FROM CONNECTED DEVICES TO REAL-TIME DECISION INFRASTRUCTURE

5G and IoT: Enabling Real-Time Connectivity

Executive briefing — Network and technology strategy leaders | ~20 min

Why 5G Changes the IoT Equation

- 4G/LTE was designed for human-scale traffic; 5G is designed for machine-scale traffic
- Three technical levers move together: latency, device density, and bandwidth
- Latency: air-interface latency can drop into the single-digit millisecond range under 5G (industry-reported range), versus tens of milliseconds on 4G
- Density: 5G specifications target roughly 1 million connected devices per square kilometer (industry-reported range), well above 4G ceilings
- Bandwidth: multi-gigabit peak throughput supports video, sensor fusion, and telemetry at a scale 4G could not sustain concurrently

From 'Connectivity' to 'Control Loop'

- Lower, more consistent latency turns wireless from a monitoring channel into a control channel
- Enables closed-loop actions where a sensor reading can trigger a machine response within the same network cycle
- Jitter and reliability matter as much as raw speed for control applications — 5G's scheduling improves consistency, not just averages
- This shifts the conversation from 'is the device connected' to 'can this connection be trusted for a real-time decision'
- Strategy implication: connectivity choices now belong in the operational technology (OT) reliability conversation, not just IT procurement

Private 5G Networks for Industrial Sites

- A private 5G network is a dedicated cellular network scoped to one site, campus, or facility, operated for a single organization's traffic
- Gives the operator control over coverage design, prioritization, and data residency that public carrier networks do not offer by default
- Common deployment models: fully self-managed, carrier-managed private network, or hybrid with a neutral host
- Well suited to environments with dense machinery, mobile assets (AGVs, forklifts), and areas where Wi-Fi has historically struggled with interference or roaming handoff
- Illustrative scenario: a manufacturing site replacing a patchwork of Wi-Fi access points with a single private 5G network to support mobile robotics — not a verified case study

Network Slicing for Differentiated IoT Workloads

- Network slicing partitions a single physical 5G network into multiple logical networks, each with its own performance guarantees
- Allows an operator to run mission-critical control traffic, video surveillance, and routine asset-tracking telemetry on one infrastructure without one workload starving another
- Each slice can be tuned for latency, throughput, or reliability priorities independently
- Reduces the need to build and maintain separate physical networks per use case, which is a meaningful capital and operating cost lever
- Slicing maturity varies by vendor and deployment model — worth validating specific SLA guarantees during vendor evaluation rather than assuming parity across providers

Use Cases Unlocked by Low Latency

- Real-time process control: closed-loop adjustments to machinery, robotics, or production lines based on live sensor input
- AR-assisted maintenance: technicians view overlaid diagnostic or repair guidance while working, requiring low-latency video and data sync
- Coordinated mobile robotics: multiple autonomous units operating safely in shared space depends on consistent, low-latency communication
- Remote and tele-operated equipment: operating machinery from a control room in near real time, particularly in hazardous environments
- These use cases were technically constrained under prior-generation wireless — 5G removes latency as the primary blocker, though application-layer engineering still matters

Coexistence with LPWAN and Wi-Fi, Not Replacement

- 5G does not replace existing LPWAN (LoRaWAN, NB-IoT) or Wi-Fi deployments — each serves a different point on the cost/range/power curve
- LPWAN remains the more efficient choice for low-frequency, low-bandwidth sensors (e.g., periodic environmental or asset condition readings) where battery life spans years
- Wi-Fi remains appropriate for fixed, high-bandwidth applications within a confined area at lower infrastructure cost
- 5G's role is filling the gap: mobile, latency-sensitive, or high-density scenarios that LPWAN and Wi-Fi were not designed for
- Most mature IoT strategies will run a mixed connectivity portfolio rather than standardizing on a single technology

Cost and Coverage Tradeoffs

- Private 5G infrastructure (radios, core network, spectrum access, integration) carries meaningfully higher upfront cost than extending existing Wi-Fi or LPWAN
- Total cost of ownership depends heavily on spectrum acquisition path, site density, and whether the network is self-managed or carrier-managed
- Coverage design for 5G, especially at higher frequency bands, requires more careful RF planning indoors than lower-frequency LPWAN
- Return on investment is strongest where the use case genuinely requires low latency or high device density — applying 5G to a use case LPWAN already serves well is unlikely to justify the cost
- Recommend cost modeling be use-case-driven, not connectivity-technology-driven, to avoid over-building infrastructure

