GSMA

Private 5G Industrial Networks

An analysis of Use Cases and Deployment

June 2023

GSMA

The GSMA is a global organisation unifying the mobile ecosystem to discover, develop and deliver innovation foundational to positive business environments and societal change. Our vision is to unlock the full power of connectivity so that people, industry and society thrive. Representing mobile operators and organisations across the mobile ecosystem and adjacent industries, the GSMA delivers for its members across three broad pillars: Connectivity for Good, Industry Services and Solutions, and Outreach.

This activity includes advancing policy, tackling today's biggest societal challenges, underpinning the technology and interoperability that make mobile work, and providing the world's largest platform to convene the mobile ecosystem at the MWC and M360 series of events.

GSMA Digital Industries

GSMA Digital Industries is a community of network operators, industrial organisations and the wider ecosystem working together to advance the adoption of mobile technologies in the industrial and manufacturing sector. As the industrial revolution continues towards digitalisation and connected intelligence, the community explores all aspects of the industrial value chain from raw material extraction, to refining, supply chain, component production, assembly, and smart warehousing.

Through a series of forums, activity work streams and events including MWC, the GSMA Digital Industries community aims to:

- Understand the business and operational needs required from across the industrial value chain.
- Identify new kinds of innovative opportunities and collaborations to develop stronger solutions and propositions that harness the benefits of 5G disruptive technologies; AI, Telco Edge Cloud, computer vision, robotics, AR/ VR and digital twins.
- Unlock and address barriers to digital transformation in the sector.
- Share key knowledge including new implementations, successful use cases, achievements and commercial propositions from global leaders.
- Drive new relationships with the wider ecosystem to achieve success.

Find our more and how to get involved at:
gsma.com/iot/digital-industries

Follow the GSMA IoT on LinkedIn:
linkedin.com/showcase/gsma-internet-of-things

Contents

Contents

Executive summary

The industrial sector is undergoing a major generational shift. Industry 4.0, the digitisation of the sector, is set to create far more flexible, efficient and sustainable production lines. Mobile technologies, such as 5G IoT, underpin this transformation by enabling industrial and manufacturing companies and their supply chain partners to use emerging technologies, such as AI and machine vision, wirelessly. As a result, they have vastly improved visibility and control over all aspects of their business. Increasingly, the industrial sector is looking to obtain exclusive access to network resources using private networks.

This document, which has been produced by members of the GSMA Digital Industries forum, takes a close look at the role of private networks in the context of the industrial and manufacturing sectors. It discusses the business ownership models and deployment options available to enterprises. The section on ownership models covers standalone non-public networks (SNPN), public network integrated non-public networks (PNI-NPN) and neutral host networks (NHN).

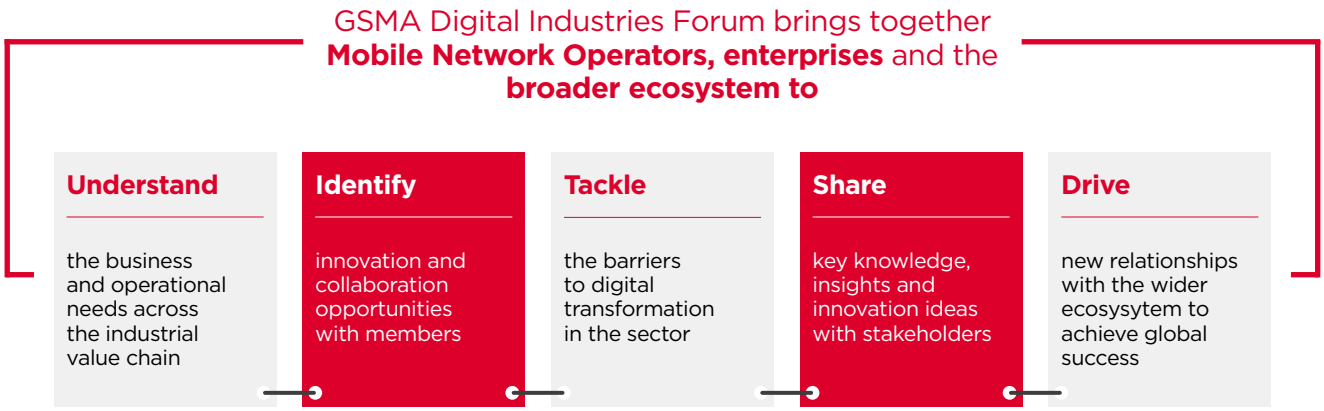
The document also explains the role of the industrial enterprise and connectivity provider and implications for management of the SNPN. A SNPN could be managed directly by the enterprise or provided as a managed service by a mobile network operator (MNO), or by a third party such as an equipment vendor or a software or cloud vendor. A PNI-NPN could be managed by an MNO or jointly by an MNO and the industrial enterprise. Beyond the ownership models, the document reviews deployment options across single-factory, multi-factory and connected factory scenarios.

To illustrate, the document includes several use cases, including automated guided vehicles, campus networks, industrial crane operation automation, ports, airports, smart tools and XR applications. Finally, the document looks at the industrial and manufacturing sectors' requirements for private networks.

GSMA Digital Industries

GSMA Digital Industries is a community of network operators, industrial organisations and the wider ecosystem which is working together to advance the adoption of mobile technologies in the industrial and manufacturing sectors. Through collaboration and shared objectives, the forum aims to understand the business and operational needs across the industrial value chain, identify innovation and collaboration opportunities with members, tackle the barriers to digital transformation in the sector, share key knowledge, insights and innovation ideas with stakeholders and drive new relationships with the wider ecosystem to achieve global success.

Figure 1 | The aims of the GSMA Digital Industries Forum



Source: GSMA

Acknowledgements

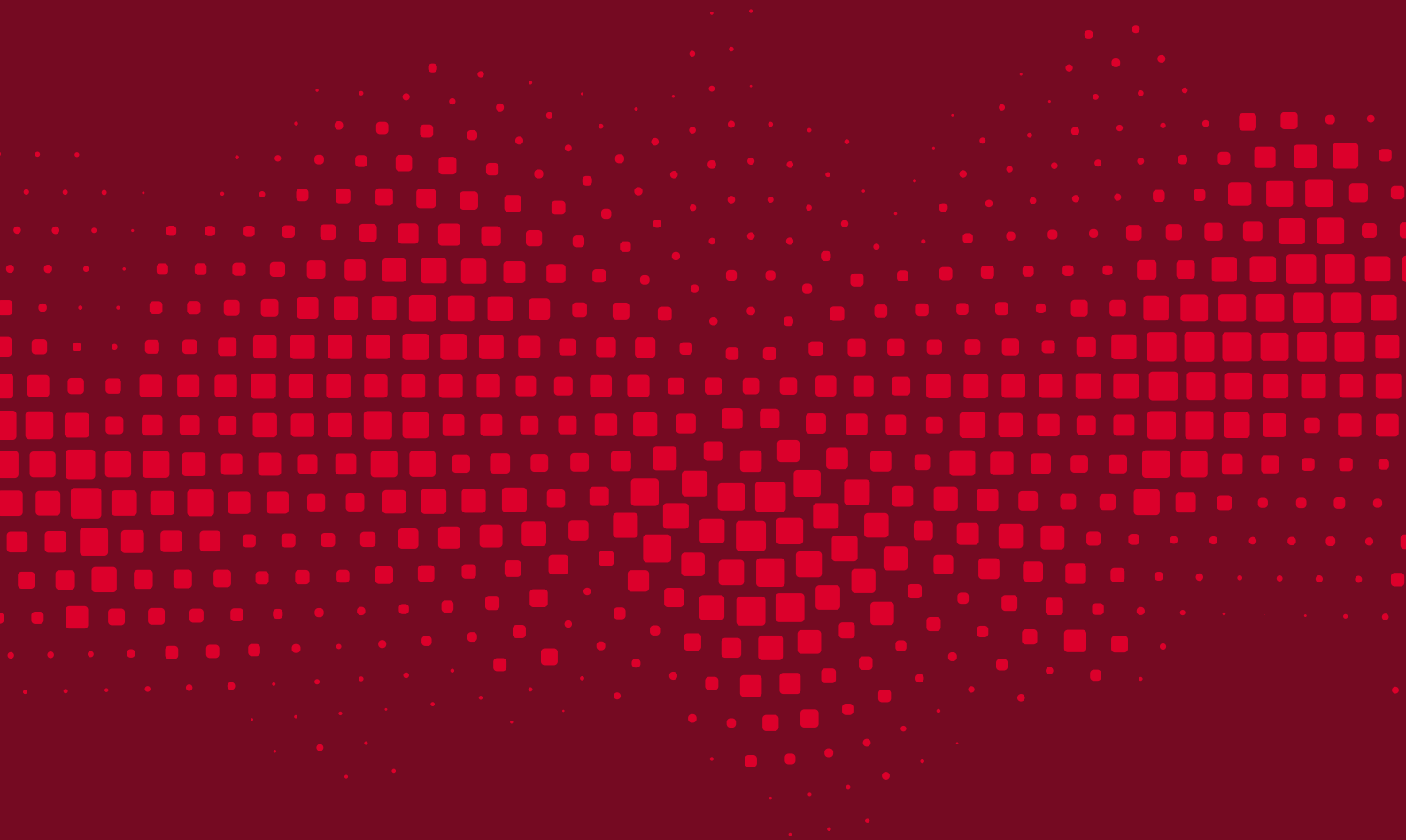
The document has been created thanks to the following contributing Digital Industries Members.

Lead Mobile Operator:

Supporting GSMA Members:

Digital Industries Ecosystem Contributors:

Introduction



Overview

Aimed at industrial enterprises and operational technology companies, this document will provide analysis and guidelines for 5G private networks, deployment options, use cases and high-level requirements. The document draws on previous GSMA studies **[1]** and GSMA 5G industry campus network deployment guideline **[2]**.

Crucially, 5G delivers low-latency and high bandwidth wireless connectivity. Enterprises from across the industrial value chain, including raw material extraction, refining, supply chain, component production, assembly and warehousing, can all harness the benefits of these new technologies. The GSMA 5G Transformation Hub[1] provides a catalogue of 5G case study examples across a range of sectors including smart manufacturing.

The concept of an enterprise having exclusive access to a private network has been around for some time. Increasingly, the industrial and manufacturing sectors view private networks as important to achieve the speed, security, privacy, bandwidth and low-latency connectivity required for their digital transformation and Industry 4.0 ambitions.

The document uses examples from different industrial sectors to illustrate different deployment needs based on local regulatory rules and business requirements. It also discusses the benefits of using 5G networks as a unifying technology which can meet many Industry 4.0 wireless networking needs, including wide coverage and interoperability with legacy devices and networks.

The GSMA has previously published a paper on the technical and operational differences of Wi-Fi and 5G/4G Industry 4.0 networks **[3]**, which discusses how 5G cellular technology is particularly suitable for a range of Industry 4.0 use cases.

1 gsma.com/5ghub/

Scope

This document's scope is as follows:

- Identification of different use cases deployed today and planned for the next five years
- Understanding critical Key Performance Indicators (KPIs), device requirements and network management and slicing requirements for non-public networks/ private networks (NPN)
- Business models for NPN
- Understanding deployment models for operational technology (OT) device management, configuration, authentication, user management and service requirements
- Understanding the limitations of standalone NPN and when public integrated non-public networks (PNI-NPN) are used
- Network slicing use-cases in industrial networks
- Mobility use cases and device requirements
  - Movement of devices from public networks (run by MNOs) to NPNs
  - Movement between different zones in the same NPN
  - Movement from one NPN to another
- Conclusion and high-level guidelines for end users (large and small/medium enterprises)

Objective

The primary objective of this document is to investigate the mutual benefits for both information and communication technology (ICT) and operational technology (OT) in the integration of 5G networks into industrial premises, while keeping a focus on 3GPP standards development and practical business objectives.

The document aims to help:

- The OEMs/vendors to comply with enterprise requirements.
- End users (industrial operators and enterprises) to better understand the practicality of real-world situations.
- Private networks providers and MNOs to understand industrial enterprises' requirements for quality of service and mobility.
- Management of the 5G network across NPNs, including public network integrated NPNs.

The document should also provide readers with a basic understanding of today's end-to-end 5G private networks offerings.

3GPP on Private Networks

To support private networks, 3GPP developed the non-public networks concept in 5G for:

- Network control (applying configuration and control that is not possible through the public networks).
- Achieving sufficiently low latency for critical operations.
- Guaranteed coverage indoors and inside the industrial shops and industries (throughout the premises, if outside connectivity is not required).
- Higher performance (to provide industrial operators with controlled configurations and quality of service).
- Applying security based on roles, access, positions etc. specific to the needs of the vertical or entity.

As 5G is designed to employ a service-based architecture [TS23.501], it is now possible to place the core network control and data plane functions in distributed locations rather than needing to keep them all together in the central location of a mobile network operator. This flexibility enables different vertical industries to meet their specific requirements, such as low latency, jitter and bandwidth aggregation, close to the devices. Also, 5G has introduced application functions which can be located near the premises or in the cloud. Through the network slicing concept, a 5G core and RAN can provide isolated and QoS maintained services, thereby enabling vertical industries to provide their respective customers with a service level agreement (SLA).

3GPP R15 introduced a completely isolated standalone NPN (SNPN) while R16 improved and worked on the SNPN devices requirements. However, 3GPP R16 does not allow SNPNs to interconnect with SNPN devices or to connect to a PLMN (public land mobile network). This is primarily for security and traceability reasons. The SNPN devices are private and un-trusted for the PLMN (public land mobile network) unless they are registered for a PLMN service.

Operators are subject to rules and regulatory requirements for public networks, but these restrictions are not imposed on standalone private networks. 3GPP R16 specifies the ability to identify, discover, select and implement access control for NPNs. In addition, section 5.30 of TS23.501(R16) supports SNPN access via PLMN.

In R17, 3GPP extends the SNPN service to allow Authentication, Authorisation and Accounting (AAA) and specifies user equipment (UE) onboarding for 5G connectivity and remote provisioning for accessing NPN services. In this release, 3GPP also allows IMS voice and emergency services for the SNPN. Further work is continuing in 3GPP studies to enhance NPN capabilities.

Benefits of 5G Private Networks

The industry 4.0 concept introduces cellular wireless connectivity into industrial networks. Private wireless networks provide a number of advantages to an industrial operator or enterprise, including ultra-low latency, privacy, security and aggregation of high-bandwidth data, while modernising the manufacturing lines by enabling them to share equipment, mobile robots and Automated Guided Vehicles (AGVs) at different times.

