INTERNATIONAL JOURNAL OF SCIENTIFIC RESEARCH IN ENGINEERING AND MANAGEMENT (IJSREM)
VOLUME: 09 ISSUE: 05 | MAY-2025 SJIF RATING: 8.586 ISSN: 2582-3930

Private 5G Deployment Challenges in Oil & Gas: Architecture, Propagation, and OT Integration

Rahul Bangera, Ellicott City, MD, USA.
Email: rahulmbangera@gmail.com

***Abstract*— The global energy sector is experiencing a digital transformation, often called "Oil and Gas 4.0," where operational efficiency and safety rely heavily on dependable wireless connectivity. Private 5G, or Non-Public Networks (NPNs), offers a predictable alternative to traditional Wi-Fi for critical tasks such as autonomous drilling and remote inspections. However, deploying 5G New Radio (NR) in the oil and gas industry presents unique engineering challenges, particularly in dense, metallic environments, including RF propagation issues, spectrum regulatory complexities, and the integration of Layer 2 industrial protocols with Layer 3 cellular networks. This paper provides a technical analysis of these challenges and compares the effectiveness of Standalone NPN (SNPN) and Public Network Integrated NPN (PNI-NPN) architectures. It explores RF scattering in refineries, shared-spectrum management (CBRS), and cybersecurity concerns arising from blending IT and OT domains under IEC 62443. The findings suggest that successful deployment demands a fundamental shift in network design, with a focus on uplink capacity and precise channel modeling rather than traditional downlink-centric planning.**

Keywords: Private 5G, Non-Public Networks (NPN), Industrial IoT, Oil & Gas, RF Propagation, Operational Technology (OT), IEC 62443, Spectrum Management.

I. INTRODUCTION

The oil and gas industry operates in some of the most physically demanding and economically volatile environments on Earth. Operators face increasing pressure to reduce Operational Expenditures (OPEX) and improve worker safety. Digitalization efforts, such as "Digital Twins" and predictive maintenance sensors, are essential tools to achieve these goals [1]. However, these technologies require connectivity with strict reliability and low latency, which legacy infrastructure often cannot support.

Historically, connectivity in oil and gas facilities has been fragmented. Wired options like Industrial Ethernet (PROFINET, EtherNet/IP) offer reliability but limit asset flexibility. Wireless solutions such as Wi-Fi (IEEE 802.11) encounter inherent challenges in industrial environments, including interference in unlicensed bands and "break-before-make" handovers that disrupt moving assets [2].

Private 5G addresses these issues by providing a cellular-grade architecture specially designed for industrial applications. 3GPP Release 16 and 17 introduced features targeting the Industrial Internet of Things (IIoT), such as Ultra-Reliable Low-Latency Communication (URLLC) and Time Sensitive Networking (TSN) [3]. Despite these benefits, shifting to Private 5G is a complex architectural transition that involves spectrum management, RF propagation modeling, and OT protocol integration. This paper discusses these challenges and offers architectural recommendations for the industry.

II. ARCHITECTURAL OPTIONS FOR NON-PUBLIC NETWORKS (NPN)

3GPP standards define "Non-Public Networks" (NPNs) to differentiate private cellular deployments from public mobile networks. For the O&G sector, choosing the right architecture determines the network's security, resilience, and operational control.

A. Standalone Non-Public Networks (SNPN)

An SNPN is a fully isolated network where both the Radio Access Network (RAN) and the 5G Core (5GC) are deployed locally. This architecture is effectively "air-gapped" from public Mobile Network Operator (MNO) infrastructure [4]. For critical assets such as offshore platforms, the SNPN model is preferred for its resilience and data sovereignty. User plane traffic never leaves the facility, ensuring proprietary process control data remains within the operator's physical control. This isolation also ensures that local operations, such as autonomous drilling control, continue uninterrupted even if the satellite backhaul to the mainland is severed [5].

B. Public Network Integrated NPN (PNI-NPN)

In a PNI-NPN model, the enterprise shares specific network resources with a public MNO. A common implementation is the Control and User Plane Separation (CUPS) model, where the User Plane Function (UPF) is deployed locally for low latency, but the Control Plane remains in the MNO's cloud [4]. This model reduces Capital Expenditure (CAPEX) and is beneficial for onshore logistics where vehicles must move seamlessly between the private facility and public roads. However, reliance on an external control plane presents a risk: if the link to the MNO is lost, new sessions cannot be established, which may be unacceptable for safety-critical systems.

