



<https://doi.org/10.5281/zenodo.17698416>

5G Non-Public Networks for Industry 4.0: Architecture, Use Cases, and Future Directions

Syed Owais Shah¹

owais@hu.edu.pk

Muhammad Asad Khan^{2*}

Corresponding Auhtor Email: asadkhan@hu.edu.pk

Mohsin Shah³

syedmohsinshah@hu.edu.pk

Nasir Mehmood Bahadar⁴

nasir.mehmood@hu.edu.pk

Mohsin Khan⁵

mohsin_btn@yahoo.com

Abstract

The integration of 5G Non-Public Networks (NPNs) in Industry 4.0 has the potential to revolutionize industrial automation by offering ultra-reliable, low-latency communication, and secure connectivity for mission-critical applications. This paper explores the role of 5G NPNs in industrial environments, highlighting the architectural components, deployment models, and key use cases, such as real-time control, predictive maintenance, and remote monitoring. The paper also addresses the challenges associated with NPN deployment, including spectrum management, latency issues, and integration with legacy systems. We provide recommendations for industrial adopters, emphasizing the need for hybrid deployments,



<https://doi.org/10.5281/zenodo.17698416>

careful spectrum planning, and the adoption of edge computing to minimize latency. Additionally, the paper outlines the future research directions, including the role of AI/ML in optimizing 5G NPNs and the importance of security and energy efficiency in the sustainable deployment of 5G networks.

Index Terms: 5G Non-Public Networks (NPNs), Industry 4.0, Time-Sensitive Networking (TSN)

INTRODUCTION

The fourth Industrial Revolution, commonly referred to as Industry 4.0, is fundamentally transforming global manufacturing and industrial processes [1]. This paradigm shift is characterised by the integration of cyber-physical systems, the Internet of Things (IoT), cloud computing, and artificial intelligence, leading to highly automated, flexible, and data-driven smart factories. The realization of this vision, however, is critically dependent on a robust, high-performance, and secure communication infrastructure that can meet the stringent requirements of industrial applications [2]. Traditional connectivity solutions, such as Wi-Fi and wired Ethernet, often fall short in providing the necessary combination of massive device connectivity, ultra-low latency, high reliability, and guaranteed quality of service (QoS) across complex industrial environments.



<https://doi.org/10.5281/zenodo.17698416>

The advent of Fifth Generation (5G) mobile networks is the key enabling technology to bridge this connectivity gap. Unlike previous generations, 5G was designed with three distinct service categories in mind: enhanced Mobile Broadband (eMBB), massive Machine-Type Communications (mMTC), and Ultra-Reliable Low-Latency Communications (URLLC). The URLLC capability, promising latency as low as 1 millisecond and reliability exceeding 99.999%, is particularly crucial for time-sensitive industrial control, robotics, and remote operation applications [3]. Furthermore, 5G's capacity for mMTC allows for the connection of millions of sensors and devices per square kilometre, essential for comprehensive industrial monitoring and data collection.

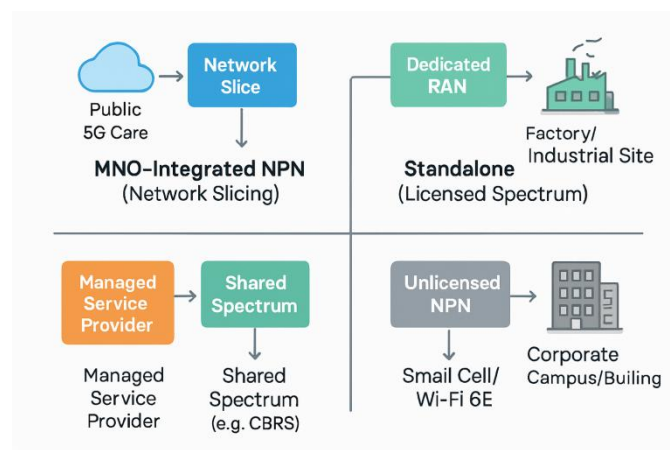


Figure 1: 5G Non-Public Network Configuration Scenarios for Industry 4.0

While public 5G networks offer significant improvements, the unique demands of industrial environments—including strict



<https://doi.org/10.5281/zenodo.17698416>

security protocols, data sovereignty requirements, dedicated QoS, and coverage tailored to specific premises—have necessitated the development of 5G Non-Public Networks (NPNs), also widely known as the 5G NPNs [2] [5]. A 5G NPN is a dedicated, localized 5G network deployed for a specific entity, such as a factory, port, or campus. These networks provide the enterprise with full control over its network resources, security policies, and data, ensuring that mission-critical applications are isolated from public network traffic and performance fluctuations. The 3GPP has defined various deployment options for NPNs, ranging from fully isolated standalone networks to those integrated with a Mobile Network Operator's (MNO) infrastructure, offering flexibility to meet diverse industrial needs [6].

The four primary deployment models for 5G NPNs are illustrated in Figure 1, which highlights the differences in core network ownership, spectrum usage, and integration with public networks. A detailed comparison of these models, focusing on key performance indicators such as latency, security, and cost, is provided in Table 1.

The convergence of 5G NPNs and Industry 4.0 is a pivotal moment for industrial digitalization. NPNs are poised to unlock a new generation of industrial use cases that were previously



<https://doi.org/10.5281/zenodo.17698416>

technologically infeasible. These include, but are not limited to, real-time control of Automated Guided Vehicles (AGVs) and robotics, high-definition video-based quality inspection, remote expert assistance via Augmented Reality (AR) and Virtual Reality (VR), and predictive maintenance powered by massive sensor data aggregation [1]. The ability of NPNs to provide guaranteed performance and enhanced security makes them the ideal foundation for these critical applications, driving operational efficiency, reducing downtime, and enabling entirely new business models [13].

Despite the immense potential, the deployment and operation of 5G NPNs in industrial settings present several challenges [5]. These include the complexity of network planning and integration with existing industrial IT/OT (Information Technology/Operational Technology) infrastructure, the need for specialized skills for maintenance, the management of spectrum allocation, and the development of cost-effective and scalable architectural solutions. Furthermore, as the technology matures, there is a continuous need to explore new architectural paradigms, such as edge computing integration and network slicing, to fully optimize NPN performance for the most demanding industrial applications [7] [15].