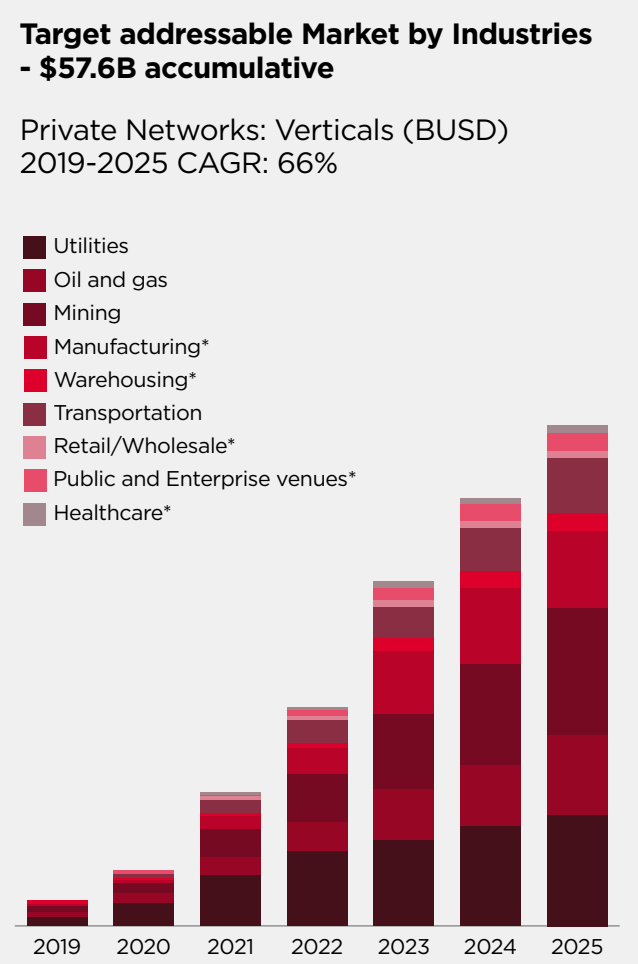
The following diagrams (Figure 2) from 5G Americas **[4]** illustrate the development of the addressable market for private networks in different industry sectors over time **[5]** and estimate the revenue opportunities.

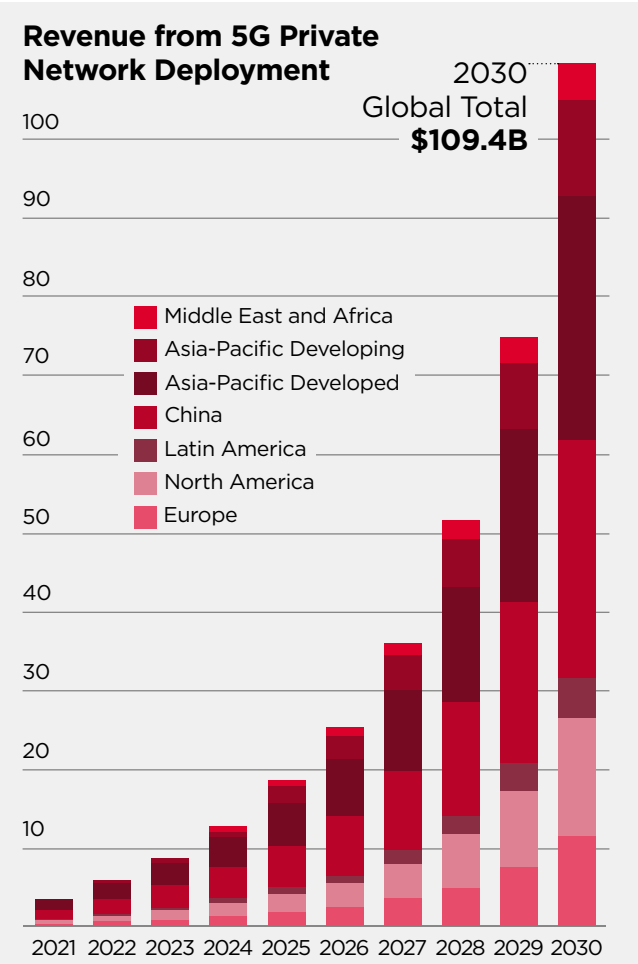
As Figure 2 indicates, manufacturing industries will be significant users of private networks to generate revenues and cost savings. This paper will primarily discuss the operational and technical benefits of 5G for increasing the efficiency of the industrial sector and the transition to Industry 4.0.

For example, without cellular wireless connectivity, a device needs to be connected with a long Ethernet cable, making it difficult to move it across the manufacturing floor. Another advantage of a private network is that the data plane of the 5G system can be on site so customer data need never leave the industrial owner's premises. Most mobile network operators can support private networks with secure access to their public networks.

A private network can be standalone with private spectrum, or it can use national licenced spectrum or unlicenced spectrum depending on the applications employed.

Figure 2 | The addressable market and revenue opportunities for 5G private networks





5G Americas (left,**[4]**), IEEE COMSOC (right, **[5]**)

Why 5G in Industry 4.0 ?

Multiple wireless technologies exist today for local networks. The GSMA previously produced an analysis of the difference between Wi-Fi and 5G **[3]**. While Wi-Fi 6 claims to support Industry 4.0 services, 5G provides better reliability and continuous connectivity if the radio coverage is well-designed. Wi-Fi 6, which can use the 2.4 GHz, 5 GHz and 6 GHz spectrum bands, is designed for indoor and local area networks, but industrial networks require highly reliable connectivity both indoors and outdoors, which 5G cellular technology is able to provide. Future cellular technologies beyond 5G will provide further performance and automation benefits for advanced industrial networks.

Thus, 3GPP 5G networks offer two distinct benefits to industrial enterprises:

1) A flexible virtualised infrastructure with licenced and unlicenced spectrum coverage and management of the network via network slicing, standard API, analytics functions with feedback control and a scalable microservices architecture.

2) Greater wireless coverage, reliable service, inbuilt security and authentication features, ultra-low latency and time-synchronisation services.

Moreover, 3GPP 5G infrastructure components go through a compulsory certification and integration test process.

Figure 3 shows the current and future 5G functionalities identified by the 5G-ACIA (5G Alliance for Connected Industries and Automation) **[6]** for 5G smart factories and process automation. Not all of the functionalities shown in Figure 3 may be available in the market today, but 3GPP R16 has tried to address many of them and 5G Advanced will address most of them.

Figure 3 | 5G functions that are useful for factories and process industries

Functionality	Type / Component	Examples
Quality of service	Data traffic	• Periodic deterministic communication • Aperiodic deterministic communication • Non-deterministic communication • Mixed traffic
	End-to-end latency	0.5 ms to 500 ms
	Data rate up to	Several Gbit/s
	Line synchronicity	Down to 1 µ
Dependability	Communication service availability	Varies from 99.9% to 99.999999%
	Communication service reliability	Varies from 1 day to 10 years
Deployment	Non-public networks	Standalone: NPN and PLMN are deployed on a separate network infrastructure Hosted: NPN is hosted completely or in pan on in part on PLMN infrastructure In-rated: NPN 5G network is integrated into a larger non-3GPP communication network such as an IEEE 802 based network
	Slicing and isolation	Based on a physical network that might be operated by a public operator or an enterprise 5G providers the means to run multiple virtual networks (called slices) for different communication purposes. 5G allows to run those slices independently and if desired isolated from each other
Interworking	Seamless integration	5G can be integrated with wired technologies on the same machine or production line
	Service continuity between 5G non-public and public 5G networks	5G supports mobility between a 5G core network and an evolved packet core (EPC, the core 4G network)
Security	Availability	20 years
	Integrity	Data received not tampered with and was transmitted by the sender
	Confidentiality	Optimising and minimising signaling overhead, particularly for small packet data transmissions In-network caching and operating servers closer to the network edge
Positioning		Between 0.2m and 10m
Efficency	Spectrum, battery (power) and protocol efficiency	
Operation and maintenance		• Fault management • Configuration management, Including provisioning and lifecycle management • Accounting, including online and offline charging • Performance management Including the definition of key performance Indicators (KPIs) • Security management

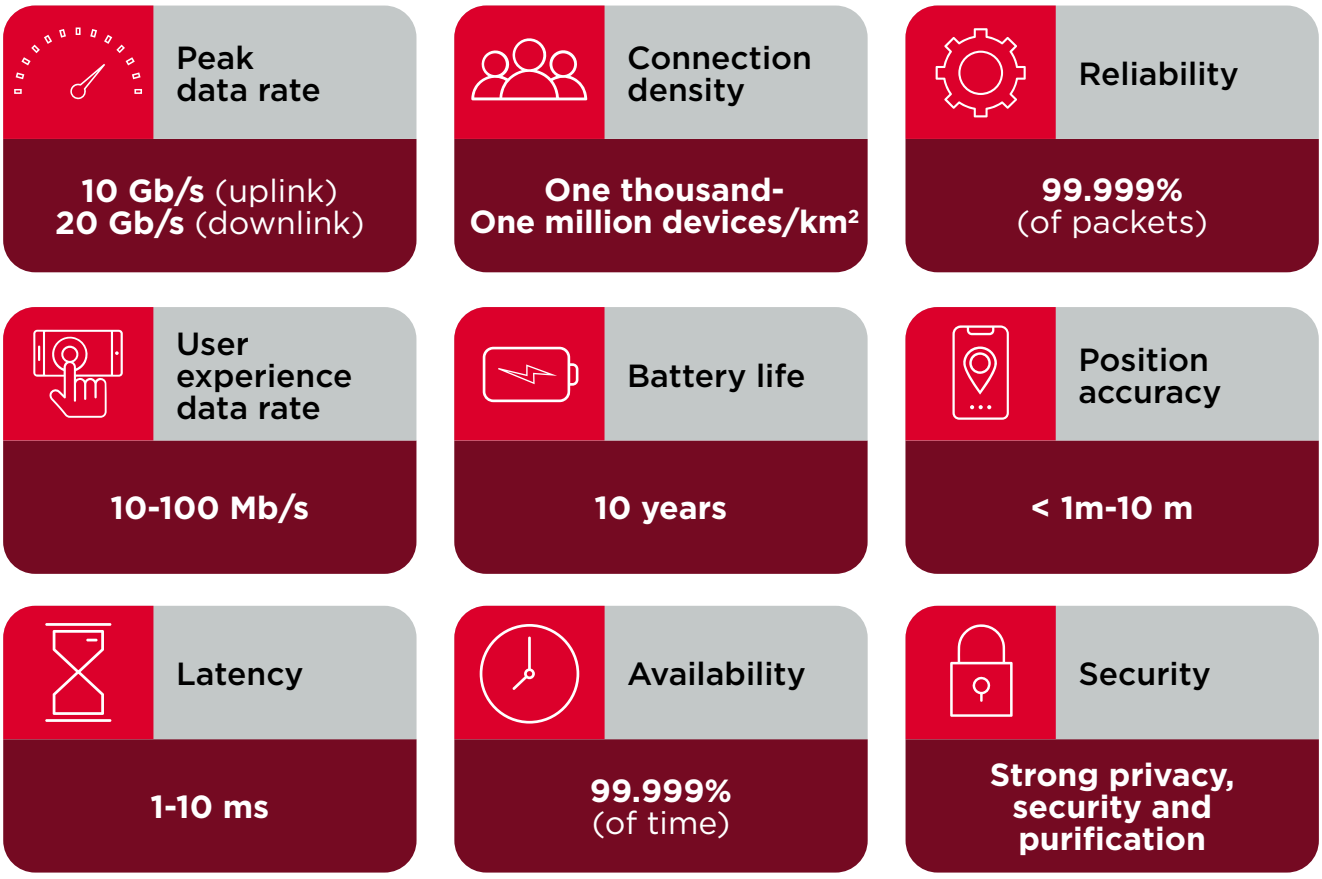
Source: 5G-ACIA

5G provides EAP AKA (extensible authentication protocol authentication and key agreement) authentication-based security and offers 5G system-wide security as part of the 5G network and global identity of devices. Wi-Fi 6 uses the EAP framework and device identity management at the local level. A 5G private network also supports Ultra Reliable Low Latency Communication (URLLC) and network slicing for application isolation.

Each 5G device and network component is tested and certified through an extensive process of standardisation and testing. 3GPP has an extensive process for test specification for device features and network standards and performance. 3GPP RAN and interoperability tests are defined by GSMA, while the actual certification tests are executed by Global Certification Forum (GCF) in Europe and/or the PTCRB in the USA also perform device certification. 3GPP device and equipment manufacturers are responsible for having their products certified by an accredited certification test laboratory. Additionally, MNOs maintain their own certification programmes for device acceptance in their networks. Thus, 5G devices and network equipment have been tested for security, performance and high quality before they are deployed in the MNO's network.

Typical industrial process and manufacturing applications include process automation and control, controller-to-controller communication, sensors' data aggregation and on-premises processing for taking appropriate action quickly, asset management, mobile robots and AGV management.

Figure 4 | 5G target KPI from 5G-ACIA Whitepaper **[7]**



Source: 5G-ACIA

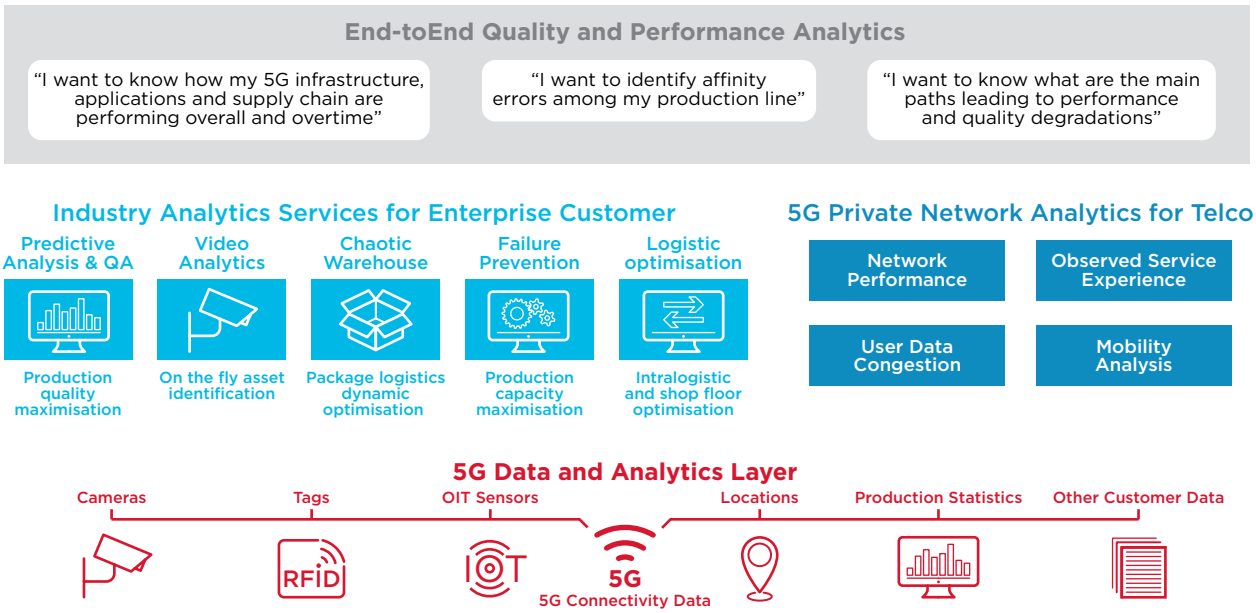
5G private networks can offer wireless, secure, reliable, low-latency, time-sensitive abilities for device-to-device and device-to-applications services along with access to the authorised PLMN devices inside the private networks. Figure 4 lists the 3GPP-defined 5G target key performance indicators that satisfy most of the Industry 4.0 network requirements shown in Figure 2.