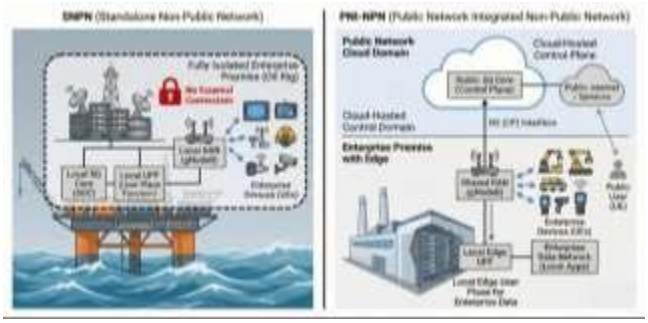

Figure 1: Architecture comparison between SNPN and PNI-NPN.

III. SPECTRUM REGULATION AND MANAGEMENT

Securing access to the radio frequency spectrum is a prerequisite for Private 5G. Unlike Wi-Fi, 5G spectrum is regulated to prevent interference, and regulations differ around the world.

A. The CBRS Framework (United States)

In the U.S., the Citizens Broadband Radio Service (CBRS) band (3.55–3.70 GHz) supports private 5G through a three-tier sharing system managed by a Spectrum Access System (SAS) [6]:

1. Incumbent Access: Reserved for US Navy radar and satellites.
2. Priority Access License (PAL): Auctioned licenses offering interference protection.
3. General Authorized Access (GAA): Open access, coordinated by SAS to minimize interference.

Challenges in O&G:

- Power Limits: CBRS limits outdoor (Category B) device power to 47 dBm/10 MHz [6]. While this is substantial, it is lower than macro-cell power, which may require higher tower density for extensive onshore oil fields.
- SAS Dependency: Radios must periodically connect to the cloud-based SAS. In remote fields with inconsistent internet, this increases the reliability risk. Backup internet solutions providing connectivity to the SAS are often needed to buffer this connection and keep uptime during the primary internet backhaul outages [7].

B. Global Industrial Spectrum

Outside the US, many regions adopt a "verticals" model, reserving specific bands for certain industries. For example, Germany allocates 3.7–3.8 GHz for campus networks [8]. In the North Sea, offshore operators like Tampnet use dedicated frequency bands (e.g., 700 MHz for wide-area coverage, 2.6 GHz for capacity) licensed from shelf states (Norway/UK) to establish basin-wide coverage [9].

Table 1: Comparative Analysis of Spectrum Options for O&G [6] [8]

Feature	Licensed (MNO Sub-lease)	Shared (CBRS - USA)	Local/Vertical Licensing (e.g., Germany)
Reliability	High (Protected)	Medium (GAA) to High (PAL)	High (Exclusive usage)
Cost Model	OPEX (Lease fees)	Low (GAA is minimal OPEX) / CAPEX (PAL)	Low regulatory fees
Power Limits	High (Macro levels)	Medium (47 dBm max)	High (Regulator defined)
Deployment	Dependent on MNO	Enterprise controlled	Enterprise controlled
Suitability	Onshore logistics, roaming	Refineries, plants (US only)	Critical process control

IV. RF PROPAGATION IN "HEAVY METAL" ENVIRONMENTS

A major challenge in oil and gas (O&G) is the physical propagation environment. Refineries and platforms are known as "heavy metal" environments because of the dense steel pipe racks, distillation columns, and vessels.

A. Multipath Fading and Delay Spread

In these environments, signals interact with metallic structures through reflection and diffraction, creating a complex multipath environment. Studies in industrial settings measure Root Mean Square (RMS) delay spreads up to three times higher than in typical enterprise environments [10]. Excessive delay spread can surpass the Cyclic Prefix (CP) of the 5G OFDM symbol, leading to Inter-Symbol Interference (ISI) and reduced throughput.

Mitigation: Network planners need to optimize the Subcarrier Spacing (SCS). While a wider SCS (e.g., 30 kHz) decreases latency, it also shortens the CP symbol duration. Finding the right balance is crucial, often favoring 15 kHz or 30 kHz with robust channel coding. Using directional antennas at the user equipment (UE) side can also help spatially filter multipath components [11].

B. The Faraday Cage Effect and Coverage Densification

Dense pipe racks act as nested Faraday cages, preventing RF signals from passing through. This creates deep shadow zones where coverage drops sharply. As a result, O&G facilities require a much higher density of Small Cells than logistics warehouses. 5G networks in refineries are often limited by interference rather than noise, requiring careful inter-cell interference coordination [12].

