International Journal of Leading Research Publication (IJLRP)
E-ISSN: 2582-8010 ● Website: www.ijlrp.com ● Email: editor@ijlrp.com

Architecting and Analyzing Private 5G/LTE Networks for Ultra-Reliable and Deterministic Industrial IoT Environments

Rahul Bangera

Ellicott City, MD, USA.
rahulmbangeragmail.com

Abstract:
The realization of Industry 4.0 fundamentally depends on secure, scalable, and deterministic connectivity for cyber-physical systems [1]. Traditional wireless solutions often do not meet the stringent requirements for Ultra-Reliable Low-Latency Communication (URLLC). This paper explores the architecture and deployment strategies of Private 5G/LTE Networks integrated with Mobile Edge Computing (MEC), designed for Industrial IoT (IIoT) environments. It proposes an architecture reference that emphasizes the need for 5G Standalone (SA) Core localization and 3GPP Release 16 Time-Sensitive Networking (TSN) integration to ensure predictable performance. The paper ends with a discussion of challenges, including AI-driven resource orchestration and ultra-precise time synchronization.

Keywords: Private 5G, Industrial IoT (IIoT), URLLC, mMTC, Mobile Edge Computing (MEC), Time-Sensitive Networking (TSN), Deterministic Communication.

I. INTRODUCTION

The industrial sector is experiencing a major digital shift, driven by Industry 4.0 principles that use interconnected cyber-physical systems for flexible manufacturing, remote operations, and predictive maintenance [2]. The key enabler of this shift is implementing secure, scalable, and deterministic connectivity for Industrial IoT (IIoT). Traditional communication technologies, like enterprise Wi-Fi, often struggle to meet the diverse needs of this environment, which includes large sensor networks requiring high device density (mMTC) and mission-critical control loops needing Ultra-Reliable Low-Latency Communication (URLLC) [3].

Manufacturing facilities require guaranteed Quality of Service (QoS), highly predictable performance (low jitter), and clear data sovereignty; none of which can be reliably provided by traditional shared public wireless infrastructure due to network contention and interference [1]. Private 5G/LTE Non-Public Networks (NPNs) offer a dedicated architectural solution. By providing dedicated radio resources, localized core processing, and carrier-grade reliability, NPNs are uniquely suited to enable the next generation of industrial automation. The inherent security features, such as SIM-based identities and robust segmentation through slicing, further meet the strict security requirements of Operational Technology (OT) networks [4].

This paper details the necessary architectural framework and deployment strategy for successfully integrating private cellular networks into IIoT environments.

The key contributions of this paper are summarized as follows:

1. Comprehensive Architectural Framework: A strong Private Wireless Reference Architecture is introduced, including a 5G Standalone (SA) Core, Mobile Edge Computing (MEC), and a specialized 5G-TSN bridging function, explicitly meeting the strict latency and reliability needs of URLLC traffic.
2. Deployment and Integration Methodology: Best practices are examined for deployment, emphasizing effective spectrum management (e.g., CBRS), specialized RF planning techniques needed for challenging

environments, and the essential integration layer between 5G cellular protocols and existing industrial OT standards (e.g., EtherCAT/PROFINET) [5].

II. USE CASES AND REQUIREMENTS FOR IIOT

Successful deployment requires accurate mapping of industrial processes onto the performance profiles defined by 3GPP. The main factors driving private wireless adoption come from three interconnected industrial scenarios [4]:

A. Industrial Scenarios Driving Private Wireless Adoption

Automation and Robotics: This category covers applications needing strict URLLC capabilities. These include controlling Automated Guided Vehicles (AGVs) and Autonomous Mobile Robots (AMRs), collaborative robots (cobots), and remote operations of heavy machinery at ports or mines. As an example, AGV logistics fleets rely on strong, low-latency connectivity for navigation updates and safety protocols, often aiming for latency below 10ms.

Massive Sensor Deployment**:** Large-scale condition monitoring, predictive maintenance, and asset-tracking systems utilize Massive Machine-Type Communication (mMTC). These applications require supporting extremely high device densities, often exceeding 1,000 devices per square km, while emphasizing long battery life and extensive coverage [3].