Businesses are increasingly looking for real-time, distributed and interconnected analytics. The 5G architecture and ecosystem can provide a scalable data analytics platform to unify and orchestrate analytics across all vertical applications to manage end-to-end services and their respective SLAs.

5G can enable a large variety of use cases in many different domains, functions and industries. Telcos can take the opportunity presented by enterprise demand for private 5G networks to expand their footprint, and their range of services and lines of revenue, by combining network data with industry-specific data, analytics and predictions in order to provide end-to-end quality and performance insights.

Provided by Teradata, Figure 5 illustrates the 5G networks analytics, service analytics and analytics data captured by a cloud platform. The analytics data provides a useful indication of network and service performance for industrial operators and enterprises. The diagram shows a number of analytics services from multiple applications from different industrial sectors.

Figure 5 | 5G Network and industrial applications analytics services – an example of a cloud analytics platform



Source: Teradata

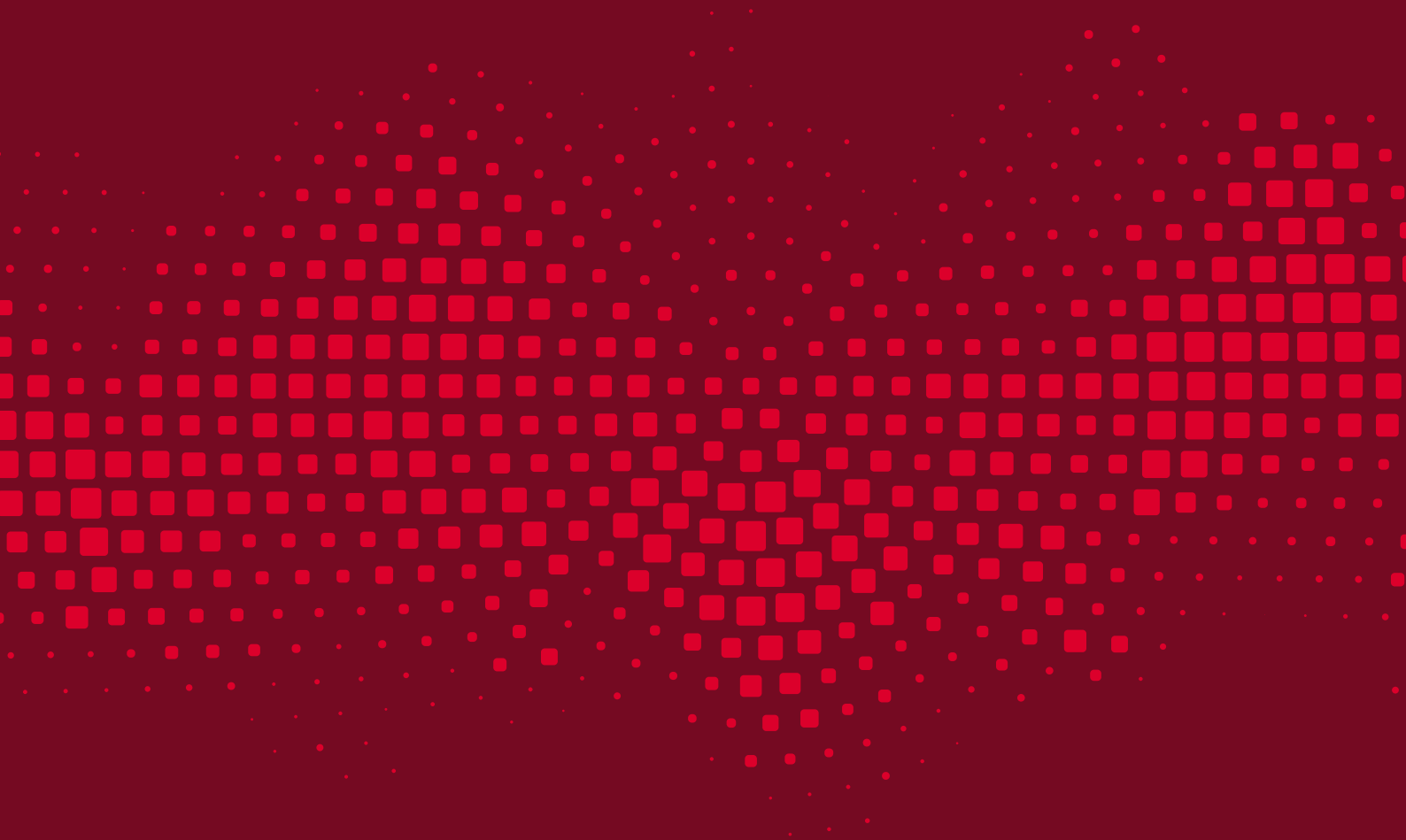
Definitions

Term	Description
5G Massive IoT	5G Massive IoT refers to narrowband IoT (NB-IoT) and LTE-M IoT-connected devices, such as sensors, actuators and other smart devices working with the 5G network system.
5G NSA	5G non-standalone core architecture where a 5G radio network is used with a 4G LTE core architecture.
Core	3GPP defined system and services through network interfaces, control and administrative functions and their interfaces toward the applications.
Network Slicing	3GPP has introduced the concept of end-to-end virtual networks within an operator's network. A network slice is a logical network that runs on top of the shared physical infrastructure and provides isolation of services with required QoS.
NPN	NPN or non-public network is the term 3GPP uses to refer to private 5G networks tailored to different vertical industries. The implementation and placement of the 3GPP network functions and application functions vary due to the vertical industry requirements. A NPN is made possible by the distributed and service-based architecture (SBA) in 3GPP 5G (starting from R15). A NPN can be offered by a mobile network operator or a third-party service provider. NPNs can be standalone or integrated with a public network.
NWDAF	The network data analytics function is defined in 3GPP TS 23.501. This new function collects data from different 5G core functions, user data, user equipment, 5G edge cloud, operation and maintenance functions and analyses them to observe the network behaviour and provides insight into the 5G core network. This function is able to send the feedback data to the relevant 5G system for correcting service performance.
MEC	Multi-access edge computing is a cloud infrastructure platform with storage, computing and network connectivity located near the data source and processing of applications.
MNC	A PLMN is identified by a globally unique PLMN code, which consists of a MCC (Mobile Country Code) and MNC (Mobile Network Code).
PNI-NPN	A PNI-NPN is another configuration of NPN where the private network is connected and integrated with the MNO's PLMN network, typically using the national licenced spectrum. The MNO and the industrial operator may agree on placement of the user-data plane on-site and the RAN could be made private for the enterprise. In this case, the MNO uses 5G network slicing to offer isolation and security protection of customer data and control messages. A PNI-NPN is useful when enterprise applications do not require critically low latency operations. This option is favoured when the industrial owner does not have the capacity to run 5G operations in-house and maintain the quality of their own vertical products and services.
PTCRB	PTCRB certification verifies compliance with global industry standards for wireless cellular devices. It works closely with Global Certification Forum (GCF).
RAN	3GPP radio access network that specifies the air interface and connects the cellular devices to the core network.
SNPN	A standalone NPN, which is deployed in an enterprise location, isolates the 5G core, RAN, devices and device and user information. In the strict sense, the SNPN can be completely isolated from any connectivity to an external network. However, it can be connected with a PLMN network for emergency communications and for selected devices that are registered with a PLMN network in dual mode communication. A SNPN is normally owned and operated by the enterprise owner without any dependency on a PLMN network. The SNPN 5G on-site service may be offered by an MNO or a third-party 5G service provider. In some cases, industrial operators may choose to design, install
Spectrum Leakage	When the energy at one frequency appears to leak out into all other frequencies. See Wikipedia for a detailed technical description
UPF	User data plane function in 5G Core as defined in 3GPP TS 23.501.
URLLC	Ultra-reliable low-latency communication is introduced in 3GPP 5G. This capability will be useful for Industry 4.0 and self-driving vehicles in particular. Typically, a URLLC radio and network service promises to ensure network latency of less than 1ms and the reliability of more than 99.999% for data transmission. URLLC has yet to be launched in the market.

Abbreviations

3GPP	Third Generation Partnership Project
5G-ACIA	5G Alliance for Connected Industries and Automation
AI/ML	Artificial intelligence/machine language
API	Application programming interface
CBRS	Citizen Broadband Radio Service (Range: 3.55-3.70 GHz)
eSIM	Embedded SIM
LiDAR	Light detection and ranging
MEC	Multi access edge computing
mmWave	Millimetre wave frequency band. High band radio (Range 30-300 GHz)
MNC	Mobile network code
MNO	Mobile network operator
NPN	Non-public networks (a 3GPP term introduced with 5G Core specification)
NHN	Neutral host network
NSA	5G non-standalone core (it uses 5G-NR as radio and a 4G core network)
O&M	Operation and maintenance
OT	Operational technology
PN	Private network
PNI-NPN	Public network integrated NPN
RAN	Radio access network
RedCap	5G reduced capability devices
SBI	Service based interface
SLAM	Simultaneous localisation and mapping
SNPN	Standalone non-public network
UE	User equipment (user device)
UICC	Universal integrated circuit card (sometimes known as the SIM card)
UL	Uplink
UPF	User plane function
PLMN	Public land mobile network
IMS	IP multimedia services, as defined by 3GPP
EAP AKA	Extensible authentication protocol – authentication and key agreement
ITU-R	International Telecommunication Union – Radio communication sector
SI	Service integrator
CUPS	Control and user plane separation of 3GPP systems
WAN	Wide area network
SDWAN	Software defined wide area network
DAS	Distributed antenna system
AGV	Automated guided vehicle
AMR	Autonomous mobile robot
PLC	Programmable logic controller

Types of Private Networks



Types of Private Networks

There are a several types of private networks discussed in many industry groups. Many of them originated from 5G ACIA NPN White Paper **[8]** and 3GPP 5G Specification **[9]**.

1) Standalone private networks without any access to and from PLMN

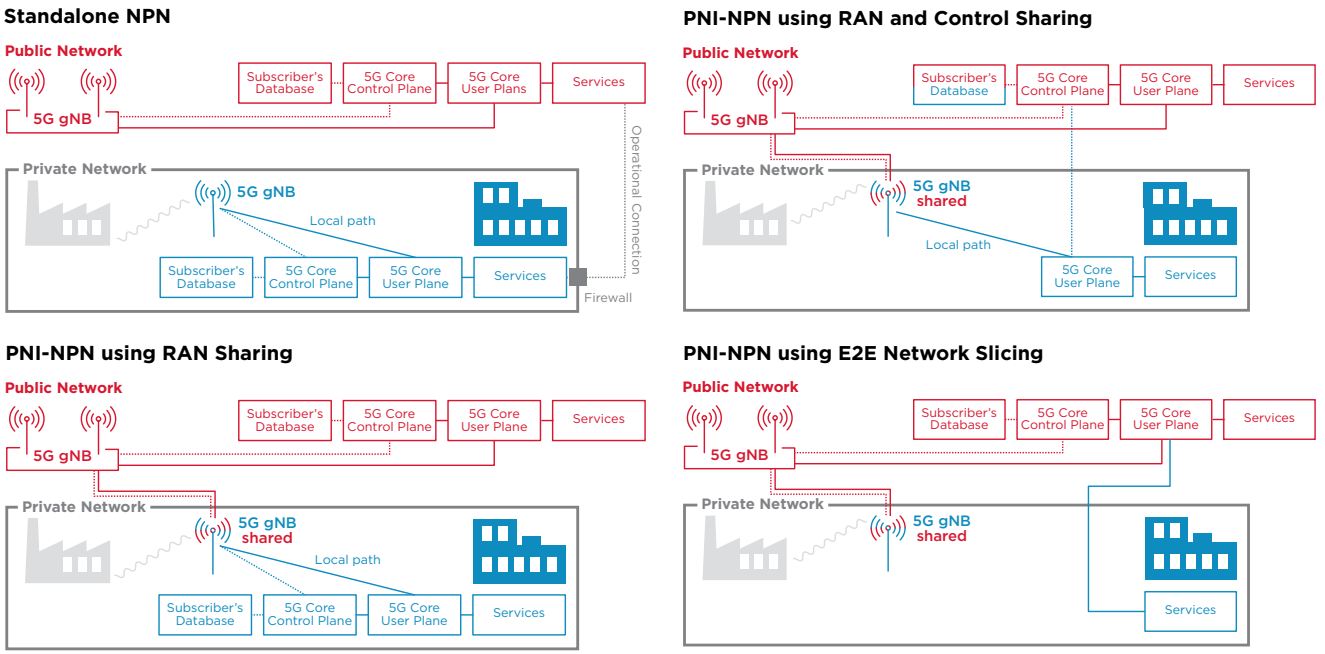
2) Standalone private networks with MNO providing shared RAN

3) Public network integrated private networks using RAN and control sharing

4) Public network integrated private networks using end-to-end network slicing

In Figure 6, red icons indicate the system is managed by an MNO and blue icons signify the system is managed by the enterprise. Red and blue colours indicate the component is shared (e.g. shared RAN and database).

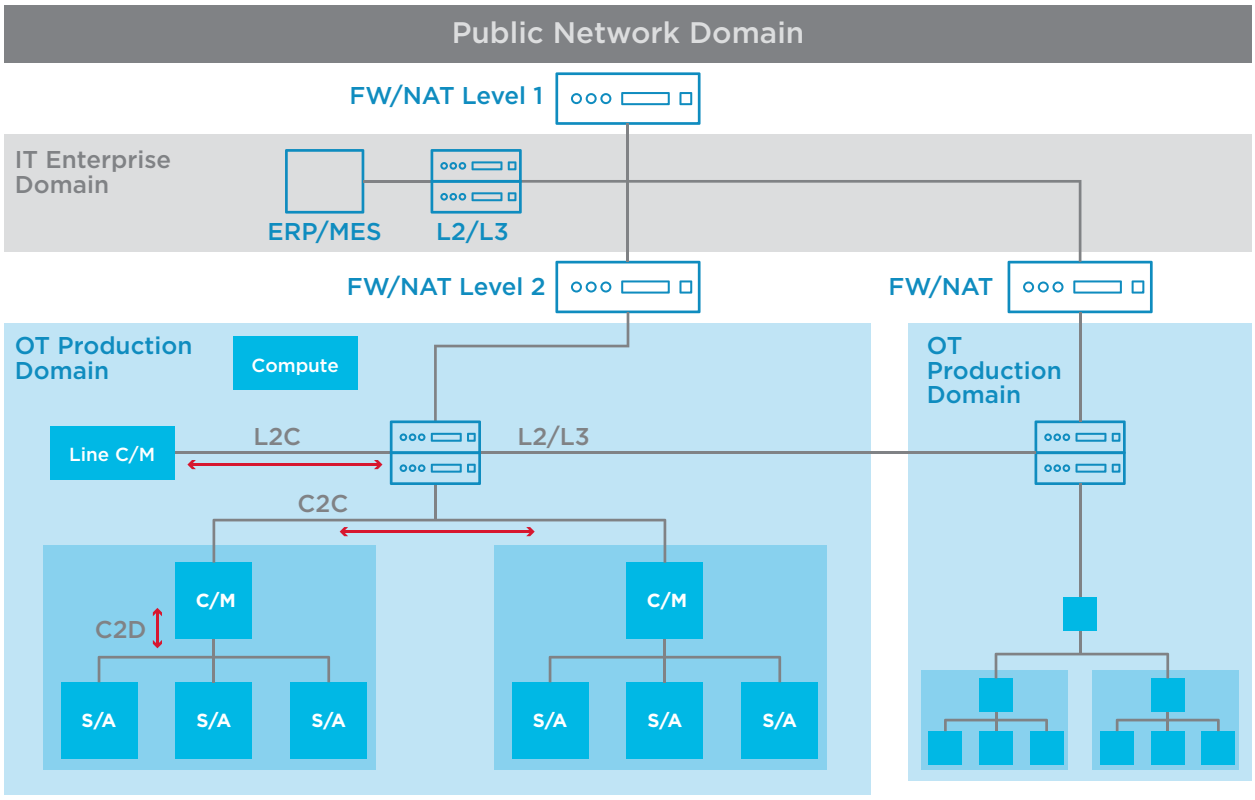
Figure 6 | Private Network configurations



Source: 5G-ACIA

There can be multiple domains in an operational technology network, as shown in Figure 7 **[10]**. There are different policies, requirements and security levels in each domain. Thus, it is possible that the most restricted applications domain will run their own 5G SNPN, while other domains may share a 5G SNPN core network. The various acronyms depicted in Figure 7 are defined in the 5G-ACIA White Paper on 5G Integration of Industrial Ethernet integration **[11]**.

