survey adapters and backup devices
- Sufficient storage for raw data and heat maps

Network Test Equipment:

- Portable access points or test radios with known configurations
- Known-good client devices

- Traffic generation and measurement tools (e.g., iPerf for throughput testing)
- Required mounting hardware, cabling, and adapters

Environmental Instrumentation (as required):

- Thermal sensors or imaging tools (e.g., FLIR cameras for gradient mapping)
- Time synchronization across measurement devices (e.g., NTP or GPS for correlated logs)

Passive Spectrum and Environmental Survey

Passive measurements shall be conducted before active testing to establish baseline noise floors and identify interference sources.

Spectrum Analyzer Configuration:

- Full-band sweeps appropriate to each technology
- Resolution bandwidth appropriate to the band under test (e.g., 100 kHz for Wi-Fi bands, 30 kHz for narrowband EMI)
- Peak or sample detector with max-hold enabled
- Capture of instantaneous, average, and max-hold traces

Measurement Locations:

- Furnace perimeters and hot-end zones
- Metal conveyor paths and high-power machinery
- AGV routes and charging areas
- Electrical rooms and control cabinets
- Office and administrative areas

Survey Outputs:

- Noise floor by band and zone (e.g., target -85 to -95 dBm in clean areas)
- Persistent interferers and duty cycle characteristics
- Transient or production-correlated EMI events
- Time-of-day and shift-based variation
- Indicators of severe multipath or delay spread (e.g., via channel impulse response if tool supports)

Active Coverage and Link-Performance Survey

Active surveys shall validate signal propagation and link quality under representative operating conditions.

Temporary Access Point Deployment:

- Representative mounting height and orientation (e.g., 3-5 m above floor for industrial APs)
- Power levels and channel widths consistent with intended design (e.g., 20 dBm EIRP, 40 MHz channels)
- Secure, safety-compliant cabling and power
- Logging and time stamping enabled

Survey Execution:

- Walking surveys conducted at production-relevant device heights
- Separate datasets captured for each frequency band
- Measurements taken during normal operating conditions

Metrics Collected:

The following table outlines key metrics and example pass criteria for industrial wireless in glass environments:

Metric	Description	Example Pass Criterion
RSSI	Received Signal Strength Indicator	> -70 dBm in coverage zones
SNR	Signal-to-Noise Ratio	> 25 dB for reliable links
PDR	Packet Delivery Ratio	> 99% for mission-critical use cases
Latency	End-to-end packet delay	< 20 ms for control/automation traffic
Jitter	Variation in latency	< 5 ms for time-sensitive applications
Roaming/Handover	Transition behavior (where mobility applies)	< 50 ms handover time, no packet loss

Performance and Stress Validation

Additional testing shall confirm resilience under load, interference, and edge-of-coverage conditions.

Concurrent Load Testing:

- Emulation of maximum expected client density per access point (e.g., 20-50 clients for dense zones)
- Traffic generation matching anticipated use-case patterns (e.g., UDP for telemetry, TCP for file transfers)
- Monitoring of airtime utilization, retries, throughput, and latency
- Pass criterion: Graceful degradation without hard failures (e.g., airtime < 60% under load)

Peak-Production EMI Testing:

- Execution during periods of maximum interference
- All furnaces and major equipment operating

- Monitoring of noise floor changes, retries, and error indicators
- Pass criterion: Performance remains within defined tolerances (e.g., PDR > 95% during EMI bursts)

Edge-of-Coverage and Mobility Testing:

- Systematic testing at designed cell boundaries
- Observation of packet loss and handover stability
- Pass criterion: No coverage gaps and stable transitions (e.g., < 100 ms recovery from fades)

Interference Correlation and Prioritization

Observed EMI patterns shall be correlated with production schedules using time-aligned measurements.

- Distinguish expected equipment-generated EMI from anomalous interference
- Identify maintenance- or testing-friendly time windows
- Validate effectiveness of mitigation strategies
- Establish baseline data for future comparison

Interference Impact Priority:

- Critical - safety or production-critical impact
- High - significant operational degradation
- Medium - best-effort traffic affected
- Low - marginal impact acceptable

CBRS Considerations (Where Applicable)

- Identify facility proximity to coordination or protection zones
- Complete registration with an approved spectrum access system
- Monitor grant status during testing
- Document preemption events and recovery behavior
- Measure operational impact and failover response (e.g., < 5 s to alternate band)

Reporting and Deliverables

Executive Summary:

- Facility and survey dates
- Objectives and evaluated technologies
- Coverage achieved and key performance results
- Critical gaps and risks identified
- High-level recommendations

Detailed Findings:

- Coverage heat maps by zone and band
- RSSI and SNR distributions
- Performance, capacity, and mobility results
- Identified EMI sources and quantified impact
- Observed thermal and multipath effects

Recommendations:

- Immediate mitigations (critical or high priority)
- Pre-deployment tasks and dependencies
- Required approvals
- Residual risks and documented assumptions

Post-Survey Validation and Monitoring

To support long-term resilience, periodic resurveys are recommended annually or after major layout changes.

- Compare new measurements against established baselines
- Update EMI correlations as production conditions change
- Integrate findings into monitoring and alerting systems
- Document deviations and corrective actions