Mission-Critical Private 5G Network Planning: A Comprehensive Framework for Coverage, Capacity, and Deterministic Quality of Service (QoS)

Rahul Bangera

Ellicott City, MD, USA.
rahulmbangera@gmail.com

Abstract:
The deployment of Private 5G networks for mission-critical industrial applications demands a fundamental shift from best-effort cellular planning to a deterministic, reliability-focused design. This paper presents a rigorous engineering framework for constructing Standalone Non-Public Networks (SNPN) capable of supporting Industry 4.0 use cases, such as isochronous motion control and high-density machine vision. We analyze the key trade-offs between spectral efficiency and latency and propose a dimensioning method that emphasizes uplink-heavy Time Division Duplex (TDD) frame structures (e.g., DSUUU) to achieve gigabit-class uplink capacity. Additionally, we detail the physical-layer planning required for high reliability in cluttered Indoor Factory (InF-DH) environments. The integration of Time-Sensitive Networking (TSN) is discussed through the IEEE 802.1AS transparency model and accurate Quality of Service (QoS) mapping strategies. Finally, we recommend a Zero-Trust security architecture utilizing Subscription Concealed Identifiers (SUCI) and secondary authentication to enhance the industrial edge.

Keywords: Private 5G, Non-Public Networks (NPN), URLLC, Time-Sensitive Networking (TSN), Network Dimensioning, TDD Frame Structure, Industrial IoT, 5G Security, Channel Modeling.

I. INTRODUCTION

The industrial sector's shift to Cyber-Physical Systems (CPS) increases demand for wireless connectivity that provides the same level of determinism as wired fieldbuses. While public 5G networks aim to optimize downlink throughput and coverage, mission-critical private networks must ensure bounded latency (often under 10 ms) and ultra-high reliability (above 99.999%) for applications ranging from autonomous mobile robots (AMRs) to closed-loop process automation [1] [2].

Designing these networks involves managing a complex mix of radio-frequency (RF) physics, protocol overheads, and architectural choices. Standard macro-cellular planning tools, designed for outdoor urban environments and downlink-focused traffic, are not suitable for the reflective, metallic environments of a factory floor where uplink traffic from video sensors often dominates [3]. Additionally, the requirement for microsecond-level synchronization via Time-Sensitive Networking (TSN) imposes strict limits on residence time variation within the 5G system [4]. This paper presents a comprehensive planning framework for industrial Private 5G. We carefully analyze architectural preferences for Standalone NPNs (SNPN), the mathematical dimensioning of uplink-focused radio resources, and the security mechanisms needed to protect critical infrastructure.

II. ARCHITECTURAL STRATEGY FOR DETERMINISM

The selection of deployment architecture determines the network's isolation, survivability, and control. For industries with mission-critical needs, the Standalone Non-Public Network (SNPN) model is the essential baseline.

A. SNPN vs. Public Network Integration

3GPP Technical Specification (TS) 23.501 defines SNPN as a network that operates independently of Public Land Mobile Networks (PLMN) [5].

- Isolation: SNPNs use a unique Network Identifier (NID) combined with a private PLMN ID, preventing signaling storms or core network outages in the national carrier network from affecting the factory floor.
- Data Sovereignty: In an SNPN, the 5G Core (5GC) is hosted on-site. User plane traffic flows directly from the gNodeB to a local User Plane Function (UPF) and then to the Operational Technology (OT) network, ensuring that sensitive production data never travels over public backhaul or cloud infrastructure [6].

B. High Availability Design

To guarantee industrial-grade availability, the architecture must eliminate single points of failure.

- Control Plane: Deploying stateless Access and Mobility Management Functions (AMF) in an N+1 redundancy cluster ensures seamless failover.
- User Plane: The UPF, which often uses stateful packet inspection, requires a 1:1 hot-standby configuration for mission-critical deployments. 3GPP Release 16 introduces redundant PDU sessions, allowing a User Equipment (UE) to establish two separate paths through disjoint RAN and UPF resources, mirroring the redundancy of IEC 62439-3 Parallel Redundancy Protocol (PRP) [5] [7].