<https://doi.org/10.5281/zenodo.17698416>

This article aims to provide a comprehensive and structured overview of the role of 5G Non-Public Networks in enabling the Industry 4.0 vision. The main contributions of this work are summarized as follows:

Architecture Analysis: We detail the various deployment models and architectural components of 5G NPNs, with a specific focus on configurations best suited for industrial environments.

Use Case Elaboration: We present a thorough examination of key industrial use cases that are critically dependent on the capabilities of 5G NPNs, providing a clear link between network features and industrial benefits.

Future Directions and Challenges: We identify and discuss the current technical and operational challenges in NPN deployment and outline promising future research directions, including the integration of AI/ML for network management and the evolution towards 6G.

The remainder of this paper is organized as follows: Section 2 provides an overview of the Industry 4.0 communication requirements and 5G deployment models. Section 3 details the architecture, key components and data flow in 5G NPNs. Section 4 explores the functional and performance requirements of NPNs in Industry 4.0. Section 5 discusses the application testing key



<https://doi.org/10.5281/zenodo.17698416>

categories and evaluation criteria. Section 6 explains the key risks in the deployment of 5G NPN in Industry 4.0. Section 7 concludes and presents some recommendations, while Section 8 summarizes the future direction in this area.

Table 1: Comparison of 5G Non-Public Network Deployment Scenarios for Industry 4.0

Feature	1. MNO-Integrated NPN (PNI-NPN)	2. Standalone NPN (SNPN)	3. Shared Spectrum NPN	4. Unlicensed NPN (NR-U/Wi-Fi 6E)
Description	Enterprise utilizes a slice of the Mobile Network Operator's (MNO) network, with a dedicated RAN and UPF/MEC.	Enterprise owns and operates the entire network (Core and RAN) using dedicated licensed spectrum.	Enterprise operates the network using shared spectrum with other users (e.g., CBRS in the US, local licensed in Germany).	Enterprise operates the network using unlicensed spectrum (e.g., 5 GHz band for Wi-Fi 6E or NR-U).
Spectrum	MNO's Licensed Spectrum	Dedicated Licensed Spectrum	Shared/Priority Licensed Spectrum	Unlicensed Spectrum

Spectrum of Engineering Sciences

**SPECTRUM OF
ENGINEERING
SCIENCES**

Online ISSN

3007-3138

Print ISSN

3007-312X



<https://doi.org/10.5281/zenodo.17698416>

<p>Ownership/ Control</p>	<p>Low to Medium. MNO manages the core; enterprise has control over the local RAN and edge applications.</p>	<p>High/Full. Enterprise has complete control over the network elements and policies.</p>	<p>High. Enterprise manages the network, but spectrum is open to all users. governed by a sharing framework.</p>	<p>High. Enterprise manages the network, but spectrum is open to all users.</p>
<p>Latency</p>	<p>Low (typically 10-20 ms). Dependent on the location of the MNO's core and MEC.</p>	<p>Ultra-Low (can achieve <1 ms). Optimized for URLLC due to local core and dedicated resources.</p>	<p>Low (typically 5-15 ms). Performance is generally excellent but can be affected by spectrum sharing rules.</p>	<p>Variable (typically 10-30 ms). Subject to interference and contention from other unlicensed devices.</p>
<p>Security</p>	<p>High. Leverages MNO's robust security framework, but traffic mixes with</p>	<p>Highest. Complete isolation from public networks;</p>	<p>High. Isolated from public networks, with enterprise-level security</p>	<p>Medium. Isolated from public networks, but susceptible to local radio</p>

Spectrum of Engineering Sciences

**SPECTRUM OF
ENGINEERING
SCIENCES**

Online ISSN

3007-3138

Print ISSN

3007-312X



<https://doi.org/10.5281/zenodo.17698416>

	public network at the core.	enterprise controls security policies and data sovereignty.	policies. all security and data sovereignty.	interference and requires strong local security management.
Reliability	High. Backed by MNO's infrastructure and Service Level Agreements (SLAs).	Highest. Dedicated resources ensure guaranteed QoS and minimal external interference.	High. Spectrum sharing mechanisms (e.g., SAS in CBRS) provide reliable access, but not fully guaranteed.	Medium. Susceptible to interference and congestion, making guaranteed QoS difficult.
Initial Cost	Lowest. Lower capital expenditure (CAPEX) as the MNO provides the core infrastructure.	Highest. Requires significant CAPEX for core, RAN, and spectrum acquisition/leasing.	Medium. Lower cost than dedicated, but still requires investment in hardware and	Low. Utilizes readily available, lower-cost equipment.

Spectrum of Engineering Sciences

**SPECTRUM OF
ENGINEERING
SCIENCES**

Online ISSN

3007-3138

Print ISSN

3007-312X



<https://doi.org/10.5281/zenodo.17698416>

	Medium.	Highest.	Full	Medium.	OPEX	Low to Medium.
	Monthly	operational	for	for	OPEX	for
	subscription/serv	expenditure	maintenance	maintenance	maintenance	
Operational	ice fees paid to	(OPEX)	for	and spectrum	and local	IT
Cost	the MNO.	maintenance,	access fees.	staff.		
		power, and				
		skilled				
		personnel.				
	Enterprises	Mission-	Enterprises	in	Non-critical	
	needing high	critical	regions	with	applications	or
	performance but	applications	shared	areas	where	
	preferring a	requiring	spectrum	existing	Wi-Fi is	
	managed service	absolute	availability,	insufficient,	and	
	and lower initial	lowest latency,	seeking	a cost	is the	
Best For	investment.	highest	balance	of	primary	
		reliability, and	performance	constraint	(e.g.,	
		complete data	and cost	(e.g.,	office buildings,	
		sovereignty	ports, logistics).	general	IoT).	
		(e.g., advanced				
		manufacturing				
		, remote				



5G Non-Public Networks in the Industry 4.0 Environment

The realization of the Fourth Industrial Revolution, or Industry 4.0, is predicated on the seamless integration of cyber-physical systems, industrial Internet of Things (IIoT) devices, and cloud-based analytics. This transformation from traditional, centralized automation to decentralized, flexible, and data-driven manufacturing necessitates a communication infrastructure that can support an unprecedented level of connectivity, speed, and precision [1] [2]. Traditional industrial networks, such as fieldbuses, Industrial Ethernet, and even current-generation Wi-Fi, are often insufficient to meet the diverse and stringent demands of modern industrial applications, particularly in terms of mobility, massive device density, and guaranteed Quality of Service (QoS) [3].