Figure 7 | An example of existing domains of a factory (red lines indicating possible wireless migration)

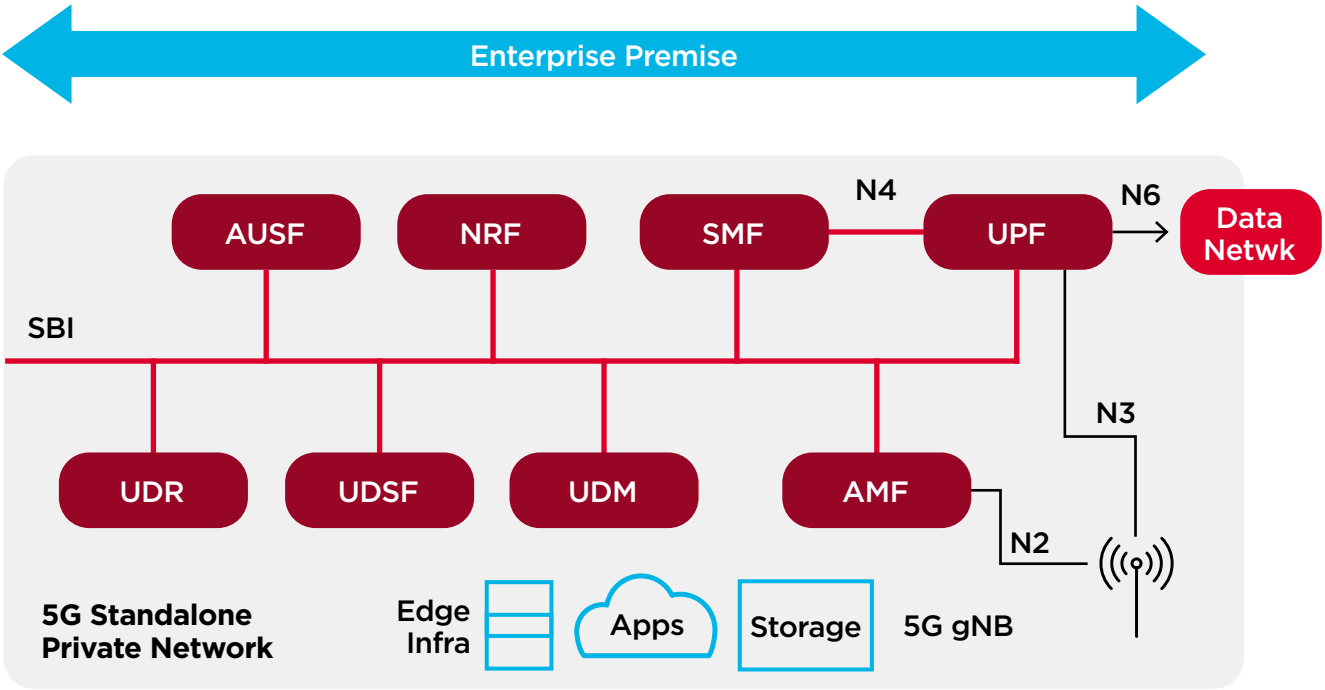


Source: 5G-ACIA. See reference **[11]**

Standalone Non-Public Networks (SNPN)

A SNPN network is usually a self-contained standalone network, which is operated by an industrial operator with leased, unlicenced or privately licenced spectrum, which is blocked for access outside the enterprise, as shown in Figure 8. The implementation has its own radios and 5G network system components, storage and LAN to ensure applications can run quickly and have the capacity they need.

Figure 8 | Isolated SNPN: 5G Core components and RAN, Apps, Storage are all in the Enterprise



Source: Verizon

Figure 8 shows 5G core components and RAN all located inside the enterprise without any PLMN connection. The 5G core components contain both control and data plane functions. Multiple radios are possible in one SNPN. As discussed above, an enterprise may contain different domains.

While an isolated SNPN provides autonomy, data privacy, low latency, local wireless and availability of 5G operations with in-house networks and devices, it can come with a few challenges. These networks require regular maintenance and QoS validation of the connection. There is the possibility of security attacks and leaks of radio signals, and they will require software upgrades and integration with different components of the network. Unlicenced spectrum coverage may be insufficient, so there may be a need for an MNO or third party to integrate spectrum coverage for a larger space. There is a chance of spectrum leakage (where the energy from one frequency leaks out into other frequencies) when shared spectrum is used and when it is not managed by a trusted entity, such as a large MNO. For those reasons, small and medium enterprises typically invite an MNO or a system integrator to install and manage the 5G private network services for them.

Standalone Non-Public Networks with access to Public Networks

SNPN do not need to be completely isolated. There are several reasons for employing outside connectivity using public RAN sharing or other methods. Only a small number of countries, such as the UK, Germany and Japan, will allocate licence spectrum to landowners, meaning enterprises elsewhere may need to use shared RAN for an SNPN. On the other hand, many countries allow MNOs to share their nationally licensed spectrum with landowners. In the US, Citizen Broadband Radio Service (CBRS) spectrum is available for general use in selected areas and a CBRS PAL (Priority Access Licence) is available to businesses, but the bandwidth allocation may not be enough to carry the full load of the industrial operations. In such cases, additional spectrum (such as C-Band and mmWave) may be required from the MNO or other spectrum providers.

In future, 3GPP will support unlicenced spectrum for general use. However, the unlicenced spectrum is not ideal for critical operations in industrial communication because it may be subject to interference, jamming and denial of service attacks etc.

A SNPN may have a connection to the PLMN network for regulatory reasons. There are a number of ways in which a PLMN could support a SNPN:

1) A connection to a PLMN network for voice and data in case of an emergency.

2) SNPN with shared RAN: In this scenario, 5G network components (including the user data base and authentication service and data) are all inside the enterprise premises, but the spectrum is provided by the MNO. The public network and the isolated private network could share a RAN where the spectrum is hosted/shared by the PLMN. With a spectrum sharing solution enabled, both networks may share the antenna and a RF combiner or an antenna and a base station. These solutions are often based on 3GPP Multi-Operator Core Network (MOCN) or Multi-Operator Radio Access Networks (MORAN) technology **[10]**.

3) A connection to a PLMN network as a backup or a failover network (for example, a utility network may need a fallback connection for public safety or regulatory aspects).

4) Allowing devices from a PLMN network into the SNPN network to connect after the user device registers and authenticates itself through the PLMN network (a prior agreement between the PLMN and the SNPN owner must exist).

5) Similarly, 3GPP specifications **[12]** may allow selected SNPN devices (which are registered to the PLMN network) to access a PLMN network during shipment or transit.

Among the above options, some PLMN service providers offer options 1, through 4 above through RAN sharing mechanisms and allow movement between Private and public networks.

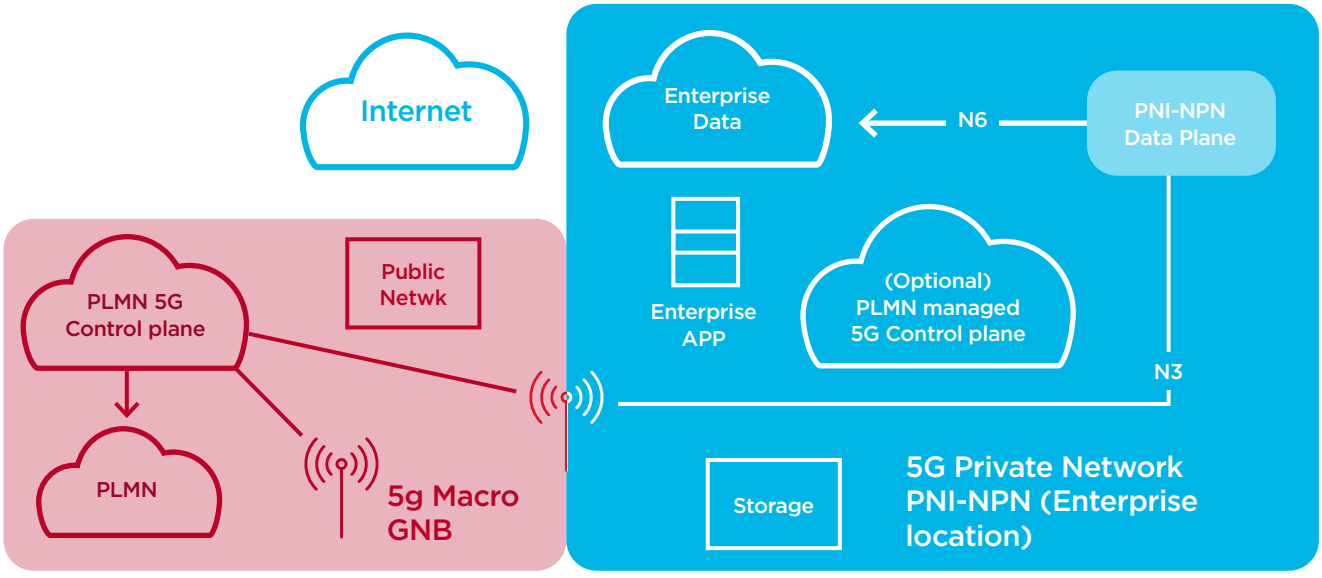
Public Network Integrated Non-Public Networks (PNI-NPN)

A MNO can provide a PNI-NPN in one of two ways:

Option 1: A fully remote managed service in which the MNO employs network slices to isolate private networks for each enterprise or the customers of the enterprise. This option provides a high-level of security and can ensure compliance with an SLA. This is a suitable option when there is no demanding low latency requirement and no local offload of data for processing is required on-site.

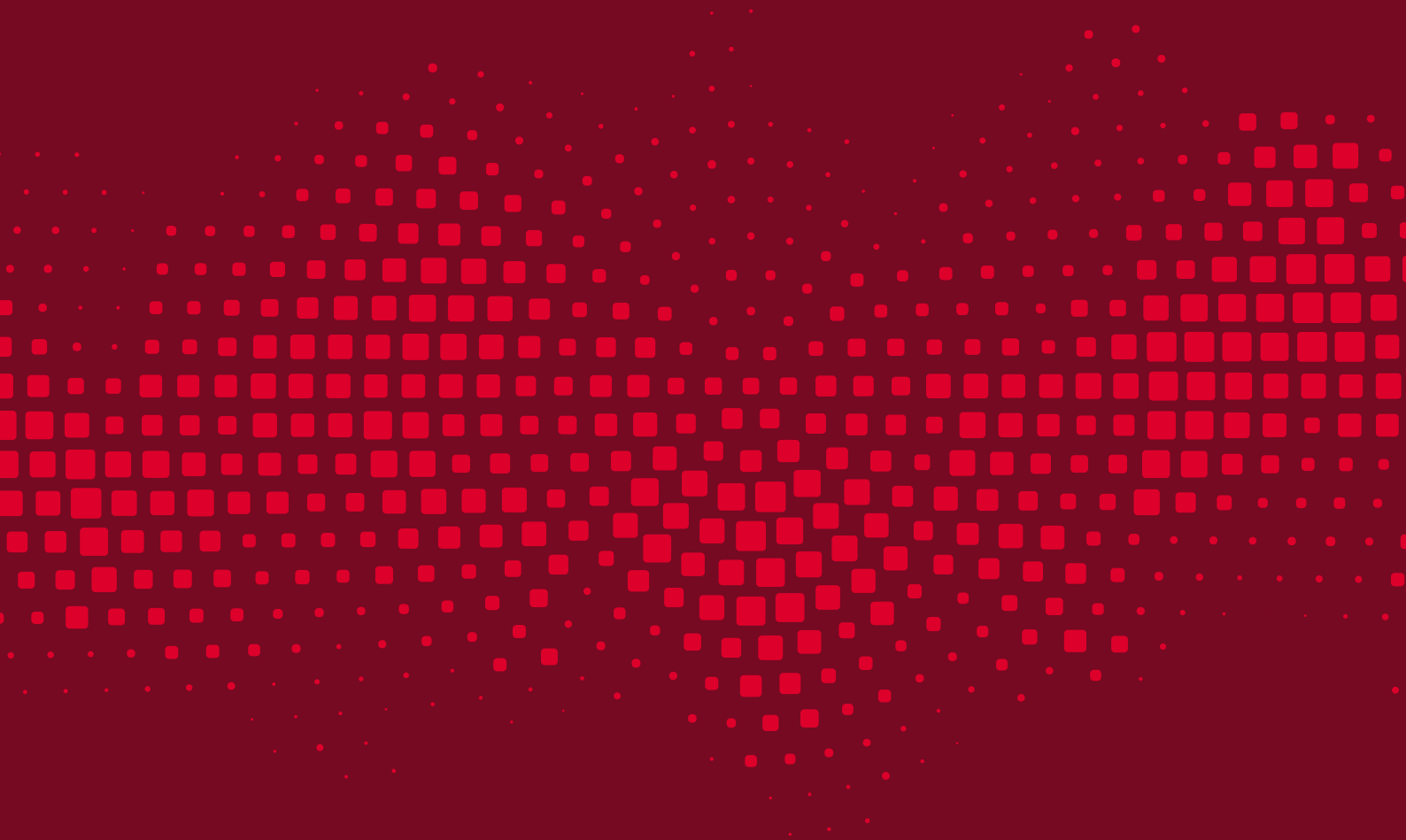
Option 2: (see Figure 9) The MNO and the industry operator agree to place the dedicated or shared 5G RAN/radio and part of the 5G core (UPF, NWDAF or other core functions) on-site for low latency, data offloading and local processing support. In this configuration, most of the control plane remains in the MNO network. A closed access group (CAG) mechanism is used in PNI-NPN configuration to isolate the RAN cells and protect the private network from public network traffic.

Figure 9 | PNI-NPN (option 2) Data plane inside the Enterprise and control plane may reside close-by or on-premise



Source: Verizon

Business models of Private Networks



Planning a Private Network

The model and planning for a private network should consider the following aspects based on the requirements of the organisation, the applications, cost constraints, suppliers and regulatory restrictions:

Spectrum availability

- Does the region have national spectrum only or are unlicenced and privately licenced spectrums available?
- Does the organisation require mid-band or mmWave spectrum?
- How much spectrum capacity is sufficient for the enterprise in the near-term and long-term?