Figure 2: Mitigation strategy by using a "mesh" of small cells to fill coverage gaps.

V. INTEGRATING INDUSTRIAL OPERATIONAL TECHNOLOGY (OT)

The primary advantage of Private 5G is its ability to transfer data from Industrial Control Systems (ICS). However, a fundamental mismatch exists between OT protocols and cellular infrastructure.

A. The Layer 2 vs. Layer 3 Mismatch

5G is fundamentally a Layer 3 (IP-based) technology. However, mission-critical automation protocols such as PROFINET (RT/IRT) and EtherNet/IP often rely on Layer 2 (MAC) communication and broadcast mechanisms for device discovery [13]. A standard 5G connection blocks these frames from being transmitted.

Solution: Layer 2 Tunneling. To support these protocols, the 5G system must implement "Ethernet PDU Sessions" or Layer 2 tunneling (such as VXLAN or GRE). The 5G User Equipment (UE) encapsulates the raw industrial Ethernet frame inside an IP packet. This packet travels through the 5G core to the UPF, where it is decapsulated and handed to the controller, effectively creating a "virtual wire" [14].

B. Time Sensitive Networking (TSN)

For closed-loop control, standard Ethernet causes unacceptable jitter. 3GPP Release 16 added TSN support, allowing the 5G system to synchronize with the industrial "Grandmaster Clock" (IEEE 802.1AS). The 5G scheduler then coordinates radio resource allocation with the deterministic cycle times of the automation system, reducing latency. Although effective, deploying TSN over 5G requires precise integration between the 5G Core's Translation functions (DS-TT/NW-TT) and the wired industrial network [3] [13].

VI. CYBERSECURITY AND DATA SOVEREIGNTY

Connecting critical infrastructure to a wireless network breaks the traditional "air gap," creating new threat vectors.

A. IEC 62443 Compliance

Security strategies must align with IEC 62443, the standard for industrial cybersecurity. The standard divides networks into "Zones" separated by "Conduits." A Private 5G network acts as a conduit. Network slicing enables the creation of isolated logical conduits; for example, a "Safety Slice" for emergency shutdown systems can be logically separated from a "Surveillance Slice" for CCTV, preventing a video bandwidth spike from congesting safety traffic [15].

B. Zero Trust and SIM Authentication

5G provides robust hardware-based security through the SIM (or eSIM), which is much harder to spoof than Wi-Fi credentials. Platforms like "OneLayer" offer visibility into these cellular devices, bridging the gap between the cellular core and IT security policies. This enables a Zero Trust model, in which each device (e.g., a connected pressure sensor) is authenticated and authorized before data exchange [16].

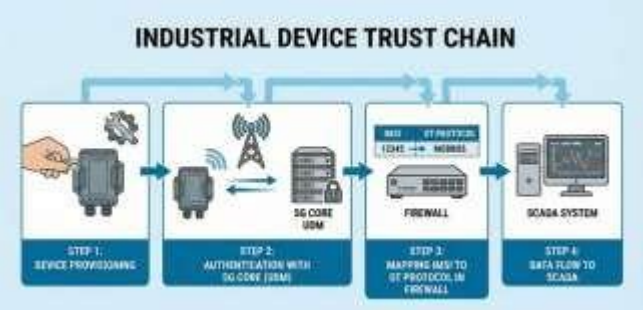

Figure 3: Onboarding and authentication of an industrial device on a private 5G network

VII. CONCLUSION

The deployment of Private 5G in the oil and gas industry marks an important step in its digital evolution. By addressing coverage and mobility challenges associated with Wi-Fi, 5G enables autonomous operations and the "Connected Worker." However, success depends on overcoming the industry's specific engineering hurdles. RF propagation physics in metal-rich environments requires dense, carefully planned radio networks. Integrating legacy OT protocols demands advanced Layer 2 tunneling and TSN features. Additionally, the security framework must blend cellular standards with IEC 62443 industrial safety requirements. As the ecosystem develops, Private 5G is expected to become the standard "digital nervous system" for modern energy sites, improving efficiency and safety in a more complex operational landscape.

REFERENCES

[1] H. S. Arpitha, K. R. Anand, and B. Gullapalli, "Digital Transformation of Oil & Gas Fields Architecting Multi-Services Digital Private Network on 5G NR-U Model," in *2022 IEEE Wireless Antenna and Microwave Symposium (WAMS)*, Rourkela, India, 2022, pp. 1–5, doi: 10.1109/WAMS54719.2022.9848382.