The advent of Fifth Generation (5G) mobile networks has been specifically engineered to address these gaps. Unlike previous generations primarily focused on consumer broadband, 5G was designed with a service-centric architecture to support three distinct, yet complementary, service categories defined by the International Telecommunication Union (ITU-R) and standardized by the 3GPP [6]:

Industrial Communication Requirements



<https://doi.org/10.5281/zenodo.17698416>

Industrial applications within the Industry 4.0 paradigm can be broadly categorized based on their communication requirements, which directly map to the three 5G service categories. These requirements are significantly more demanding than those of typical consumer or enterprise networks. The most challenging requirements stem from the Critical Control applications, which demand Ultra-Reliable Low-Latency Communications (URLLC). For instance, wireless control of industrial robots requires end-to-end latency below 10 milliseconds, with some applications, such as coordinated motion control, requiring latency as low as 1 millisecond and a reliability of $1 - 10^{-5}$ (99.999%) or better [5]. This level of performance is essential to replace wired connections with flexible, mobile wireless links without compromising safety or operational efficiency.

Table 2: Industrial Communication Requirements and 5G Service category

Industrial Application Category	Key Requirements	Corresponding 5G Service Category	Example Use Cases
Critical Control	Ultra-low latency (< 10 ms), Ultra-high reliability (>	URLLC (Ultra-Reliable Low-Latency Communications)	Real-time control of robotics, closed-loop process control, wireless safety

Spectrum of Engineering Sciences

**SPECTRUM OF
ENGINEERING
SCIENCES**

Online ISSN

3007-3138

Print ISSN

3007-312X



<https://doi.org/10.5281/zenodo.17698416>

	99.999%)		systems, remote surgery.
Massive Monitoring	Massive connection density (> 1 million devices/km ²), Low power consumption, Long battery life (up to 10 years)	mMTC (massive Machine-Type Communications)	Asset tracking, condition monitoring, massive sensor networks, predictive maintenance.
High-Bandwidth Data	High throughput (up to 10 Gbps), High mobility	eMBB (enhanced Mobile Broadband)	High-definition video surveillance, Augmented Reality (AR) for maintenance, Virtual Reality (VR) for remote training, large file transfers.

Table 3: Key Challenges 5G Deployments in Industry 4.0

Pain Point	Description	Mitigation
------------	-------------	------------

Spectrum of Engineering Sciences



**SPECTRUM OF
ENGINEERING
SCIENCES**

Online ISSN

3007-3138

Print ISSN

3007-312X

<https://doi.org/10.5281/zenodo.17698416>

Information shortage	Operators may receive incomplete or inaccurate data	Real-time data validation via 5G
Safety hazards	Industrial environments demand strict safety	5G wireless reduces hazardous cabling and enables safer remote control
Strict industrial requirements	Latency, reliability, security thresholds	Use URLLC features, slicing, and edge computing
Legacy device integration	Factories contain decades-old systems	Adaptation layers and industry protocol support
Usability	Industrial staff may not be trained on telecom systems	5G-LAN and simplified management interfaces

Role of 5G-LAN and Time Sensitive Networking (TSN)

Two foundational technologies—5G-LAN and Time Sensitive Networking (TSN)—serve as crucial enablers for fulfilling the diverse performance and reliability requirements inherent to Industry 4.0 applications.

- *5G-LAN Integration* leverages the wireless adaptability of 5G technology alongside the established practices of enterprise Ethernet environments. This integration facilitates the seamless inclusion of wireless devices into existing Layer-2 network domains, promoting interoperability and operational continuity. Key features include support for robust enterprise-grade security policies and



<https://doi.org/10.5281/zenodo.17698416>

the ability to administer networked devices through familiar management platforms. As a result, industrial administrators are able to oversee and control 5G endpoints with the same efficacy as traditional Ethernet-connected devices, thereby simplifying operational workflows and reducing administrative overhead.

- *Time Sensitive Networking (TSN) Support* this extension of TSN capabilities across wireless domains, introducing significant challenges, particularly concerning precise time synchronization, deterministic packet scheduling, and ultra-low latency communications. To address these requirements in a 5G context, advanced TSN support encompasses:

- *Reliable (g)PTP-based time synchronization mechanisms,*
- *Maintenance of ultra-low jitter across radio links,*
- *Deployment of TSN translators both within the network infrastructure and end devices,*
- *Assurance of consistent performance regardless of device mobility.*

With these capabilities, 5G NPNs are equipped to support highly synchronized motion control systems, safety-critical industrial automation, and other real-time operation scenarios, positioning them as a foundational technology for advanced industrial environments [16].



<https://doi.org/10.5281/zenodo.17698416>

Benefits of 5G NPNs in Industry 4.0

5G enables Industry 4.0 by delivering ultra-fast data speeds, extremely low latency, robust reliability, and secure connectivity, which support real-time automation, predictive maintenance, and smart manufacturing processes. These advances facilitate large-scale device integration, immediate process adjustments, and seamless operations in industrial environments, resulting in greater efficiency, flexibility, and safety for next-generation factories and supply chains. Unlike Wi-Fi, 5G NPN can serve large areas without excessive handovers, ensuring deterministic coverage.