5G system components and different suppliers of components

- Does the organisation host and manage the 5G network itself?
- Does the organisation commission an ICT company to maintain and manage the 5G network inside the organisation?
- Does the organisation require the data plane and data to be inside the premises, but is prepared to outsource the RAN and control plane to an MNO to manage?
- Does the factory or industrial enterprise require two different domains of connectivity (standalone and PLMN integrated) based on production, shipment, IT and logistics needs?

Configuration of ownership and user interfaces

- Ownership of different departments of a manufacturing facility or other industrial premises.
- Ownership of installation, management and maintenance of 5G networks (private and public networks connectivity and inter-connectivity, isolation between them).
- Device subscription ownership: Which devices should be registered at the factory premises and which devices have access to both the SNPN and a PNI-NPN?
- Who is responsible for device maintenance and network performance?
- Ownership of maintenance and enhancement of the 5G system of the interfaces between the enterprise applications and the 5G system or edge computing services.

SLA maintenance

- How often does the organisation require reports on the performance of the network?
- If there are multiple owners, who is responsible for reporting for different section of networks?
- What is the responsibility of each component owner when something goes wrong?
- Negotiation of the KPIs of different network requirements and QoS.

Consider APIs

- For network management and performance monitoring tools.
- For device configuration, onboarding and management.
- For predictive maintenance.

Service providers and services

- 5G network services provided via the industrial operator, an MNO or a third party such as a network vendor.
- Edge computing on premises or off-premises but close to the premises, provided by an MNO, a third party or a hyperscaler cloud company.
- Network slicing-as-a-service: a private network could employ a network slice, or network slices to isolate different customers of the industrial enterprise. An MNO provides guaranteed QoS for the defined slices with robust data security and authentication.
- Managed services of the 5G network for the industrial enterprise.

Security and Privacy

- 5G networks have in-built security already.
- Does the industrial operator require all data to remain inside the premises for privacy?
- If a portion of the data generated can reside within the service provider's domain, then what security options are available?
- Does the organisation require role-based security and access for machines, devices or units? What is required beyond firewalls, user registration and video monitoring?

Management platform and visibility tools

- Management and ownership of different operational parameters (such as provisioning, monitoring, KPIs, resource allocation options, subscriber database location and management or device management) will have to considered.
- Understanding OSS/BSS management aspects of the industrial operation and responsibilities.

Private Networks ownership models

Decisions about how to approach a private network deployment model will be governed by spectrum availability, OT requirements and cost. However, in general, very few industrial enterprises have the necessary expertise in managing and maintaining cellular wireless networks, which encompasses:

- Assessment of radio coverage on the areas of operations.
- Maintaining the coverage.
- Monitoring and maintaining the hardware and software upgrades.
- Ensuring security against intrusion and other threats that do not require internal physical access.

Below are some options for deployment models:

Managed Services

Option A: An industrial enterprise specifies the service provider and vendors, and customised solutions based on its design requirements. A system integrator then builds the network. Maintenance may be negotiable among the integrator, the industrial enterprise and the communication service provider company.

Option B: An MNO-managed private network. In this case, the industrial enterprise may specify its choice of spectrum, any special vendor needs, required QoS for the services, monitoring tools, APIs and SLA agreements for different levels of failures etc. Some countries make private licenced spectrum available to industrial enterprises at a nominal cost, but this might be a low-bandwidth spectrum and the enterprise might need more spectrum to scale its operations, while unlicenced spectrum is not reliable for critical operations. In the USA, CBRS PAL is available in some regions. In other situations, when the industrial enterprise does not hold its own spectrum, it could potentially use MNO-provided mid-band or mmWave spectrums and managed services from local service providers.

Enterprise-run full service

A large enterprise may decide to install its own 5G network and manage its premises. This is not straightforward, because it requires experience in radio coverage, running the cellular networks, managing vendors, training employees and upgrading the software and hardware as needed. The overall cost of maintaining the network may be higher than with an outsourced approach.

Neutral Host Model

This is a deployment model where the industrial enterprise may take advantage of two different service providers to run its networks. For example, one service provider may manage the private networks and the other provider can take care of the PNI-NPN portion of the facility.

The following table (Figure 10) maps the ownership models of private network deployment among industrial operators, service providers and their ownership of the network components.

Figure 10 | Private network deployment models

Type of private networks/ ownership	Industrial enterprise roles	Service provider type and offerings	Service provider roles
Standalone non-public networks (SNPNs)			
Enterprise-managed SNPN	Provides requirements, vendors, device choices and networking space. May provide spectrum in some regions or ask for spectrum from a MNO	Not applicable	Not applicable
SNPN delivered as a managed service by an MNO	Provides requirements to the MNO	An MNO is hired by the enterprise to install, design and support the 5G SNPN. The MNO may need to provide spectrum and the deployment may use RAN sharing.	Managed service and provision of spectrum, as needed
SNPN delivered as a managed service by a third party, such as an equipment vendor, software or cloud vendors or an MNO	The enterprise may use spectrum it has licenced itself locally or it may use unlicenced spectrum, such as CBRS General Access	The third party provides software and hardware, radio and management of 5G SNPN, but it does not provide licenced spectrum	Managed service without licenced spectrum
Public integrated non-public networks (PNI-NPN)			
Managed by MNO	The industrial enterprise is responsible for providing requirements and space for on-premises servers and equipment. The enterprise may use RAN sharing from a MNO	The MNO and industrial enterprise decide the requirements and the MNO installs 5G components in PLMN or inside the enterprise premises as per an SLA. The MNO may provide RAN sharing feature and/or use network slicing (see deployment models section)	MNO fully managed or partially managed service for the 5G Network. MNO selects its vendors/partners
Or jointly by MNO and enterprise as per SLA	The enterprise and MNO may split the device management roles	An MNO might also provide edge services or other compute services through its partners/vendors	The enterprise and MNO may split the device management roles
Neutral host network (NHN)			
Hosted by an enterprise or MNO	The enterprise makes a decision on multiple operators or multiple types of private networks	MNO provides the 5G networks as requested by the enterprise. An MNO may allow other network operators to provide the network service using the MNO's physical resources	Managed service for the requested portion of the network

Source: GSMA Digital Industries

Neutral Host Networks

A neutral host allows multiple parties, such as enterprises, managed service providers and MNOs to leverage existing cellular networks to provide services to a venue or campus. A neutral host network (NHN) can be hosted by the enterprise itself or by a third-party MNO who has already been providing service to the enterprise. As shown in Figure 11, a NHN will allow other MNOs to support their devices inside the enterprise network. NHN can also serve as a logically separate network from another service provider.

An NHN can be configured using spectrum-based neutral hosts or multi-operator small cell networks sharing the same radio network resources.

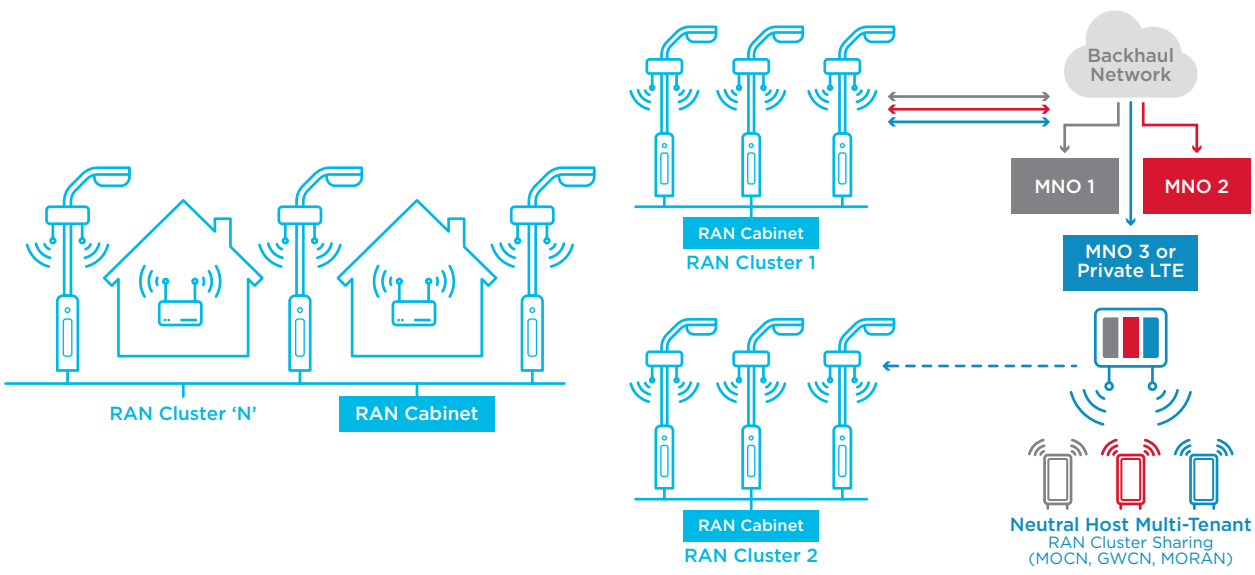
Neutral host networks are a business model which is deployed in multiple different ownership models in different parts of the world. In some deployments, neutral host networks are developed by landlords/owners, for example, of office sites, stadiums, ports and other venues that are willing to deploy a wireless indoor infrastructure on their premises. These organisations typically design and deploy the network architecture working with third-party system integrators and/or equipment vendors. Once the indoor network is deployed, typically jointly with Wi-Fi/WLAN, the landlord/owner offers the connectivity to either its internal workforce or rents it to external small and medium businesses (SMB). The challenge these NHNs face is typically getting access to wireless spectrum to operate these sites.

NHN deployment in UK

The following examples are from UK deployment experiences:

- Using an MNO's licenced spectrum, which requires a signed contract for NHN.
- Using MNO-shared spectrum (e.g. 3.8-4.2 GHz), which requires a signed contract and dual SIM devices to support this mode of operation (one SIM to access indoor and another SIM to access the outdoor MNO network).
- Using Ofcom's (the UK regulator) Shared Access licences (SAL) **[13]**, which provide for shared spectrum with limitations in terms of power and security (typically a small coverage area limited to a single base station).
- Using Ofcom's Digital Dividend spectrum (700MHz) – there are limitations in terms of bandwidth, which has an impact on data rates and coverage.

Figure 11 | NHN example in the 5GCity trial project, 5GPP **[14]**



Source: 5G-PPP

- Using 5G New Radio Unlicenced (NR-U) in unlicenced spectrum frequencies – there are trade-offs, such as a limited number of channels, limited coverage and limited data rates.

The deployment of NHNs can be driven by total cost of ownership (TCO) considerations, such as a desire to avoid vendor lock-in, extend 5G coverage in rural areas and the need for high-density coverage indoors.

NHN deployment in USA

In some regions of the USA, CBRS spectrum has general availability (CBRS GAA), as well as national spectrum (mid-band and mmWave) from the mobile operators, for industrial usage. Using neutral hosts, an enterprise or mobile operator can create multiple logical service networks, managed by different service providers. This is a cost-effective way of using the spectrum and resources. For example, part of the private network is using CBRS and part of the private network is using shared spectrum from an MNO. Alternatively, multiple operators can provide services through a small cell-as-a-service model, while using a single operator's spectrum **[15]** via a NHN service model.

NHN challenges for consideration

While a NHN brings cost efficiency, it also brings challenges in terms of who takes responsibility during a service failure, device installation, configuration, SIM card distribution etc.

Correct billing, payment and SLA maintenance among the multi-party system can also be a challenge and present an additional cost for an enterprise operator.

Examples of Private Networks suppliers

Private network suppliers vary in size and roots from different industries. They come from different backgrounds in terms of expertise and range from telco equipment vendors to start-ups and cloud vendors. Some of them have worldwide coverage with their service offerings, while others focus on specific regions only.

1. MNOs, including Verizon, AT&T, Telefonica, Orange, KPN, Deutsche Telecom and NTT Docomo, provide licenced 5G spectrum. Many of them provide or plan to provide private network (SNPN and/or PNI-NPN) solutions to enterprise customers.

2. Private vendors, such as CTS, Boingo and Betacom, offer products and services such as '5G-as-a-Service' (5GaaS).

3. Equipment vendors such as Nokia, Huawei, ZTE, Ericsson, Cisco, Samsung and Fujitsu also have 5G SNPN network products. Nokia and Ericsson have worldwide footprints and can access licenced spectrum through collaboration MNOs. Other vendors, such as Huawei and ZTE, have a significant presence in China providing services to enterprises.

4. Cloud providers (hyperscalers) such as Amazon Web Services, Google Cloud Platform and Microsoft Azure are offering 5G private network (SNPN) integrated with their edge computing solutions.

5. Chipset and module companies, including Qualcomm, NXP, Intel and ARM, are working with equipment vendors and communication service providers/MNOs to meet the requirements for 5G Industry 4.0.

6. Start-ups and small companies such as Cradlepoint, Sierra Wireless and Druid Software are offering 5G private networks, typically focusing on specific industries, based on their expertise in networking, infrastructure and system integration.

Private Network deployment models

Private Network deployment models

The primary private network business models (discussed in the previous chapter) allow for various deployment models, including:

- Fully dedicated/on-premises isolated network (full core and RAN), which are mostly deployed in critical environments where data cannot leave the enterprise's network. Examples exist in nuclear plants, manufacturing plants, ports and airports. Most NPNs are currently deployed following this model.

- Hybrid edge network with control plane and user plane on the customer premises and the management plane hosted by the service integrator or operator cloud. A cloud-based management plane, which is used to centralise configuration of user/subscriber data, health/performance log aggregation and dashboarding, can control several on-premises 5G edge cores on multiple remote sites. The link between edge and cloud is often restricted to management data only and is protected by high security standards, involving encryption, identity access protection and resiliency.

- Other deployment models are similar to a hybrid edge deployment, but full core network functions are on service integrator or operator networks, with only a user plane function (UPF) deployed on the edge following the CUPS (control and user plane separation) architecture. In this deployment model, the operator or systems integrator manages the full cloud core, which includes the control plane and management plane, while the data plane remains on the customer network and interfaces with the customer network through a UPF.

The radio access network can also be deployed in different ways:

- A fully dedicated RAN including basebands and radio units is deployed using dedicated fibre backhaul.

- RAN is shared: RAN sharing allows for a logical split in the radio equipment between several core networks. This is often used when the customer has a public MNO network on its premises and can segregate it between critical applications and public access.

- Neutral Host: this model involves the enterprise deploying its own infrastructure supporting multi-band capabilities and a dense network (with Dynamic Antenna System (DAS) or small cells). This infrastructure can host a single or multiple carrier frequencies and its own private network or a third-party private network. A neutral host can also be offered by a carrier.

Most of these deployment types are associated with specific financial models: capital-intensive where the enterprise invests in the cellular equipment and incurs management and maintenance OPEX, or a managed services model (OPEX only) where the equipment is rented. Third-party service providers tend to be flexible and will negotiate costs to meet different business needs. Small- and medium-sized businesses (SMB) may prefer to go with a reliable service provider to run their 5G private network as per an SLA. The financial models should also reflect the cost of a network failure and the practicality of managing multi-vendors for a private network.