High-Bandwidth Applications**:** Enhanced Mobile Broadband (eMBB) is essential for applications that require high data rates, such as 4K/8K video streaming for centralized operational oversight, AI-driven video analytics, and Augmented Reality (AR) instructions used by technicians for complex maintenance procedures [1].

B. Key Performance Indicators (KPIs) and Service Demands

The requirements for industrial applications far exceed typical expectations for mobile broadband. The most important KPIs are latency, reliability, and jitter.

Table 1: IIoT Requirements mapped to corresponding 5G profile

KPI	Typical IIoT Requirement	5G Profile
End-to-End Latency	1 ms to 10 ms (Target 4 ms)	URLLC
Reliability	99.999% to 99.9999% (1 error in 10^5-10^6 packets)	URLLC
Jitter	< 1 s (Crucial for synchronization)	URLLC, TSN
Device Density	> 1000 devices/km^2	mMTC

C. SLA and Determinism Considerations

In industrial control systems (OT), delivering consistently, predictable latency (low jitter) is often more critical than achieving the absolute lowest latency [3]. Reliable performance is maintained through dedicated resources and tailored network policies.

This requires that Private 5G networks effectively support a variety of profiles. For example, an AGV typically uses an mMTC profile for routine updates but needs an immediate switch to URLLC capabilities for emergency stops or real-time obstacle avoidance. This integration means static traffic separation is not enough; true industrial flexibility demands dynamic, detailed resource allocation managed through strict QoS mapping [6]. Service Level Agreements (SLAs) must ensure that the 5G system aligns strict industrial timing needs (such as EtherCAT protocol cycle times) with the 5G QoS Identifier (5QI) framework, utilizing network slicing for precise traffic segmentation [6].

III. ARCHITECTURE AND TECHNOLOGIES

Implementing Private 5G for IIoT needs a dedicated, localized architecture that brings network intelligence and computing resources as close to endpoint devices as possible.

A. Proposed Reference Architecture for Private Wireless + Edge

The optimal architecture uses a 5G Standalone (SA) Non-Public Network (NPN) integrated with Mobile Edge Computing (MEC). The structure must isolate user-plane traffic locally to reduce transport delays.

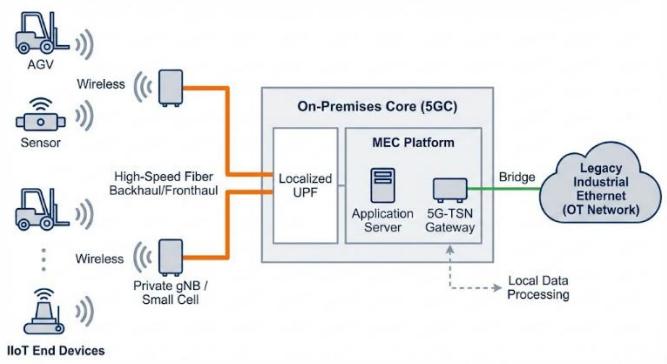

Figure 1: Private 5G/MEC Reference Architecture for IIoT

B. RAN Options and Deployment

Private networks use small-cell deployments for dense indoor coverage, often adopting open-standard approaches like O-RAN (which separates Radio Units and Baseband Units) to improve flexibility and scalability. To meet URLLC requirements, the RAN must support adaptable numerology and short Transmission Time Intervals (TTIs) as specified in 3GPP Releases 15 and 16 [1].

Spectrum availability is a key factor. In the USA, shared bands like CBRS (3.5 GHz) are often preferred because they help lower the Total Cost of Ownership (TCO), making Private 5G more accessible [7]. Enterprises usually choose between General Authorized Access (GAA) for quick, free access or bidding for Priority Access Licenses (PALs) through the FCC to secure dedicated spectral resources and ensure consistent performance [7].