Key Pain Points and Solutions

Deploying NPNs in Industry 4.0 is not without challenges. The integration of these advanced networks into industrial environments is not without its challenges. From ensuring data accuracy to addressing legacy system compatibility, several key pain points must be overcome. This subsection explores these challenges and provides insights into how 5G technologies, such as real-time data validation, ultra-reliable low-latency communications (URLLC), and wireless solutions, can effectively mitigate these obstacles, enabling a seamless transition to smarter, more connected industrial systems [14]. These challenges are summarized in Table 3.



<https://doi.org/10.5281/zenodo.17698416>

Industry 4.0 Use Case: Architecture, Components and Data Flow

The integration of 5G technology into industrial environments, as part of the Industry 4.0 vision, presents transformative potential by replacing traditional wired communication systems with wireless connectivity. This section outlines the architecture, scenario, and key components involved in a generic Industry 4.0 use case, demonstrating how 5G non-public networks (NPNs) can enhance industrial processes.

Architecture Overview

The architecture of the Industry 4.0 use case leverages several key technologies to enable seamless communication and control. Below is an overview of the critical components integrated into the system, highlighting their roles and interactions in the overall architecture [4].

- *Devices and Controlling Stations:* The end-user devices and their respective controlling stations are integrated into the system to facilitate the industrial applications. These devices interact with the 5G network, providing real-time data and control over various industrial processes such as automation, monitoring, and control.
- *5G Modems:* End-user devices are connected to the 5G network through 5G modems, which serve as the physical interface



<https://doi.org/10.5281/zenodo.17698416>

between the devices and the 5G network. These modems provide the necessary hardware components and input/output ports to support communication across industrial applications.

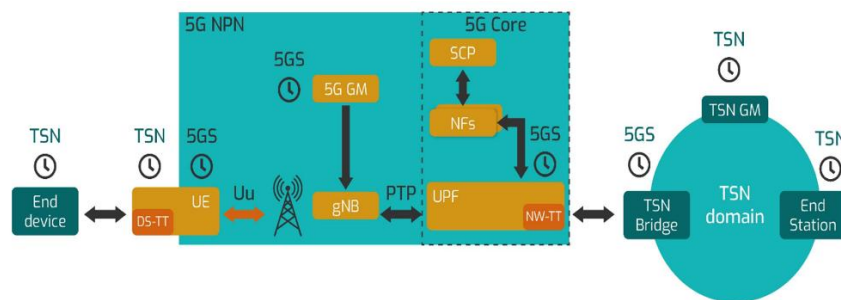


Figure 2: High High-Level Topology of the Industry 4.0 Use Case

- **5G RAN (Radio Access Network):** The 5G Radio Access Network (RAN) is essential for enabling 5G connectivity for industrial devices, ensuring wireless access to the network and associated applications. The RAN supports network slicing, which allows the network to allocate resources and prioritize traffic based on the specific requirements of different industrial applications, such as low latency or high bandwidth [24].
- **5G Core Network (5GC):** The 5G Core Network is virtualized, based on a Service-Based Architecture (SBA) that supports key industrial requirements like Time-Sensitive Networking (TSN) and time synchronization. The 5GC handles traffic routing, device management, and network orchestration to ensure that industrial



<https://doi.org/10.5281/zenodo.17698416>

applications receive the necessary connectivity, security, and performance.

- *5G Core Management*: The 5G Core Management component provides a management console for overseeing network operations, including the mapping of network slices to different industrial devices and the management of security zones (e.g., IEC 62443 security zones) defined within the fixed industrial network. This ensures that the industrial network operates securely and efficiently.
- *TSN-AF (Time-Sensitive Networking Application Function)*: The TSN Application Function (TSN-AF) facilitates the seamless integration of 5G networks with existing wired industrial devices, such as TSN controllers. TSN-AF ensures the transmission of time-sensitive data packets with minimal delay and precise synchronization.
- *TSN Controller*: The TSN Controller is responsible for maintaining high-precision time synchronization across the network and industrial devices. This component enables flexibility in traffic scheduling, reducing latency and ensuring that time-sensitive applications operate in real-time as required in industrial environments.



<https://doi.org/10.5281/zenodo.17698416>

- *Service Communication Proxy (SCP)*: The Service Communication Proxy (SCP) facilitates communication between all service-based network functions (SBI-enabled 5GC NFs) by enabling transparent service routing for HTTP-based services. The SCP ensures that network functions can interact efficiently and securely across the system.
- *Service Function Virtualisation Orchestrator (SFVO)*: The Service Function Virtualisation Orchestrator (SFVO) is a cloud-native orchestration framework that is used to manage and orchestrate the lifecycle of 5GC network functions. By utilising location-aware orchestration and cross-layer analytics, the SFVO optimises the management of network functions, ensuring that the network operates smoothly and meets the performance requirements of industrial applications.

High-Level Topology

The architecture connects various industrial devices, such as sensors, actuators, and controllers, to a central management system through a 5G network. This high-level topology ensures efficient communication, minimal latency, and robust time synchronization across the system [23]. Key elements of the topology are shown in Fig. 2 and described below:

- *User Equipment (UE)*: End devices, such as sensors, actuators,



<https://doi.org/10.5281/zenodo.17698416>

and controllers, are connected to the network through 5G modems or edge devices, facilitating seamless wireless communication within the industrial environment.

- *TSN Bridge*: The TSN bridge ensures that time-sensitive data is transmitted across the network with minimal latency, ensuring precise synchronization and communication for real-time industrial applications.
- *5G Core Network*: The 5GC manages traffic routing, network slicing, and overall communication between devices. It ensures that all data flows meet the required performance standards (such as latency, bandwidth, and reliability).
- *Network-Side Translator (NW-TT)*: The NW-TT component integrates wireless and wired devices, maintaining time synchronization across the system and ensuring that industrial devices, whether wired or wireless, can interact seamlessly.

This architecture enables the integration of both wired and wireless components, facilitating a flexible and scalable network that can support a wide range of industrial applications and requirements.