[2] O. Elijah *et al.*, "A Survey on Industry 4.0 for the Oil and Gas Industry: Upstream Sector," *IEEE Access*, vol. 9, pp. 144438–144468, 2021, doi: 10.1109/ACCESS.2021.3121302.

[3] J. Sasiain, D. Franco, A. Atutxa, J. Astorga, and E. Jacob, "Toward the Integration and Convergence Between 5G and TSN Technologies and Architectures for Industrial Communications: A Survey," *IEEE Commun. Surveys Tuts.*, vol. 27, no. 1, pp. 259–321, Feb. 2025, doi: 10.1109/COMST.2024.3422613.

[4] *5G-ACIA, "Non-Public Networks for Industrial Scenarios," 5G Alliance for Connected Industries and Automation, White Paper, 2021. [Online]. Available: [https://5g-acia.org/whitepapers/npns-for-industrial-scenarios/].*

[5] *K. Kousias et al., "Coverage and Performance Analysis of 5G Non-Standalone Deployments," in Proc. 16th ACM Workshop Wireless Netw. Testbeds, Exp. Eval. Characterization (WiNTECH), Sydney, Australia, Oct. 2022, pp. 61–68, doi: 10.1145/3556564.3558233.*

[6] OnGo Alliance, "CBRS Coexistence Technical Specifications," OnGo Alliance White Paper, Oct. 2024. [Online]. Available: [https://ongoalliance.org/wp-content/uploads/2024/10/GAA-Coexistence-Whitepaper-1.0.pdf].

[7] Verizon, "Study of CBRS and Licensed Spectrum for Dedicated Networks," Verizon White Paper, 2022. [Online].

Available: [https://www.verizon.com/business/resources/whitepapers/study-of-cbrs-and-licensed-spectrum-for-dedicated-networks.pdf].

[8] Rischke *et al.*, "5G Campus Networks: A First Measurement Study," *IEEE Access*, vol. 9, pp. 121786–121803, 2021, doi: 10.1109/ACCESS.2021.3108423.

[9] T-Mobile, Tampnet win 700MHz licences in Netherlands for off-shore 5G," *RCR Wireless News*, May 19, 2021. [Online]. Available: [https://www.rcrwireless.com/20210519/5g/t-mobile-tampnet-win-700mhz-licences-in-netherlands-for-off-shore-5g].

[10] S. S. K. C. *et al.*, "Sub-6 GHz Channel Modeling and Evaluation in Indoor Industrial Environments," in *2022 IEEE 96th Vehicular Technology Conference (VTC2022-Fall)*, London, United Kingdom, 2022, pp. 1–5, doi: 10.1109/VTC2022-Fall57202.2022.10012920.

[11] B. B. Cebecioglu *et al.*, "Experimental Analysis of 5G NR for Indoor Industrial Environments," *IEEE Access*, vol. 12, pp. 89311–89325, 2024, doi: 10.1109/ACCESS.2024.3417643.

[12] J. Senic *et al.*, "Challenges for 5G and Beyond," in *Proc. 16th Eur. Conf. Antennas Propag. (EuCAP)*, Madrid, Spain, Mar. 2022, pp. 1–5. [Online]. Available: [https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=933609].

[13] 5G-ACIA, "Integration of Industrial Ethernet Networks with 5G Networks," 5G Alliance for Connected Industries and Automation, White Paper, Nov. 2019. [Online]. Available: [https://5g-acia.org/wp-content/uploads/2021/04/5G-ACIA_Integration-of-Industrial-Ethernet-Networks-with-5G-Networks-.pdf].

[14] Celona, "Support for Real-Time Industrial Ethernet Protocols - PROFINET," *Celona Help Center*, 2023. [Online]. Available: [https://docs.celona.io/en/articles/8110556-support-for-real-time-industrial-ethernet-protocols-profinet].

[15] National Security Agency (NSA) and Cybersecurity and Infrastructure Security Agency (CISA), "5G Network Slicing: Security Considerations for Design, Deployment, and Maintenance," Enduring Security Framework (ESF), Guidance Document, Jul. 2023. [Online]. Available: https://www.cisa.gov/sites/default/files/2024-08/ESF_5G_NETWORK_SLICING-SECURITY_CONSIDERATIONS_FOR_DESIGN%2CDEPLOYMENT%2CAND_MAINTENANCE_FINAL_508.pdf].

[16] OneLayer, "Secure Automated Subscriber & Device Onboarding for Private Wireless," White Paper, Mar. 2025. [Online]. Available: [https://onelayer.com/secure-device-onboarding-private-wireless-white-paper/].