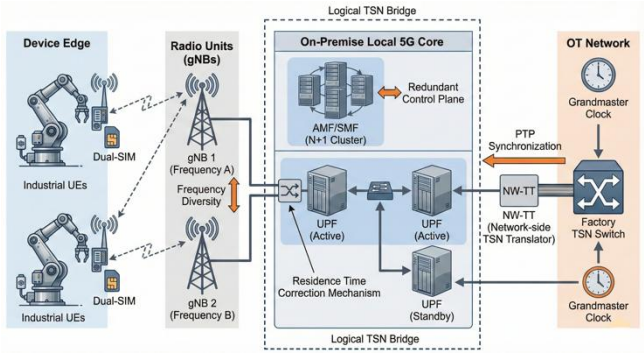

Figure 1: Proposed Private 5G SNPN Architecture with TSN Integration.

III. RADIO RESOURCE DIMENSIONING

Industrial traffic profiles are usually uplink-heavy, mainly due to use cases like machine vision cameras (10–50 Mbps per stream) and large sensor telemetry. This reverses the typical 10:1 downlink-to-uplink ratio seen in consumer networks.

A. TDD Frame Structure Optimization

Standard 5G TDD patterns, like "DDDSU" (Downlink, Downlink, Downlink, Special, Uplink), significantly limit uplink capacity. For video-heavy industrial zones, planners need to use uplink-focused frame structures.

- Recommendation: A frame structure like DSUUU (Downlink, Special, Uplink, Uplink, Uplink) with a 2.5 ms periodicity significantly increases the uplink duty cycle [3] [8].
- Throughput Impact: As shown in Table 1, switching from a standard carrier setup to an uplink-optimized pattern can nearly quadruple the total uplink cell throughput, allowing support for dozens of simultaneous 4K video streams.

Table 1: Theoretical Peak Uplink Throughput Comparison (100 MHz, 30 kHz SCS, 2x2 MIMO) [3] [9]

Frame Structure	Periodicity	UL Duty Cycle	Peak UL Throughput (Approx.)	Suitability
DDDSU (Standard)	2.5 ms	~20%	~350 Mbps	eMBB / Tablets
DDSUU (Balanced)	2.5 ms	~40%	~700 Mbps	General IIoT
DSUUU (UL Heavy)	2.5 ms	~60%	~1.1 Gbps	Machine Vision

Note: Calculations assume 256-QAM and standard overheads.

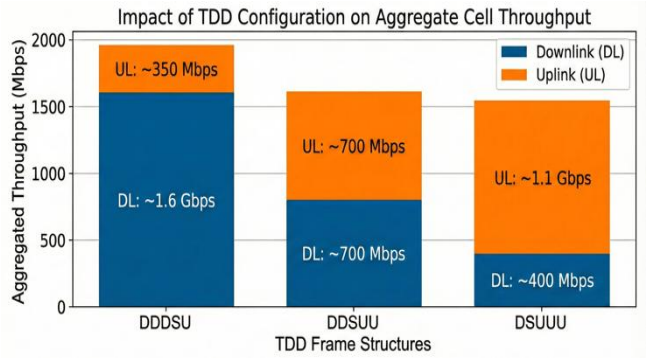

Figure 2: Impact of TDD Configuration on Aggregate Cell Throughput.

IV. RELIABILITY-CENTRIC COVERAGE PLANNING

In mission-critical planning, coverage is defined not by average signal strength (RSRP) but by the reliability margin needed to ensure packet delivery at the cell edge during deep fading events.

A. Industrial Channel Models (InF-DH)

Factories are "rich multipath" environments due to heavy metallic clutter. 3GPP TR 38.901 defines the Indoor Factory - Dense High (InF-DH) channel model to capture these effects [10].

- Shadow Fading: The 3GPP TR 38.901 InF-DH channel model exhibits a shadow fading standard deviation (σSF) of 4.0 dB for Line-of-Sight (LOS) and 6.0 dB for Non-Line-of-Sight (NLOS) conditions. In scenarios with lower base station heights (InF-DL), this NLOS variance increases to 8.0 dB, significantly surpassing typical office environment levels [10].
- Path Loss: The path-loss exponent is generally lower than in free space ($n < 2$) due to waveguide effects in aisles, but obstruction losses are severe [11].

V. DETERMINISTIC TRANSPORT & QoS DESIGN

To support protocols such as PROFINET or EtherCAT, the 5G system must operate as a transparent, low-jitter Ethernet bridge [12].

A. TSN Integration (IEEE 802.1AS)

3GPP Release 16 introduced the 5G System (5GS) as a logical bridge.