Data Flow in Non-Public 5G Network for Industry 4.0

The data flow within a 5G NPN network for Industry 4.0 typically involves various industrial devices such as sensors and actuators communicating over the 5G network infrastructure to achieve real-



<https://doi.org/10.5281/zenodo.17698416>

time control, monitoring, and automation [17]. Here's a description of this data flow and the role of edge computing as shown in Fig. 3:

- *Devices Generating Data:* Sensors installed on machines and equipment continuously collect real-time operational data such as temperature, pressure, motion, and other relevant metrics. Actuators receive control signals to perform physical actions based on processing results.
- *Data Transmission over 5G:* These devices connect wirelessly to the 5G NPN network. The 5G infrastructure provides high bandwidth, ultra-reliable low latency communication (URLLC), and network slicing capability tailored to Industry 4.0 requirements. Data from sensors is transmitted securely and reliably to nearby 5G base stations (gNodeBs).
- *Edge Computing Nodes:* To reduce latency and support real-time decision-making, an edge computing node is deployed close to the industrial site, often integrated with or adjacent to the 5G base stations. The edge node processes and analyzes data locally, minimizing the need to send all data to a remote cloud.
- *Local Data Processing and Control:* The edge computes actionable insights, such as anomaly detection, predictive maintenance alerts, or immediate control commands. It can rapidly



<https://doi.org/10.5281/zenodo.17698416>

send control signals back to actuators within milliseconds to ensure precise operational responses.

- *Cloud Integration:* For broader analytics, historical data storage, and advanced AI-driven insights, aggregated data is securely forwarded from the edge to centralized cloud servers. This multi-tier approach balances latency requirements and large-scale processing needs.
- *Device-to-Device Interaction:* The 5G NPN network enables direct device-to-device (D2D) communication where applicable, facilitating ultra-low latency coordination and synchronization without routing all traffic through the core network.
- *Network Slicing & QoS:* The 5G NPNs configure dedicated network slices for different types of industrial traffic, ensuring quality of service, prioritizing critical control data, and isolating traffic for security.

In summary, sensors and actuators communicate through the 5G NPN to exchange data and control signals. Edge computing plays a vital role by processing data locally at the network edge to drastically reduce latency and support real-time Industry 4.0 automation needs, while also enabling efficient cloud integration for advanced analytics and long-term data management [8].



<https://doi.org/10.5281/zenodo.17698416>

Functional and Performance Requirements

The successful deployment of 5G networks in industrial environments requires both functional and performance specifications to meet the stringent demands of Industry 4.0 applications. This section outlines the key functional and performance requirements that ensure the system operates effectively, securely, and efficiently for industrial use cases [9].

A. Functional Requirements

- *Precise Synchronisation:* Time synchronization is crucial for the smooth operation of time-sensitive industrial processes. The required synchronization accuracy varies depending on the device and its role in the system. For instance, certain devices may need synchronization with an accuracy of 10 μ s for real-time control, while others may tolerate a wider range of 50 ms. Achieving this level of precision is essential to ensure that all devices within the network, including sensors, actuators, and controllers, work in harmony without data discrepancies.

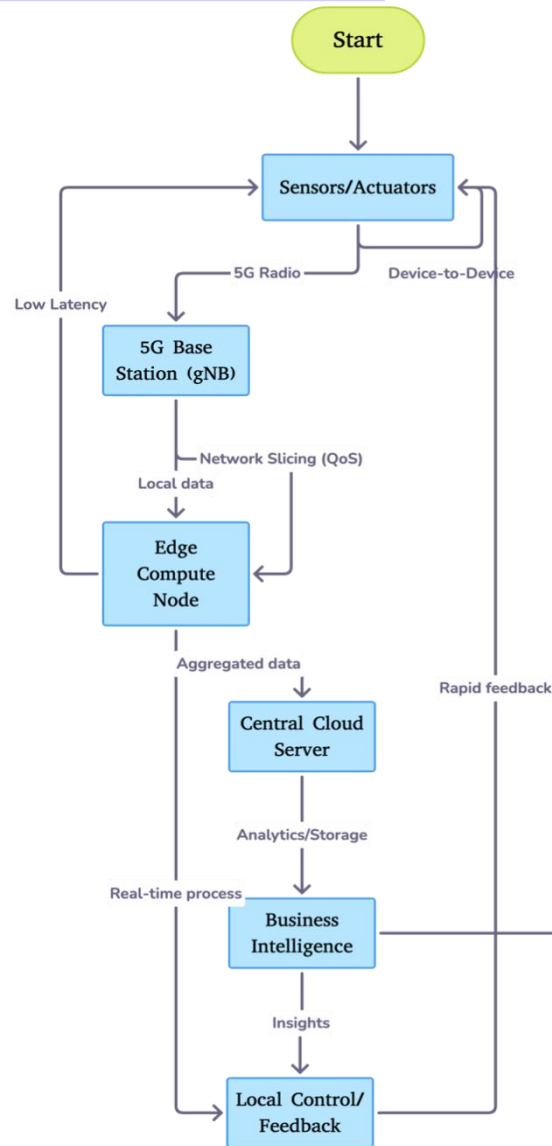


Figure 3 Data Flow in NPN 5G Network for Industry 4.0

- *Frequency Band Adaptation:* Compliance with local regulatory constraints is fundamental for ensuring that the deployed network functions within the designated frequency bands for industrial applications. Adaptation to these frequency bands allows for seamless operation of the 5G network, avoiding interference with



<https://doi.org/10.5281/zenodo.17698416>

other communication systems while adhering to legal and safety guidelines set by local authorities. This ensures that the network is deployed within permissible limits and operates with optimal efficiency [19].

- *Positioning:* The system must support device localization to track the real-time positions of devices within the industrial environment. Accurate positioning is essential for applications like automated guided vehicles (AGVs), drones, and robotics, where location awareness is required for navigation and task execution. 5G technology provides the ability to use advanced positioning techniques, including Time of Arrival (ToA) or Angle of Arrival (AoA), to achieve high-precision device localization.
- *Safety:* Compliance with industrial safety standards is paramount to avoid accidents and ensure the protection of workers and equipment. The system must meet all relevant safety regulations and standards, such as those related to electrical hazards, equipment malfunctions, and emergency shutdown processes. The deployment of wireless communication, such as 5G, reduces the need for cabling and helps in designing safer factory environments by enabling remote control and monitoring [11].
- *Security:* Strong authentication and zone-based access control are essential for protecting sensitive data and ensuring that



<https://doi.org/10.5281/zenodo.17698416>

only authorized personnel can access specific parts of the network. Industrial systems require a high level of security to prevent unauthorized access to critical assets and information. 5G networks incorporate end-to-end encryption, secure boot processes, and robust authentication protocols to protect against cyber threats. Zone-based access ensures that only authorized devices can interact within designated sections of the network, further enhancing security [12].