C. Core (5GC) and Mobile Edge Computing (MEC)

Using a Standalone (SA) 5G Core with a low footprint 5G Core (5GC) is essential for achieving the lowest latency and simplifying network management, especially when compared to Non-Standalone (NSA) architectures [8]. The core must be hosted on-premises or located close to the NPN architecture.

The physical proximity of the User Plane Function (UPF) and the MEC platform is a vital architectural requirement for URLLC. Achieving an end-to-end latency of 4 ms requires that the UPF and MEC be collocated to avoid the significant transport delay associated with centralized cloud processing [3]. This allows computational offloading from endpoint devices, which are limited in battery life and processing power, to occur with minimal delay [3]. These virtualized network functions (NFVI) are hosted on specialized, ruggedized edge servers built for industrial settings [8].

D. Determinism, Time Synchronization, and QoS

The integration of Time-Sensitive Networking (TSN) is the key technological foundation that enables deterministic communication in 5G [1]. 3GPP Release 16 standardized features that allow the 5G system to function as a logical TSN bridge [1]. This integration depends on several mechanisms:

1. Precision Timing: Synchronization is achieved using the generalized Precision Timing Protocol (PTP), aligning the 5G internal timing mechanisms (such as IEEE 1588v2) with the external OT

environment [9].
2. Traffic Mapping: TSN traffic configurations, which define flow characteristics, are accurately integrated into the 5G QoS framework.
3. Network Slicing: This feature is crucial for strictly isolating mission-critical control traffic (URLLC slice) from non-critical data (eMBB/mMTC slices) to meet different latency and reliability requirements at the same time. Techniques like Network Slicing allow detailed prioritization and policy enforcement for specific tasks, such as video surveillance or AI processing [10].

IV. DEPLOYMENT CONSIDERATIONS AND BEST PRACTICES

Deploying a private cellular network in a production environment requires methodologies that account for the unique features of industrial sites, which differ significantly from typical commercial wireless deployments.

A. Site Survey and RF Planning

Industrial environments, such as factory floors, feature dense machinery, highly reflective metallic surfaces, and dynamic equipment movement (e.g., AGVs), which together generate significant shadowing, intense multipath interference, and time-varying channel conditions [11].

RF planning must be comprehensive, going beyond basic capacity-driven coverage models. Surveys should include proactive interference detection, physical-layer acceptance testing, and ray-tracing models optimized for industrial materials. For IIoT, the focus shifts from maximizing spectral efficiency to enhancing coverage reliability and ensuring seamless handovers throughout the facility [1]. This often involves an architectural choice that favors redundancy, such as densifying antenna units in critical operational areas, to ensure strong signal strength and prevent connectivity issues for safety-critical mobile assets like AGVs [11].

Besides connectivity, deployment must focus on site safety. This involves setting Electromagnetic Field (EMF) limits, implementing cable segregation, ensuring proper grounding, and identifying necessary guard bands or potentially hazardous No-RF/ATEX zones. [10].

B. Integration with OT Stacks and Industrial Protocols

The main challenge in integrating 5G into a brownfield industrial setting is connecting the IP-based cellular system to highly deterministic Layer 2 industrial Ethernet protocols such as PROFINET, Modbus, and EtherCAT. These protocols are essential to existing control systems.

Specialized protocol conversion gateways are essential for translating industrial data structures and timing mechanisms into the 5G transport layer [7]. For high-end applications, especially motion control, EtherCAT is recognized as a leading industrial standard, offering nanosecond-level synchronization and high determinism. The 5G TSN bridging function (discussed in Section III) must meet this strict timing requirement, making the design and security of the integration gateway critical [5].

C. Security and Lifecycle Management

Private 5G inherently improves security through unique Subscriber Identity Modules (SIMs) for device authentication and network slicing for better segmentation. This foundation is used to implement a comprehensive Zero Trust security architecture [12].

In a Zero Trust model, continuous verification and risk-based access control are enforced, often closer to the devices through edge computing, thereby reducing reliance on centralized infrastructure [12]. This lessens the risk of unauthorized lateral movement within the network. Security frameworks must align with 3GPP standards and best industrial practices, such as the IEC 62443 series, which provides functional and procedural requirements for Industrial Automation and Control Systems (IACS) [4].