Security Considerations for Private 5G

- Private 5G networks bring a different threat model than public carrier networks: the organization now owns network-level security, not just endpoint security
- SIM- or eSIM-based device authentication provides stronger identity assurance than many existing Wi-Fi or LPWAN credential schemes
- Network slicing can be used to isolate OT and IT traffic logically, but isolation must be validated, not assumed from the vendor's marketing description
- Core network placement (on-premises vs. cloud-hosted) affects data residency and exposure — a relevant question for regulated industries
- Security review should be a gating step in vendor selection, not a post-deployment audit

Carrier-Provided vs. Private Network: Decision Criteria

- Carrier-provided 5G (public network, enterprise plans, or network slicing on shared infrastructure) suits distributed, mobile, lower-control-sensitivity use cases
- Private 5G suits fixed-site, high-density, or control-critical use cases where latency consistency and data sovereignty matter most
- Key questions: does the use case require guaranteed latency, does data need to stay on-premises, and does device density exceed what the carrier's shared network can prioritize for us
- Hybrid approaches are common — private 5G on-site with carrier connectivity for mobile or remote assets outside the site boundary
- Decision should be revisited use case by use case; a single connectivity decision rarely fits an entire enterprise portfolio

Spectrum and Regulatory Considerations

- Private 5G requires access to licensed, shared, or unlicensed spectrum, and availability varies significantly by country and regulator
- Some jurisdictions offer shared or lightly licensed spectrum specifically for private industrial use (regulatory frameworks differ by region and are evolving)
- Spectrum strategy affects vendor choice, equipment cost, and how much coordination is required with incumbent carriers
- Regulatory approval timelines should be built into project planning early — this is frequently the longest lead-time item in a private 5G rollout
- Legal and regulatory affairs teams should be engaged at the feasibility stage, not after network design is finalized

Where Organizations Get This Wrong

- Treating 5G as a like-for-like Wi-Fi upgrade rather than a distinct architecture decision with different cost and skill requirements
- Underestimating in-building RF planning complexity, particularly in dense industrial environments with metal structures and machinery
- Deploying private 5G before OT and IT security teams have agreed on a shared operating model for the network
- Selecting connectivity technology before use cases and latency requirements are clearly defined, leading to over- or under-engineering
- Skipping a pilot phase and committing to site-wide rollout before validating vendor claims against actual site conditions

A Practical Adoption Roadmap

- Phase 1 — Assessment: inventory current connectivity, identify use cases genuinely blocked by latency, density, or bandwidth limits
- Phase 2 — Pilot: deploy a scoped private 5G or slicing pilot on one site or one production line, with clear success criteria defined upfront
- Phase 3 — Validate: test latency, reliability, and security assumptions under real operating conditions, not just vendor lab conditions
- Phase 4 — Scale: extend validated architecture to additional sites, incorporating lessons on RF planning, spectrum, and integration cost
- Phase 5 — Operate: establish ongoing governance for network performance, security monitoring, and OT/IT coordination

Governance and Organizational Readiness

- Private 5G blurs the line between telecom infrastructure and operational technology — ownership needs to be explicitly assigned, not assumed
- Cross-functional governance (network engineering, OT, security, facilities) should be established before procurement, not after
- Vendor management shifts from a single carrier relationship to potentially multiple infrastructure and integration vendors
- Skills gap is common: most IT and OT teams have limited hands-on experience with cellular network operations and will need training or managed-service support
- Budget planning should separate one-time infrastructure investment from ongoing operating costs (spectrum fees, managed services, maintenance)

Next Steps and the Ask

- Commission a use-case assessment across priority sites to identify where latency, density, or mobility genuinely justify 5G investment
- Select one site for a scoped pilot with defined technical and business success criteria, timeboxed to a single quarter
- Engage security and regulatory stakeholders at the feasibility stage to avoid late-stage rework
- Request budget authorization for pilot-phase infrastructure and vendor evaluation, separate from any full-scale rollout commitment
- Decision needed from this group: approve the pilot site and assessment scope, and confirm cross-functional governance ownership before procurement begins