Single-factory deployments

With the different deployment models described above, it is possible to deploy a NPN in a single factory, consisting of one building or shopfloor area, or several buildings within an enterprise's campus.

In the isolated model or in a hybrid cloud/edge model, the core network is on-site while the local RAN is deployed in one or more buildings.

The density of the radio network elements depends on the type of applications used, the required bandwidth and the number of endpoints served. Often a radio study/survey is required to calculate the associated link budget and used as guidance for the physical deployment.

A single factory model is generally used when the enterprise has only one factory (SMB) or during a pilot phase before scaling to other factories.

Multi-factory deployments

A NPN network can be deployed in multiple geographical locations. Again, the different deployment models described above will drive the associated design pattern:

Fully dedicated
A single 5G packet core can be used to manage the different factories from one centralised location. In this case, only a RAN network will be deployed in the satellite sites (managed by the central site). In the transportation industry, for example, a complementary edge appliance or local breakout solution (LBO) may be deployed on the remote satellite sites allowing for local transport of the data on the satellite site network. The edge or LBO solutions are used when a local data centre is hosting the local applications or to lower the overall latency.

Hybrid edge 5G
The centralised management plane, which is hosted in the cloud, manages the 5G edge cores deployed in each factory. The main difference with the previous deployment type is the fact that each factory has a complete 5G core centrally managed in the cloud.

Connected factories

In both cases above, the factories can be interlinked using an existing enterprise WAN or SDWAN backbone. The routing between sites is designed and managed by the enterprise or a system integrator/ communication service provider. A single-factory implementation and a multi-factory implementation could be interconnected and belong to the same SNPN network.

Though they are meant to be isolated, and no data plane is accessible from outside the SNPN, 3GPP may look into creating standards for SNPN-to-SNPN connectivity or SNPN-to-MNO Public Network connectivity and vice versa to support dual access to a user or sharing equipment on multiple sites. This communication can be provided securely by MNOs by packet routing based on the network ID assigned to the SNPN and with robust authentication methods when the user or device is registered with both the enterprise and the service provider's network. Wired connectivity routing technology already exists, but increasingly there is a need for wireless mobile device connectivity. In those situations, licenced cellular connectivity would be more reliable and secure than unlicenced wireless services.

Connected factories may require regional or international connectivity. Local and regional connectivity among the factories is possible via 5G wireless fixed access (FWA) or wired connectivity in order to handle security, bandwidth and speed. When the factories are placed in different countries, the local spectrum availability and policies may require adopting different private network deployment models in two different locations.

Identification of Private Networks

A private network is identified by a PLMN ID and a network ID (NID). MNOs can use an existing PLMN ID and add a NID based on their product needs. Routing between private networks takes place based on this identification.

3GPP agreed on two assignment models:

1. **Self-assignment**
   NIDs shall be chosen by SNPNs at deployment time from a selected number space as defined in 3GPP TS 23.003 (may not be unique and non-routable).

2. **Coordinated assignment**
   NIDs are assigned using one of the following two options:
   a. unique number independent of PLMN-ID.
   b. A combination of the PLMNID and NID which is a globally unique number.

Network selection for SNPN-enabled devices

3GPP TS 23.122 specifies that user equipment (UE) reads the PLMN IDs and list of supported NIDs from the broadcast message from the RAN. In the automatic network selection method, UE can select the correct PLMN ID and NID for the SNPN selection. With manual selection, UE is configured with a list of NIDs for network selection. A SNPN-enabled UE is configured with a subscriber identifier (SUPI) and credentials for each subscribed SNPN identified by the combination of PLMN ID and NID.

5G Private Network use case and deployment examples

5G Private Network use case and deployment examples

This section describes some use cases and deployments that represent different categories of usage. The following table maps each use case to a category of application in Industry 4.0.

Figure 12 | Example use cases mapped to deployment model options and application categories

Industrial use cases deployment using private networks	Deployment model options	Application Category	Comments
Automated guided vehicles Campus networks Industrial crane operation automation	SNPN, PNI-NPN option 2	Factory and process automation	Can be enhanced with edge computing, network slicing Requires mobility indoor and outdoor
Ports, Airports	SNPN and PNI-NPN depending on use-cases	Logistics, monitoring, tracking, data collection process automation	Will involve data collection across distributed operations and inter-private network connectivity Requires mobility, public-private network access
Smart tools, XR applications	SNPN, PNI-NPN option 2	Digital twin and human machine interface application automation	Requires on-site processing, storage, edge computing, low latency operation

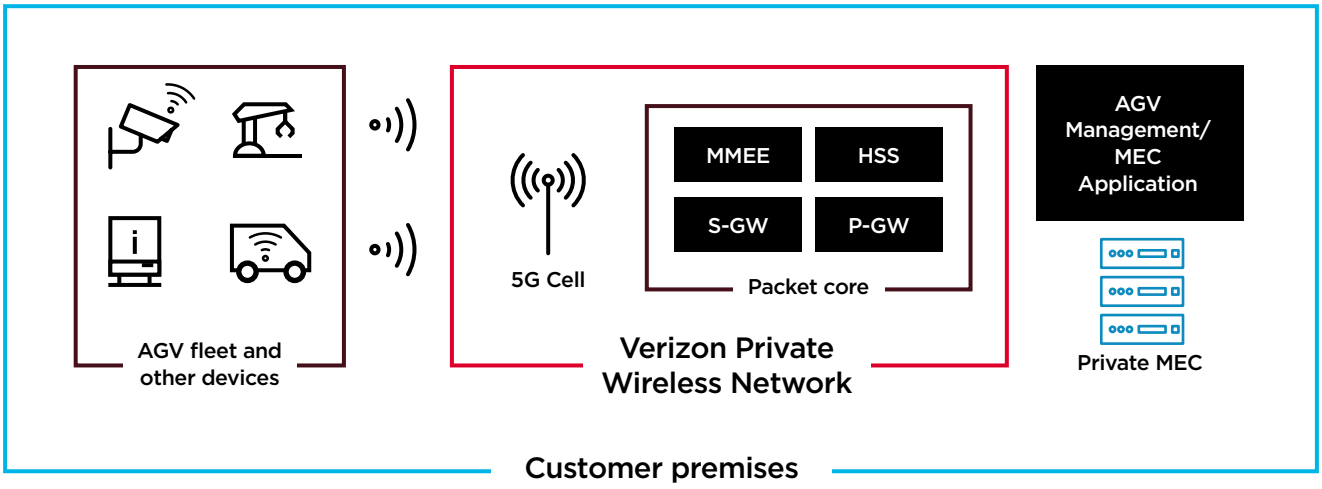
Note: The PNI-NPN options are described in 'Types of Private Networks' section on page 20.

Source: GSMA Digital Industries

1. Automated Guided Vehicles

Two types of Automated Guided Vehicles (AGVs) are used today: basic AGVs, which can carry light loads and might be used for inspections, and industrial heavy lifters. AGVs are often used along with LIDAR technologies to detect objects and measure distances from the object. Mapping technologies (for example, Simultaneous Localization and Mapping (SLAM)) can be combined with LiDAR to create a map of the environment and object location. Edge computing can be used to support the low levels of latency needed to manage an AGV or a fleet of AGVs. Figure 13 shows AGV service management via a 5G non-standalone private network with an on-premises edge computing infrastructure[2].

Figure 13 | AGV in SNPN using Edge computing



Source: Verizon

2 verizon.com/business/resources/solutionsbriefs/5g-edge-automated-guided-vehicles-agv-management.pdf

AGVs can be used with LIDAR, motion sensors and cameras to ensure worker safety in the manufacturing and industry areas. Workers may use helmets with sensors, which can interact with the AGV processors and on-site edge compute.

The AGV central manager in the edge computing platform can change an AGV's direction in less than 15ms to avoid a collision.

Figure 14 shows an Airbus AGV demo and trial at Airbus locations.

Figure 14 | Airbus AMR to transport tools in the factory

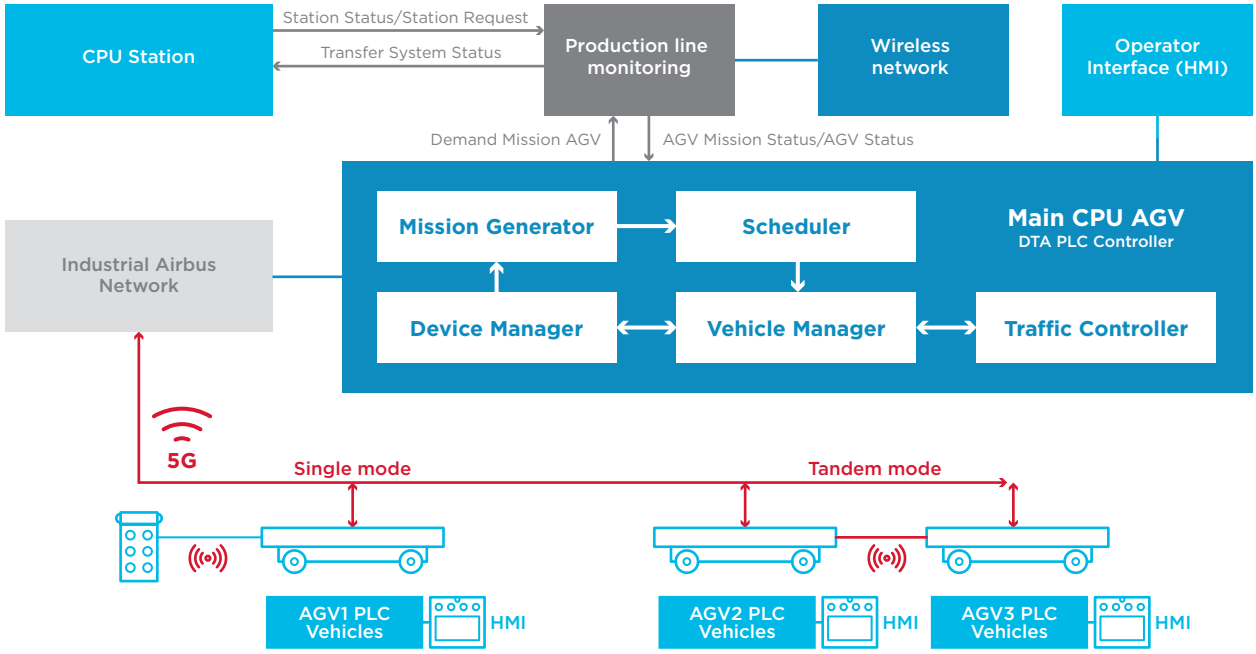
Source: Airbus

Requirements for AMRs and AGVs

AMRs (autonomous mobile robots) and AGVs are now often part of automated production lines in which several AGVs, robots, machines and operators are synchronised. In its basic configuration, 5G can carry a variety of OT protocols, such as Siemens S7, that are often used between several electromechanical processes programmed in PLCs (programmable logic controllers). This PLC-to-PLC communication over 5G allows for highly synchronised shop floor operations. Additionally, where industrial hangars are large, mobility management (handovers) between cells are improved with 5G (compared with Wi-Fi), allowing larger areas to be covered by the AGVs and resulting in fewer errors.

For some critical operations, multiple AGVs will synchronise to work in tandem, which requires very precise synchronisation over a time-sensitive wireless link. Advances in TSN (time-sensitive networking) with 5G will greatly help to achieve critical and deterministic industrial communications.

Figure 15 | AGV operations in time-sensitive applications



Source: Airbus

In Figure 15, 5G connectivity is used for the AGVs to communicate to the AGV supervisory and manager application. The performance, time synchronisation of the fleet of robots and other objects and latency can be improved by deploying TSN, and common management and control via a central guidance system, which may be located in the edge computing platform.

A common API is required to manage and control the AGV and AMR.

Today, AGVs work independently with their own management interface, without connecting to the central guiding system. However, connecting with a cellular 5G network for reliable packet quality and integrated edge computing will provide reliable and cost-effective AGV services.

Industrial AGV/AMR usually have four PLCs inside for different functions. They use proprietary protocols, which are difficult to configure. Using a remote central management system, and a common API, will resolve this issue.

In the future, a standardised common interface between the AGV/AMR devices and the central AGV management system application over a 5G network needs to be developed.

2. Industrial Crane project

An end-to-end 5G private network can be used to support an automated hoisting system.

Automated hoisting systems

Hoisting systems, such as cranes, are critical for transporting heavy equipment and materials over large distances, such as hundreds of meters. These machines are used in various supply chain and manufacturing operations from avionics and automotive to steel manufacturing and shipping, and sometimes in challenging environments such as extreme temperatures. Therefore, automating the operation of a hoisting system is important to ensure safety and efficiency.

Schneider Electric, Capgemini and Qualcomm Technologies have collaborated to build a 5G-enabled automated hoisting system for deployment across industrial and logistic sites. The technology was developed at Schneider Electric's hoisting lab in Grenoble by replacing wired connections in the industrial automation process with a private 5G network.

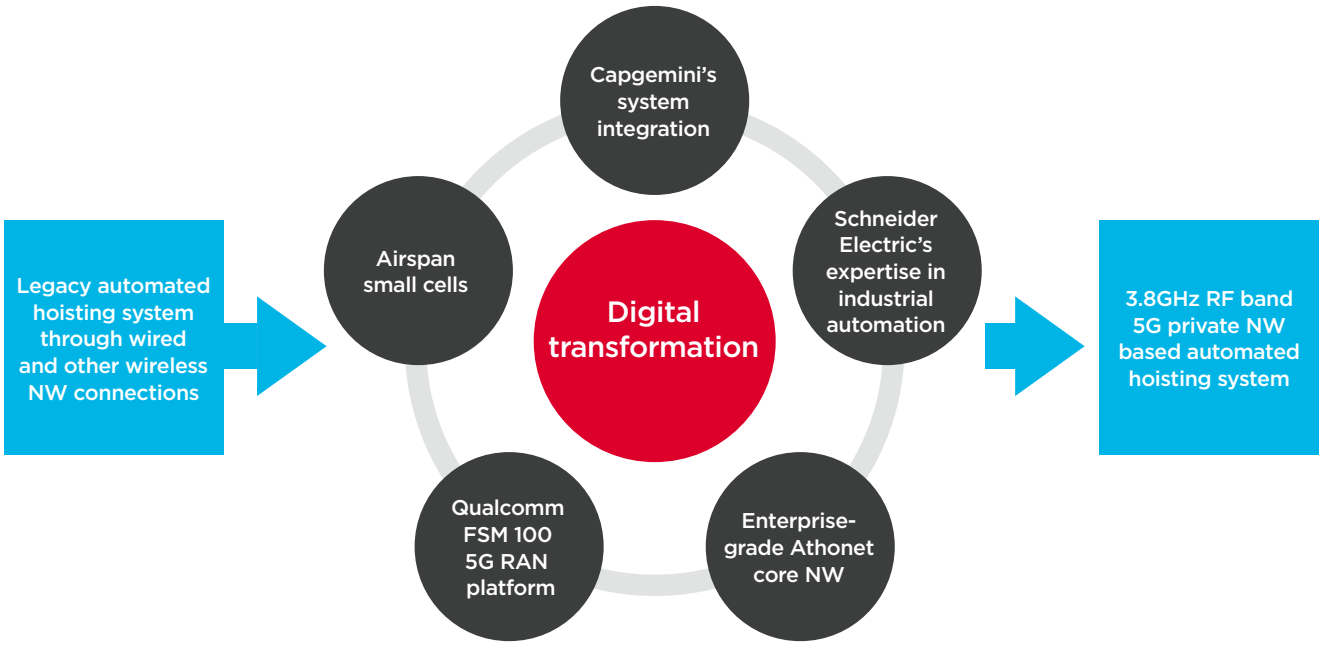
Digital transformation of an automated hoisting system

Automated hoisting systems increase productivity, safety and performance compared with manual systems, thus reducing operational costs and carbon footprint significantly. However, brownfield wire-connected setups are complex as several systems, such as heavy hoisting machinery, video cameras for monitoring and remote operation and PLCs for various control functions, are all connected through the same network. A precise, reliable and fast network connection, which is available 24/7 though the remote control-room and the overall hoisting system, is required.