From an operations perspective, deployment should proceed cautiously, progressing from a successful pilot phase to a gradual scale-up. Ongoing monitoring, strong fault tolerance, and non-disruptive update procedures are crucial to maintaining the high availability required by production-critical systems.

V. CONCLUSION

Private 5G/LTE networks, especially those using 5G NR URLLC features and deploying localized Mobile Edge Computing architecture, serve as the ultimate communication platform for advanced Industry 4.0 implementations. This dedicated infrastructure effectively addresses performance constraints and contention issues in shared wireless technologies, delivering proven, significant improvements in operational reliability and deterministic latency.

While deployment involves strategic decisions about spectrum (e.g., CBRS - PAL vs. GAA), precise RF planning focused on coverage reliability, and careful integration of TSN gateways to ensure OT protocol compatibility, the resulting platform provides unmatched safety, efficiency, and scalability for IIoT applications.

REFERENCES:

1. P. Varga et al., "5G support for Industrial IoT Applications— Challenges, Solutions, and Research gaps," Sensors, vol. 20, no. 3, p. 828, 2020. doi: 10.3390/s20030828.
2. Intelligent Visibility, "Private 5G & LTE Use Cases | Industry Applications." [Online]. Available: [https://intelligentvisibility.com/campus-networking/private-wireless/enterprise-use-cases].
3. A1 Digital, "5G and IoT: New opportunities for companies." [Online]. Available: [https://www.a1.digital/knowledge-hub/5g-and-iot-new-opportunities-for-companies/].
4. 5G-ACIA, Security Aspects of 5G for Industrial Networks. Position Paper, 2021. [Online]. Available: [https://www.5g-acia.org/wp-content/uploads/2021/05/5G-ACIA_Security_Aspects_of_5G_for_Industrial_Networks_single-pages.pdf].
5. Uctel, "How to deploy private 5G in industrial sites?" [Online]. Available: [https://www.uctel.co.uk/blog/how-to-deploy-private-5g-in-industrial-sites].
6. Arendt et al., "Towards Future Industrial Connectivity: Evaluation of Private 5G and Wi-Fi Networks in Professional Industrial Environments," in Proc. 2025 IEEE 21st Int. Conf. on Factory Communication Systems (WFCS), Rostock, Germany, 2025.
7. Federal Communications Commission (FCC), "3.5 GHz Band Overview." [Online]. Available: [https://www.fcc.gov/wireless/bureau-divisions/mobility-division/35-ghz-band/35-ghz-band-overview].
8. Advantech, Solution Brief: 5G Edge Servers for the Open RAN. Private 5G Networks for Industrial IoT, 2024. [Online]. Available: [https://campaign.advantech.online/en/Cloud-IoT/DOC/SolutionBrief/Advantech-5G-Edge-Servers-for-the-Open-RAN.pdf].
9. Comba Telecom, A Practice of TSN over 5G for Industry. White Paper, 2020. [Online]. Available: [https://www.comba-ctnsl.com/wp-content/uploads/White-Paper_A-Practice-of-TSN-over-5G-for-Industry_final.pdf].
10. M. E. Haque, F. Tariq, M. S. Hossain et al., "A Comprehensive Survey of 5G URLLC and Challenges in the 6G Era," arXiv, 2025. [Online]. Available: [https://arxiv.org/abs/2508.20205].
11. C.-P. Li, J. Jiang, W. Chen, T. Ji, and J. Smee, "5G Ultra-Reliable and Low-Latency Systems Design," in Proc. 2017 European Conf. on Networks and Communications (EuCNC), Oulu, Finland, 2017, pp. 1–5. doi: $10.1109/EuCNC.2017.7980747$.
12. Device Authority, "Zero Trust IoT Security: Implementation Guide for Enterprise Networks." [Online]. Available: [https://deviceauthority.com/zero-trust-iot-security-implementation-guide-for-enterprise-networks/].