- *Flexibility*: The flexibility of the network is facilitated through edge computing and virtualization technologies. Edge computing enables real-time data processing at the network's edge, close to where data is generated, minimizing latency and reducing dependency on centralized cloud services. Virtualization allows for dynamic network resource allocation, enabling the network to scale according to changing industrial demands and requirements. This flexibility ensures that the system can be adapted to evolving production processes and integrated with existing infrastructure [18].

Performance Requirements

- *Latency*: For critical control applications in industrial settings, latency must be minimized to ensure real-time communication between devices. The target end-to-end (E2E) latency for such



<https://doi.org/10.5281/zenodo.17698416>

applications should be between 1 ms to 2 ms . This low latency is crucial for controlling industrial machinery, robotics, and automated processes where even a slight delay could lead to performance degradation or system malfunctions [22].

- *Throughput*: Throughput requirements vary based on the type of industrial application. The network must support high uplink and downlink speeds to handle the substantial data traffic from industrial IoT devices, sensors, and video surveillance systems. Specifically, the system should support:

- Up to 200 Mbps uplink: Sufficient to handle data sent from devices to the cloud or centralized control systems, including condition monitoring and sensor data.

- Up to 4 Gbps downlink: Necessary for high-demand applications such as video streaming, remote monitoring, and large data transfers from the cloud or servers to industrial devices.

- *Reliability*: Reliability is critical in industrial networks where the failure to deliver data can result in costly downtime or operational errors. The network must ensure a *packet delivery success rate of at least 99.9%*, meaning that almost all transmitted data packets must be delivered without loss. This high reliability is essential for mission-critical applications such as safety monitoring, real-time control, and automated systems.



<https://doi.org/10.5281/zenodo.17698416>

- *Availability*: Availability refers to the system's ability to remain operational without significant downtime. Industrial environments require *up to "six nines" availability (99.9999%)*, meaning a maximum of only *0.3 seconds of downtime per year*. Achieving this level of availability is necessary to avoid disruptions in manufacturing or control processes, ensuring continuous, uninterrupted operation of industrial equipment.
- *Power Efficiency*: Optimizing power consumption is crucial to meet sustainability goals and reduce operational costs. The network must be designed to minimize energy use while maintaining performance, particularly in remote and industrial environments where power efficiency is a key consideration for both operational savings and reducing environmental impact. This includes optimizing energy consumption in devices, network components, and cloud resources.
- *Coverage*: Ensures that the network can deliver connectivity throughout the entire industrial site, including hazardous and hard-to-reach areas. The system must provide sufficient gNB (gNodeB) Effective Isotropic Radiated Power (EIRP) while meeting safety limits for hazardous areas. Ensuring optimal coverage is essential for maintaining connectivity in environments with high interference or challenging physical conditions, such as dense



<https://doi.org/10.5281/zenodo.17698416>

factory floors, industrial warehouses, or confined spaces.

Application Testing: Key Categories and Evaluation Criteria

Deploying a 5G Non-Public Network (NPN) within industrial settings, a structured approach to testing is essential for ensuring that the network meets the diverse requirements of Industry 4.0 applications. Below are the key categories of test applications that should be considered for evaluating the behaviour, performance, and integration capabilities of the NPN. Each category addresses specific aspects of industrial network functionality, from real-time monitoring to advanced control systems.

- Remote Monitoring as a Service: Test the ability of the 5G NPN to support continuous monitoring of industrial equipment and processes. This category should focus on real-time data streaming and video surveillance, evaluating the network's capacity to handle high-bandwidth applications while maintaining low latency and high reliability. Below are some guidelines for testing:
 - Data Integrity and Reliability: Ensure that sensor data and video streams are transmitted reliably without significant packet loss or delay.
 - Latency Requirements: Measure the time taken for data to travel between sensors, video feeds, and monitoring stations, ensuring it meets real-time application needs.



<https://doi.org/10.5281/zenodo.17698416>

- Scalability: Assess how the network performs when multiple monitoring systems are active simultaneously.
- *Remote Control with Real-Time Feedback*: Evaluate the 5G network's capability to support remote control of industrial devices, such as robotic arms, automated guided vehicles (AGVs), or machinery, with real-time feedback. This category ensures that operators can control devices in a timely and accurate manner from a remote location. Some testing guidelines are:
 - Low Latency: Ensure that control signals are transmitted with minimal delay, particularly for time-sensitive tasks.
 - Feedback Accuracy: Test how quickly the control system receives feedback from the devices being controlled to ensure real-time adjustments.
 - Network Reliability: Evaluate the network's ability to maintain stable control and feedback even under varying environmental conditions.
- *5G Integration and Adaptability in Industrial Environments*: Assess how well the 5G network integrates with existing industrial infrastructure, including legacy systems and equipment [20]. This category is crucial for ensuring that the 5G NPN does not disrupt ongoing operations and can work alongside current technologies. Testing guidelines are:



<https://doi.org/10.5281/zenodo.17698416>

- Compatibility with Legacy Systems: Test the ability of the 5G network to interface with older devices and protocols.
- Interoperability: Ensure smooth communication between new 5G devices and existing wired networks or legacy systems.
- Flexibility and Scalability: Verify that the 5G network can be scaled and adapted to meet future industrial demands without significant reconfiguration.
- *Process Control Over 5G*: Evaluate the ability of the 5G NPN to support real-time control of industrial processes, such as manufacturing or assembly lines, where high reliability and low latency are critical for maintaining production quality and efficiency. Some guidelines for this application testing are:
 - End-to-End Latency: Ensure that process control signals are transmitted and received in real time, meeting the required latency thresholds for critical applications.
 - Data Throughput: Test the network's capacity to handle large volumes of data from sensors and devices while ensuring real-time processing and control.
 - Reliability and Redundancy: Ensure that the network supports continuous operations with minimal risk of data loss or failure in control loops.
- *VR/AR over 5G (Optional)*: This category evaluates the