- Translators: The Network-side TSN Translator (NW-TT) at the UPF and the Device-side TSN Translator (DS-TT) at the UE function as ingress and egress ports [5].
- Synchronization: The system supports IEEE 802.1AS (gPTP). The TTs calculate the residence time (the time spent traversing the radio and core) and add it to the PTP correction field [4] [13]. This enables industrial controllers to synchronize their clocks across the wireless link with sub-microsecond accuracy (< 900 ns time error budget) [4].

B. QoS Mapping Strategy

Determinism requires strict prioritization. Control traffic must never be queued behind video data. This is enforced by mapping Ethernet Priority Code Points (PCP) to 5G QoS Identifiers (5QI) [7].

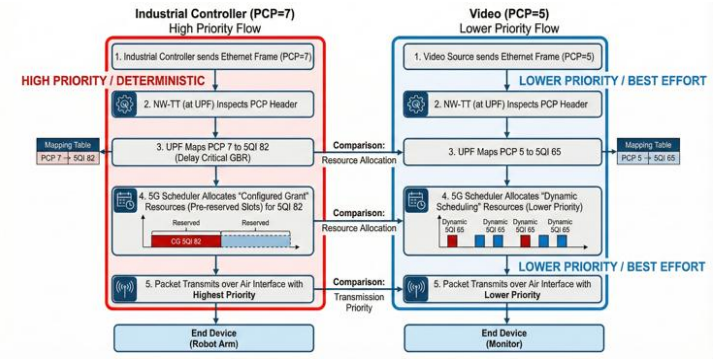

Figure 3: Comparing QoS Mapping and Traffic Flow for a high-priority Industrial Controller and a lower-priority video transmission

Table 2: Recommended QoS Mapping for Industrial Automation [5] [7]

Traffic Class	Ethernet PCP	5G 5QI	Resource Type	Target PDB / PER
Motion Control	7 (Highest)	82	Delay Critical GBR	10 ms / 10^(-5)
Safety Interlock	6	83	Delay Critical GBR	10 ms / 10^(-4)
Video (Real-time)	5	67	GBR	75 ms / 10^(-3)
Best Effort (Logs)	0 (Default)	9	Non-GBR	300 ms / 10^(-6)

For delay-critical flows such as 5QI 82-85, the scheduler typically employs Configured Grants (also known as grant-free transmission) to pre-allocate uplink resources. This mechanism eliminates the scheduling request latency loop, ensuring the strict Packet Delay Budget (PDB) is met [14].

VI. SECURITY & IDENTITY

Security in Private 5G isn't just about encryption; it focuses on strict access control and identity protection within a Zero-Trust environment [15].

A. Subscriber Privacy (SUCI)

To prevent 'IMSI Catcher' attacks (rogue base stations) from tracking critical assets, 5G introduces the Subscription Concealed Identifier (SUCI) as defined in 3GPP TS 33.501 [15].

- Mechanism: The UE encrypts its permanent identifier (SUPI) using the Home Network Public Key stored on the USIM before transmission. Only the SIDF (Subscription Identifier De-Concealing Function) in the local UDM can decrypt it [16] [17].
- Requirement: Planners must ensure USIMs are provisioned with non-null protection schemes (e.g., ECIES Profile B) to enforce this protection [18].

B. Secondary Authentication

While primary authentication (5G-AKA) verifies the SIM, it does not confirm the device's authorization to access specific industrial VLANs [19].

- EAP-TLS: 3GPP standards support secondary authentication via EAP-TLS to secure industrial connections [16]. In this setup, the Session Management Function (SMF) transmits credentials between the device and an enterprise AAA server (e.g., RADIUS). This mechanism links connectivity to a specific digital certificate, preventing a stolen SIM card from being used to access the OT network from an unauthorized device [20].

VII. CONCLUSION

Designing private 5G networks for mission-critical industries requires a comprehensive engineering approach that extends beyond traditional cellular planning. Meeting the strict demands of Industry 4.0 involves adopting the SNPN architecture for isolation, using uplink-focused TDD frame structures (such as DSUUU) for capacity, and implementing detailed InF-DH channel modeling for coverage. Additionally, integrating TSN and Secondary Authentication transforms the network from a simple data pipe into a deterministic, secure component of the industrial control system.

REFERENCES:

1. M. Wen, Q. Li, K. J. Kim, D. López-Pérez, O. A. Dobre, H. V. Poor, P. Popovski, and T. A. Tsiftsis, "Private 5G Networks: Concepts, Architectures, and Research Landscape," *IEEE Journal of Selected Topics in Signal Processing*, vol. 16, no. 1, pp. 7–25, Jan. 2022.