5G's ultra-reliable and low-latency characteristics means the technology can be used to replace fibre cables in remote-control operations, addressing the need to simplify network complexity, reduce wires and provide long-term reliable connectivity. Capgemini has designed and deployed an optimised and automated hoisting system in collaboration with Schneider Electric using an end-to-end 5G private network (see Figure 16).

The partners are now investigating and deploying further proofs of concept to deliver additional digital use cases, such as augmented operations enabled by XR (extended reality) and wearable devices, in addition to the private 5G automated hoisting system.

Figure 16 | Digital transformation of automated hoisting system

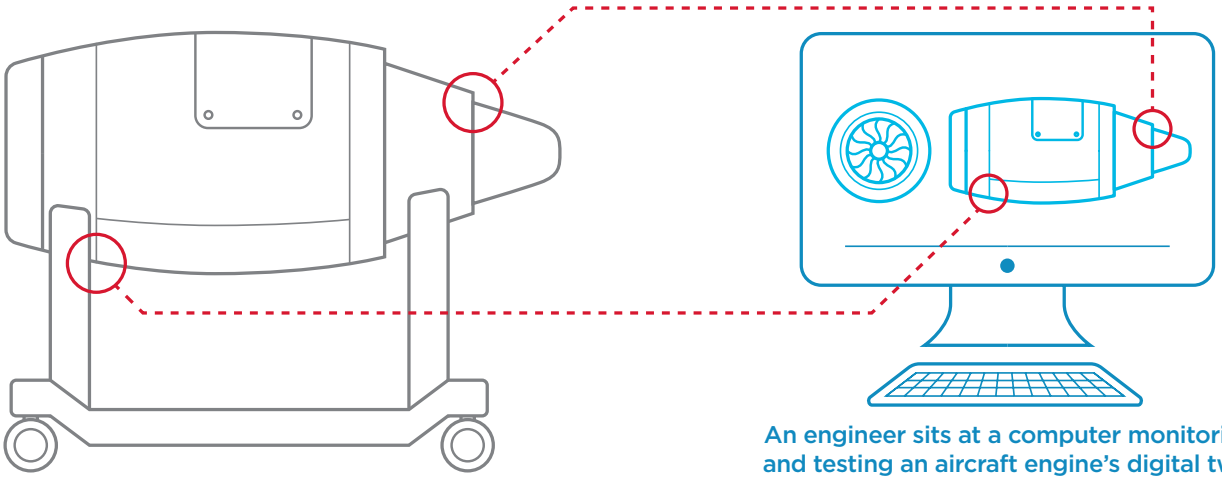


Source: Capgemini

3. Human Machine Interface: AI/ML and XR

A manufacturing facility could use AR/VR to interact with a digital twin – a digital model of a physical object that is used for designing, planning, training and debugging in the manufacturing process (see Figure 17). Using edge computing and AI/ML, data coming from the digital twin can be analysed in near-real-time and the related machine can be adjusted by a human or automatically through a control feedback system to change speed or move position in the production environment. This will reduce the production defects. The digital twin and AR/VR headset are used in conjunction for debugging and runtime movement and control of machines. 5G can provide low latency, reliability and time synchronisation. If video images will be used for analysis and detection, fast uplinks are required.

Figure 17 | Digital twin-based production quality



An engineer sits at a computer monitoring and testing an aircraft engine's digital twin

Source: Verizon

4. Human Machine Interface: Smart Tools

The manufacturing industry is piloting the use of 5G to wirelessly connect smart tools. A controller uses 5G to send the precise torque range and Newton force to be applied in the specific assembly area and bolt. In most industries, this is a very precise operation that requires insight into the operation quality. Therefore, feedback is also sent by the tool to the controller. The tool operator needs to be fully synchronised with the environment operator (position, accuracy), the tool user, the precise location of the operation and the manufacturing execution system, cascading down the configuration to be applied.

In general, these tools use 5G massive IoT communications to optimise the use of battery power, instead of an 'always on' connection.

A worker can also receive voice guidance over 5G in real-time from the OT system, allowing them to accomplish the operation safely in the right location with guidance and quality control. 5G allows better signal propagation in harsh environments and allows the use of smart tools in a more flexible manner and in places where it wasn't possible before with Wi-Fi.

Figure 18 shows an example of smart torque tool from a joint project with Atlas-Copco, Ericsson and Orange[3].

Figure 18 | 5G usage of smart tools in a factory

Source: Ericsson

3 ericsson.com/en/videos/2020/industry-connect-5g-ready-production-at-atlas-copco-airpower

5. Campus Networks

A campus network is a familiar concept in Europe where a single IT department provides a number of companies with network connectivity. With 5G private networks implementations, each factory or enterprise network is a SNPN and they can contain their own private 5G network or they may share a large private network. In another configuration, smaller enterprises may keep their own 5G data plane and RAN inside the enterprise but share the control plane with the common 5G service provider. In countries that will allocate landowners private licenced spectrum, a business may choose to use their own spectrum. Other enterprises may share unlicenced or licenced 5G spectrum.

Funded by the German Federal Ministry of Economics and Climate Protection[4], the 'CampusOS' project aims to build a modular ecosystem for open 5G campus networks based on open radio technologies and interoperable network components. This aims to create vendor independence and enable more competition and innovation. The partners in the CampusOS project intend to create a digital ecosystem that guarantees open radio technologies and interoperable network components. Deutsche Telekom, Bosch and several German companies are taking part in a project that aims to offer campus networks across Germany. Fraunhofer HHI and FOKUS are in charge of coordination of this network.

Figure 19 | 5G Campus Network in Germany (Deutsche Telecom and Bosch along with others)[4]

Source: RCR Wireless

4 rcrwireless.com/20220210/5g/deutsche-telekom-bosch-take-part-campus-network-project-germany

Figure 20 | The Smart Factory in Wichita, Kansas (Deloitte and Verizon along with others)

Source: Verizon

In the USA, a campus network typically means the IT network of a university or a company connecting its own buildings across the campus. However, in the model of European Campus Networks, Deloitte and ecosystem partners formed an initiative called Smart Factory@Wichita. Verizon teamed up with Deloitte[5] to provide 5G networks, connectivity, edge computing for mobility, low latency and coverage across the smart factory.

Participants include AWS, Siemens, SAP, DRAGOS, Infor, CheckPoint, HPE, ServiceNow, Tenable, UiPath, Canary, Drishti, Digital Immunity, Parsable, Elenco, Sewio and GuardHat, with Verizon serving as the connectivity backbone. They have defined eight industrial use cases including increasing efficiency on factory floor operations, energy efficiency, automated inspections and AGV control.

Figure 21 | a) Workforce training through AR/VR
b) Automated warehouse operations using the Private 5G Network

Source: Verizon

5 rcrwireless.com/20230109/5g/verizon-turns-on-private-5g-for-deloitte-backed-industry-4-0-showcase-at-wichita-state

6. Logistics and aviation

Smart ports

Smart ports are equipped with sensors, cameras, tablets and smart scanners all connected with a network infrastructure. 5G connected ports can provide reliable connectivity, security and mobility of shipping goods from containers to cranes to ship.

Associated British Ports (ABP), the largest port operator in the UK which handles £40 billion of exports, 600,000 vehicles and millions of cruise passengers annually, has worked with Verizon to integrate a private 5G network with the port infrastructure and various devices such as scanners and containers. The network enables ABP to collect data from its daily operations via inspector drones and tablets, sensors and tags and then use AI/ML functions to create a simulation of the real port for future design and business improvement, as a first-use case.

A smart port can address multiple business problems, such as:

1. Pallets are grouped by destination in the shipping area and loaded one by one on the dock that corresponds to that destination. However, there is no system to raise an alert if a pallet is loaded in the wrong dock. One solution is to monitor each dock with an aerial camera. A barcode is read at the top of the pallet by the camera, which verifies that the destination is correct for that dock and time slot. In case of error, a SMS is sent to the logistics manager.

2. Continuous pallet movement in the shipping area causes floor occupancy to fluctuate constantly. One solution is to use 5G-connected cameras to detect changes in the free/occupied space on the floor of the shipping area throughout the day in real-time and analytics provide the following information:

- Which packages are in the wrong location?
- What is the best route to store packages?
- What is the best location to store a package in each area?
- How to optimise space and volume in storage areas

Figure 22 | ABP Port is using a Verizon 5G Private Network

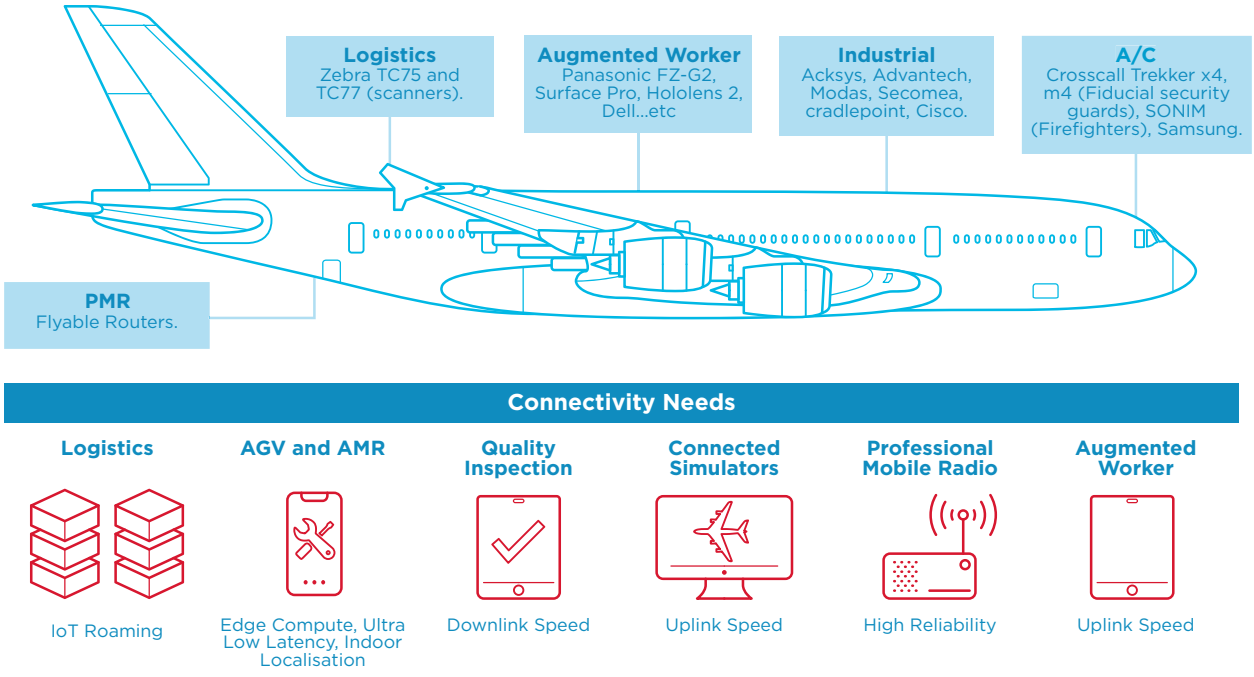
Source: Verizon

Aviation

The aviation sector is using private networks for certain operations that require high bandwidth, local applications, immediate response, visual inspections and making decisions on defects. Figure 23 and Figure 24 show how Airbus is using 4G/5G devices and different applications for the manufacturing factory, design, testing and production phases. Airbus has different requirements for each of its production and assembly lines. A combination of private networks and public networks is required. In addition, it has multiple factories in different locations, which need to be connected. High downlink and uplink speed are required for the automation of aviation industry manufacturing and maintenance operations. Ultra-low latency and reliable connectivity, edge computing, indoor positioning and IoT roaming are also required.

5G connectivity can also be used for in-service and manufacturing inspection processes connecting with the devices, workers' tablets and sensors through 5G wireless for efficient and fast resolution[6].

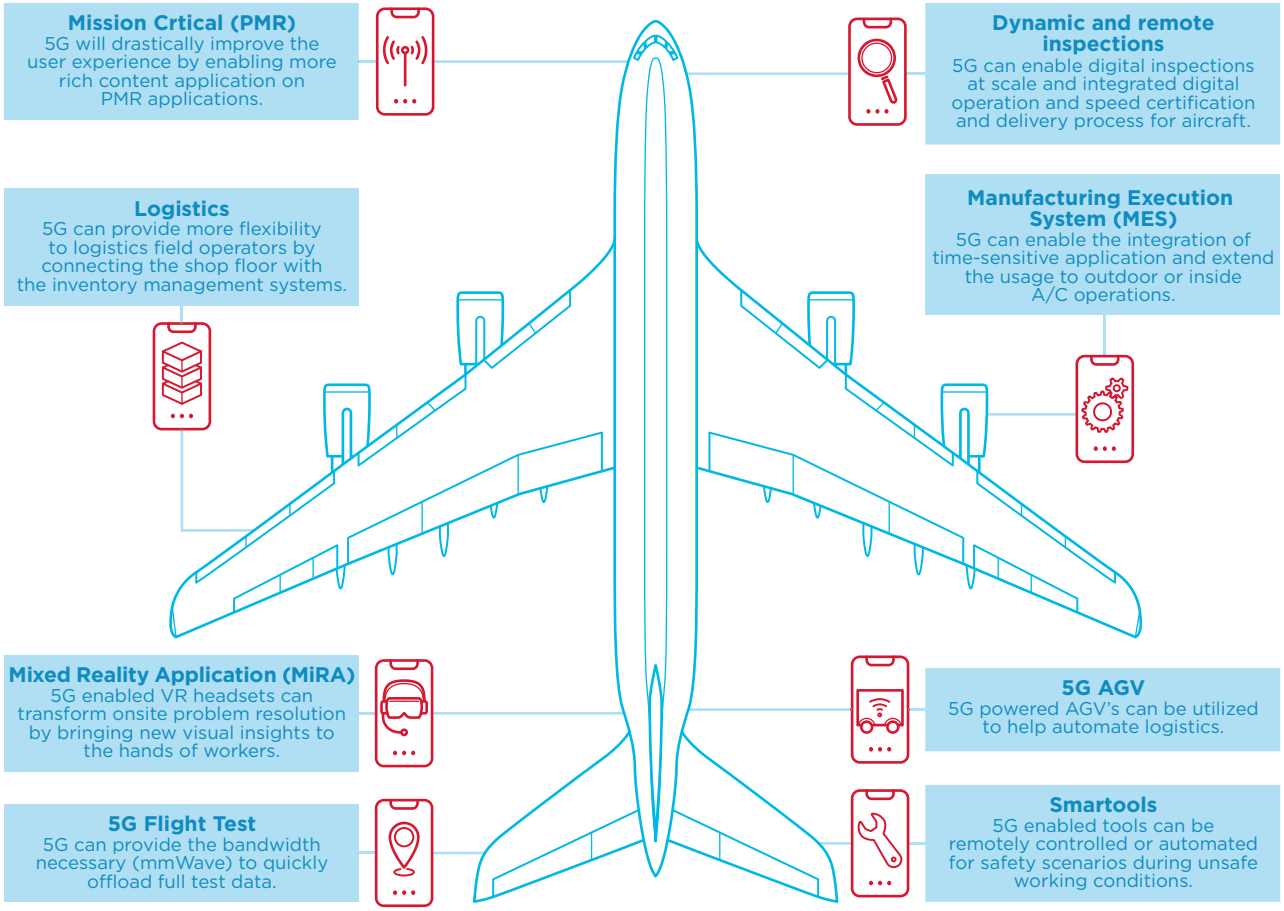
Figure 23 | Airbus 4G/5G devices, applications and connectivity needs