<https://doi.org/10.5281/zenodo.17698416>

potential of using Virtual Reality (VR) and Augmented Reality (AR) technologies over the 5G network for training, maintenance, or remote support in industrial environments. While optional, VR/AR can offer valuable applications in areas requiring immersive experiences. To test VR/AR following parameters should be evaluated:

- High-Quality Streaming: Test the ability to stream high-definition VR/AR content without interruptions or significant buffering.
- Latency and Interactivity: Measure the responsiveness of VR/AR applications in real-time, ensuring smooth interactions between the user and the environment.
- Network Bandwidth: Assess the network's ability to support the high bandwidth requirements of VR/AR applications without compromising other critical network operations.

Risk Assessment for 5G NPN Deployment in Industry 4.0

The successful deployment of a 5G Non-Public Network (NPN) in industrial environments requires identifying and addressing key risks that may arise during the process. These risks include issues related to frequency availability, latency, network coverage, timing synchronization, integration with legacy systems, and alignment with evolving 3GPP standards. Each risk poses potential challenges



<https://doi.org/10.5281/zenodo.17698416>

to the deployment and performance of the network, but with pre-defined mitigation strategies, the project can maintain its resilience and adapt to unforeseen circumstances [25].

The following Table 4 summarizes the key risks, their impact, and the mitigation strategies in place to address them:

Table 4: Summaries of Key Risks, their Impact and Mitigation Strategies

Risk	Description	Mitigation Strategy
Frequency Unavailability	Limited availability of required frequency bands due to local regulatory constraints could hinder deployment.	Ensure the use case is adapted to available frequency bands (e.g., 2.4 GHz).
End-to-End (E2E) Latency Issues	High latency in the network could affect time-sensitive applications, leading to delays in control signals.	Continuous monitoring, Edge computing will be used to reduce delays



<https://doi.org/10.5281/zenodo.17698416>

Coverage Gaps Coverage gaps in Detailed coverage industrial planning, site surveys, environments may radio planning, and result in areas optimal placement of without sufficient base stations, will connectivity. ensure comprehensive coverage.

Timing Synchronization Challenges Timing Time-Sensitive synchronization Networking (TSN) will issues may cause be integrated to delays and data maintain discrepancies, synchronization. affecting industrial process control.

Integration Delays with Existing Systems Integrating the 5G An integration strategy network with legacy will be developed early, systems may cause using middleware and delays due to protocol translation for compatibility issues. smooth communication between 5G devices and legacy systems.



<https://doi.org/10.5281/zenodo.17698416>

FUTURE DIRECTIONS

As 5G Non-Public Networks (NPNs) continue to mature, further research and development efforts will be needed to address evolving industrial needs and challenges. Several areas warrant future exploration:

B. Enhanced Integration with Legacy Systems

As industries transition to 5G, the integration of existing legacy devices and protocols will remain a significant challenge. Future work will focus on refining adaptation layers and translators to ensure seamless communication between older systems and modern 5G devices. Additionally, the development of standardized solutions to bridge these gaps will facilitate faster adoption across various industrial sectors.

C. Improved Spectrum Management and Coverage Optimization

The effective use of spectrum, particularly in challenging environments such as factories with high metal content or outdoor industrial sites, will require ongoing innovations in radio frequency planning and coverage solutions. Research into dynamic spectrum allocation and smart antenna technologies will be key to optimizing coverage and performance in complex industrial



<https://doi.org/10.5281/zenodo.17698416>

environments, ensuring that connectivity remains reliable and secure.

D. Next-Generation Edge Computing for Real-Time Applications

While edge computing is a critical enabler of low-latency and real-time decision-making, its full potential has yet to be realized in industrial contexts. Future work will explore how edge computing can be more deeply integrated into industrial workflows, providing real-time analytics, advanced machine learning capabilities, and enhanced decision support at the edge. This will empower industries to respond to events in real-time, further enhancing operational efficiency and safety.

E. Security and Privacy in 5G NPNs

With the increased use of 5G for mission-critical applications, ensuring the security and privacy of industrial data becomes even more critical. Future research will focus on developing more robust security frameworks tailored specifically for 5G NPNs. This includes improvements in authentication, encryption, and access control, as well as advanced threat detection and prevention techniques to safeguard industrial networks from cyberattacks.



<https://doi.org/10.5281/zenodo.17698416>

F. Advanced Automation and Artificial Intelligence

As the 5G NPNs become more ubiquitous in industrial settings, the next phase of their evolution will likely involve deeper integration with artificial intelligence (AI) and machine learning (ML) technologies. These technologies can enable smarter decision-making and process optimization by leveraging the massive amounts of data generated by industrial IoT devices. Future work will explore how 5G networks can support AI-driven automation, improving production efficiency, predictive maintenance, and resource management.

G. Sustainability and Energy Efficiency

As industries push towards more sustainable practices, energy consumption within industrial 5G networks will become an important focus. Future research will explore how 5G infrastructure can be optimized for energy efficiency, reducing the environmental impact of large-scale industrial IoT deployments. This includes energy-efficient hardware design, smart power management, and leveraging green technologies to minimize the carbon footprint of 5G-based industrial networks [21].

CONCLUSION AND RECOMMENDATIONS

The integration of 5G Non-Public Networks (NPNs) in industrial environments represents a pivotal step toward realising Industry



<https://doi.org/10.5281/zenodo.17698416>

4.0, offering transformative capabilities for manufacturing, automation, and industrial control systems. The 5G NPNs, powered by technologies like 5G-LAN and Time-Sensitive Networking (TSN), offer unmatched advantages in terms of ultra-reliable, low-latency, and secure wireless communication. These features make 5G NPNs ideally suited for applications that require real-time control, high data throughput, and robust security, such as motion control systems, industrial robots, autonomous vehicles, and remote monitoring.