2. X. Jiang, M. Luvisotto, Z. Pang, and C. Fischione, "Latency Performance of 5G New Radio for Critical Industrial Control Systems," in *2019 24th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*, Zaragoza, Spain, 2019, pp. 1135–1142.
3. NGMN Alliance, "5G TDD Uplink," NGMN, Frankfurt, Germany, White Paper v1.0, Dec. 2021.
4. 5G-ACIA, "Integration of 5G with Time-Sensitive Networking for Industrial Communications," 5G Alliance for Connected Industries and Automation (5G-ACIA), Frankfurt, Germany, White Paper, 2021.
5. *System Architecture for the 5G System (5GS), 3GPP TS 23.501, Release 16, V16.6.0, 3rd Generation Partnership Project (3GPP), Oct. 2020. [Online]. Available: [https://www.3gpp.org/specs].*
6. *5G-ACIA, "5G Non-Public Networks for Industrial Scenarios," 5G Alliance for Connected Industries and Automation (5G-ACIA), Frankfurt, Germany, White Paper, Jul. 2019.*
7. 5G-ACIA, "Integration of Industrial Ethernet Networks with 5G Networks," 5G Alliance for Connected Industries and Automation (5G-ACIA), Frankfurt, Germany, White Paper, Nov. 2019.
8. MediaTek, "5G Uplink Enhancement Techniques," MediaTek Inc., Hsinchu, Taiwan, White Paper, Sep. 2021
9. 5G-Tools, "5G NR Throughput Calculator," *5G-Tools.com*. [Online]. Available: [https://5g-tools.com/5g-nr-throughput-calculator/].
10. *Study on channel model for frequencies from 0.5 to 100 GHz*, 3GPP TR 38.901, Release 16, V16.1.0, 3rd Generation Partnership Project (3GPP), Dec. 2019. [Online]. Available: [https://www.3gpp.org/specs].
11. E. Tanghe *et al.*, "The industrial indoor channel: Large-scale and temporal fading at 900, 2400, and 5200 MHz," *IEEE Transactions on Wireless Communications*, vol. 7, no. 7, pp. 2740–2751, Jul. 2008.
12. 5G-ACIA, "Integration of Industrial Ethernet Networks with 5G Networks," 5G Alliance for Connected Industries and Automation (5G-ACIA), Frankfurt, Germany, White Paper, Nov. 2019.
13. 5G Americas, "Understanding 5G & Time Critical Services," 5G Americas, Bellevue, WA, USA, White Paper, Aug. 2022.
14. H. H. M. Tam, H. D. Tuan, and D. T. Ngo, "Grant-Free Radio Access for URLLC: A Survey," *IEEE Access*, vol. 10, pp. 108629–108653, Oct. 2022.
15. N. F. Syed *et al.*, "Zero Trust Architecture (ZTA): A Comprehensive Survey," *IEEE Access*, vol. 10, pp. 57143–57179, 2022.
16. *Security architecture and procedures for 5G System*, 3GPP TS 33.501, Release 16, V16.5.0, 3rd Generation Partnership Project (3GPP), Dec. 2020. [Online]. Available: [https://www.3gpp.org/specs].
17. M. Bartock *et al.*, "5G Cybersecurity: Volume B - Approach, Architecture, and Security Characteristics," National Institute of Standards and Technology (NIST), Gaithersburg, MD, USA, NIST SP 1800-33B, Oct. 2022.
18. *Security architecture and procedures for 5G System*, 3GPP TS 33.501, Release 16, V16.6.0, 3rd Generation Partnership Project (3GPP), Mar. 2021, Annex C. [Online]. Available: [https://www.3gpp.org/specs].
19. 5G-ACIA, "Security Aspects of 5G for Industrial Networks," 5G Alliance for Connected Industries and Automation (5G-ACIA), Frankfurt, Germany, White Paper, Nov. 2020.
20. M. Bartock *et al.*, "5G Network Security Design Principles: Applying 5G Cybersecurity and Privacy Capabilities," National Institute of Standards and Technology (NIST), Gaithersburg, MD, USA, Cybersecurity White Paper CSWP 36E (Draft), Jun. 2025. [Online]. Available: [https://csrc.nist.gov/pubs/cswp/36/e/5g-network-security-design-principles/ipd].