By complementing existing Ethernet infrastructures, 5G NPNs provide the scalability and flexibility required to support the increasing demands of industrial IoT (IIoT) systems. Additionally, these networks enable a level of adaptability that traditional wired solutions cannot provide, allowing for seamless reconfiguration of systems and devices in dynamic environments.

Key recommendations for industrial adopters highlight a strategic approach to deploying 5G in industrial settings. Hybrid deployments, which integrate 5G alongside legacy infrastructures, are especially beneficial where mobility and flexibility are crucial, such as in automated warehouses, AGVs (Automated Guided Vehicles), or remote operations. The adoption of Stand-Alone Non-Public Networks (SNPNs) is recommended where data



<https://doi.org/10.5281/zenodo.17698416>

sovereignty, privacy, and deterministic performance are essential—particularly in industries dealing with sensitive or mission-critical data. Edge computing is another key recommendation, as it enhances the responsiveness and processing power of the network by localizing data processing near the devices, minimizing latency, and ensuring faster decision-making capabilities.

In addition, careful spectrum planning and coverage optimization are critical in environments with complex physical conditions—such as hazardous areas or spaces with high interference (e.g., metal factories). Furthermore, prioritizing TSN for synchronization ensures that industrial systems operate in harmony, maintaining precise timing for safety-critical tasks. The ability to integrate legacy systems and devices through adaptation layers and translators allows industries to transition gradually without the need for wholesale replacements of existing assets. Finally, network slicing is essential for guaranteeing that different types of traffic (e.g., safety, control, and monitoring) are securely and efficiently segmented within the same network.

These factors collectively enable industries to harness the full potential of 5G NPNs networks, transforming their operations into more adaptive, efficient, secure, and intelligent systems, aligning with the overarching goals of Industry 4.0.



<https://doi.org/10.5281/zenodo.17698416>

REFERENCES

- [1] Varga, P., et al. (2020). 5G support for Industrial IoT Applications—Challenges and Solutions. *Sensors*, 20(3), 828.
- [2] Ordonez-Lucena, J., et al. (2019). The use of 5G Non-Public Networks to support Industry 4.0 scenarios. *IEEE Communications Magazine*, 57(11), 14-20.
- [3] Khan, B. S., et al. (2022). URLLC and eMBB in 5G industrial IoT: A survey. *IEEE Open Journal of the Communications Society*, 3, 1150-1171.
- [4] Meira, J., et al. (2023). Industrial Internet of Things over 5G: A practical implementation. *Sensors*, 23(11), 5199.
- [5] Prados-Garzon, J., et al. (2022). 5G non-public networks: Standardization, architectures, and challenges. *IEEE Communications Surveys & Tutorials*, 24(1), 40-69.
- [6] 3GPP. (2022). TS 23.501 System Architecture for the 5G System (5GS), Release 17.
- [7] ITU-R. (2020). Framework and overall objectives of the future development of IMT for 2020 and beyond.
- [8] Wu, J., et al. (2021). 5G Enabled Smart Manufacturing: Use Cases, Challenges, and Research Directions. *IEEE Communications Magazine*, 59(7), 70-76.



<https://doi.org/10.5281/zenodo.17698416>

- [9] Zhang, Y., et al. (2021). Time Sensitive Networking and 5G for Real-Time Industrial Applications. *IEEE Network*, 35(5), 124-131.
- [10] Liu, X., et al. (2020). MEC-Enabled 5G Networks for URLLC in Industrial Internet of Things. *IEEE Network*, 34(3), 24-31.
- [11] Chen, M., et al. (2023). AI-Enhanced 5G Networks for Industry 4.0. *IEEE Transactions on Industrial Informatics*.
- [12] Sheth, N., et al. (2022). Security and Privacy Challenges in 5G and Beyond Industrial Networks. *IEEE Internet of Things Journal*.
- [13] Al-Turjman, F. (2020). Industrial IoT and the Need for 5G and Beyond Networks. *Sensors*, 20(7), 1980.
- [14] Bennis, M., et al. (2018). Ultra-Reliable and Low-Latency Wireless Communication: Tail, Risk, and Scale. *Proceedings of the IEEE*.
- [15] Raza, S., et al. (2020). 5G for Industry 4.0: Overview, Use Cases, and Future Directions. *IEEE Access*.
- [16] Popovski, P., et al. (2020). Wireless Access for Ultra-Reliable Low-Latency Communication: Principles and Building Blocks. *IEEE Network*.
- [17] Chen, S., et al. (2023). Private 5G Networks for Smart Manufacturing: Architecture and Future Research Directions. *Journal of Network and Computer Applications*.



<https://doi.org/10.5281/zenodo.17698416>

- [18] Ding, Z., et al. (2021). Wireless IIoT for Smart Factory: Architecture and Security. IEEE Transactions on Industrial Electronics.
- [19] Fenouillet-Beranger, C., et al. (2022). Spectrum Sharing and Management in Industrial 5G Networks. IEEE Transactions on Cognitive Communications and Networking.
- [20] Osman, A., et al. (2022). 5G-LAN: Integrating 5G Wireless with Industrial Ethernet. IEEE Communications Letters.
- [21] Sarigiannidis, P., et al. (2023). Energy Efficiency in 5G-based Industrial IoT Networks. IEEE Transactions on Green Communications and Networking.
- [22] Sauter, M. (2021). From Industry 4.0 to Industry 5.0: Industrial Automation and Beyond. IEEE Industrial Electronics Magazine.
- [23] Garcia, O., et al. (2020). Network Slicing for 5G and Beyond: A Survey on Architectures, Requirements, and Solutions. IEEE Communications Surveys & Tutorials.
- [24] Lu, Y., et al. (2021). 5G Network Slicing for Industrial IoT: Use Cases and Challenges. IEEE Communications Standards Magazine.
- [25] Zolanvari, M., et al. (2023). Security Frameworks for Private 5G Networks in Industry 4.0. IEEE Transactions on Industrial Informatics