Source: Airbus

6 testia.com/we-inspect/manufacturing-inspection

Figure 24 | Airplane building processes and operations



Source: Airbus

5G Private Networks and Edge computing

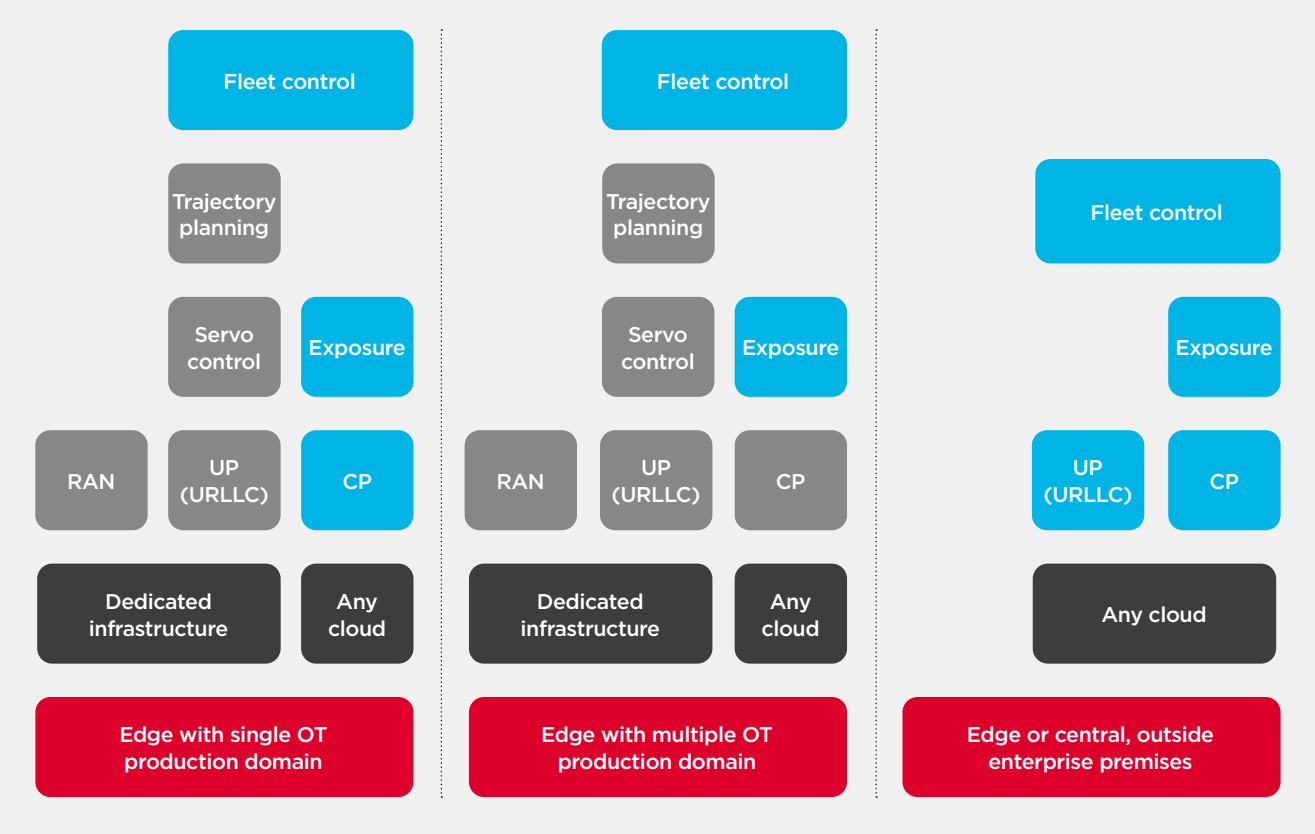
Edge computing in Private Networks

Industrial networks can support many different use cases, including critical applications such as motion control, workers' safety, extended reality and large sensor data aggregation which require very low latency and, in some cases, high-bandwidth operations. That requires in-factory computing infrastructure or a nearby computation facility offered by a service provider.

Other edge computing use cases include AGV control, digital twin-based training, debugging, production control, AI/ML and position-based tracking of moving assets etc. All of these use cases also require private edge computing or a public edge near the facility. Both public and private edge cloud services are offered by mobile network operators, while third-party 5G network providers also offer a smaller version of local edge compute and hyperscalers (AWS, Microsoft, Google etc) are integrating their solutions with MNOs' private and public networks.

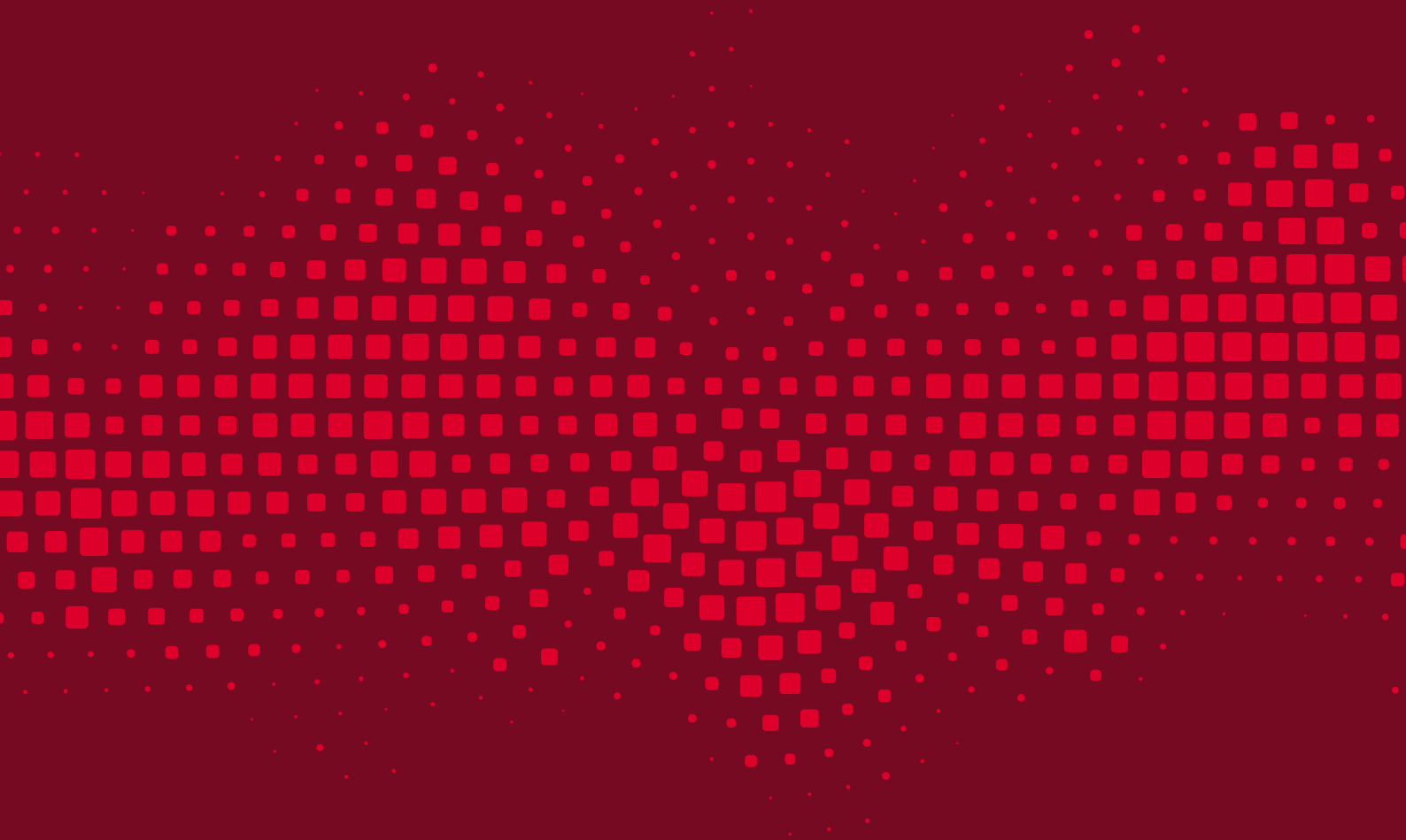
Figure 25 is sourced from the 5G-ACIA white paper on edge computing use cases, requirements and deployment **[16]**. It shows a few examples of applications and operations that can run on different edge locations, including a dedicated infrastructure on-premises.

Figure 25 | 5G-ACIA recommended edge computing deployment options



Source: 5G-ACIA

Private Networks Requirements



Brownfield considerations

GSMA Digital Industries has worked on a brownfield migration strategy **[17]** and document which provides guidelines for IT and OT integration to transition from an industrial operational network running on Ethernet and traditional proprietary protocols (such as PROFINET, CCLINK etc.) to a 5G TSN and other modern technology applications, such as XR/VR and digital twins. The document also covers how to interoperate with the legacy devices, protocols and existing Ethernet network through 5G bridges.

Considerations:

1. A private network, especially if it is SNPN and isolated, may not be able to connect with the legacy networks and devices if they are not co-located and inside the private network.

2. Integration with existing technologies, such as Wi-Fi or LTE private networks.

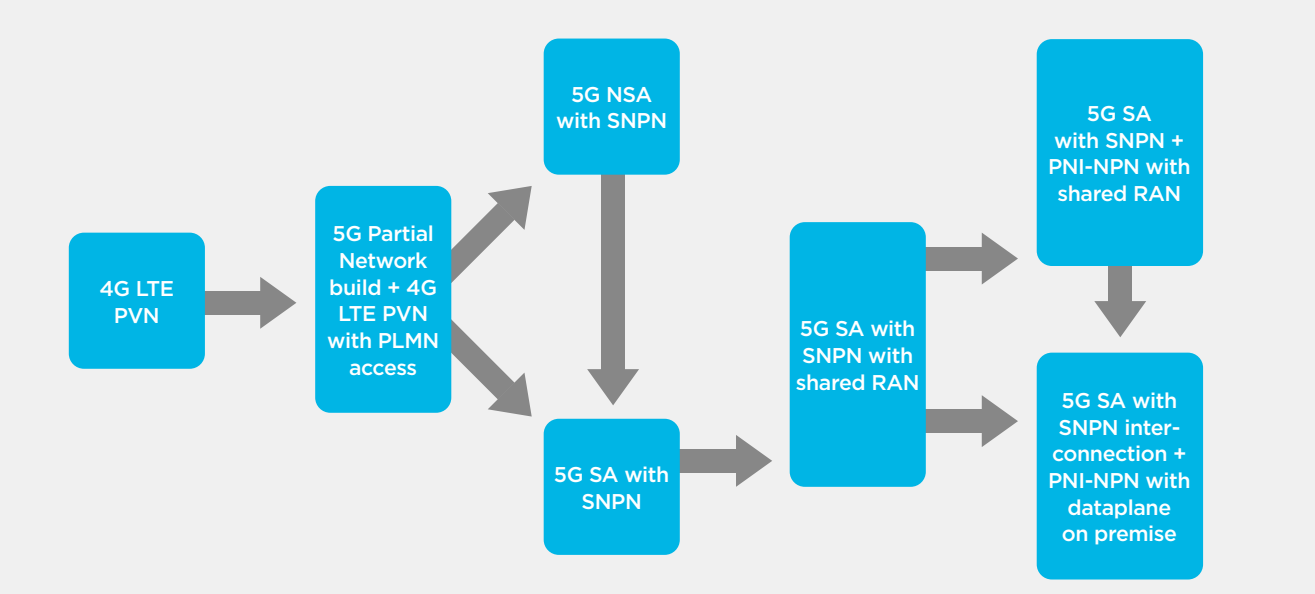
Suggestions:

If connecting with a legacy network is an issue with an isolated SNPN, it is better to co-locate the legacy network with the SNPN. Otherwise, a PNI-NPN will be helpful to transfer data over 5G network.

In a factory, the IT domain typically uses Wi-Fi for non-critical operations and enterprise use. While it makes sense to migrate Wi-Fi devices to 5G-enabled devices to connect with a 5G private network, it may also make sense to find a solution in the 3GPP future standards to interoperate with Wi-Fi devices in a legacy network. However, it might be cheaper to move all the domains of an OT network to a single 5G SNPN or PNI-NPN, or a combination of both, to avoid interoperability issues.

Figure 26 shows potential options for migration from a 4G LTE private network to a 5G private network.

Figure 26 | A gradual approach for private network migration from 4G to 5G



Source: Verizon

Network Requirements

Configuration options

The configuration requirements of 5G private networks in different deployment models are discussed in 3GPP TS 23.501, 3GPP SA5 documents. Most 5G network providers offer an orchestration portal for easy configuration interfaces where the user provides the base requirements (device capacity, security algorithm choices, type of network, device type, network options, L2/L3 interface, network slice type, QoS choices, etc.) and the network configuration takes place behind the scenes. Each provider may require different user input data and have a different display portal, so it is best to consult the provider's configuration portal during the planning phase.

5G system upgrade and maintenance

Typical requirements for software and system upgrades in SNPN and PNI-NPN deployment models should include the upgrade process, approximate downtime or fall-back mechanism during upgrade, OTA upgrade options and the testing procedure before bringing the system backup. A maintenance plan should be discussed as part of the SLA agreement.

Vendor interoperability

Vendor 3GPP compliance certification **[18]** for 5G is required and RAN and core API options should be considered for integrating the provider network with user applications. If edge computing is used, the API options to communicate with the edge applications must be considered.

Network visibility by the user is required for performance, analytics and reporting. 5G core function NWDAF can analyse the network packets and send data to the cloud analytics system or to local applications for receiving trigger feedback after the analysis. This can help service providers to improve network services or correct the operation in near-real-time to meet bandwidth, packet loss, latency and jitter requirements.

QoS and SLA

A service-level document needs to be translated into network KPI and QoS parameter requirements for RAN, core and edge computing functions. In industrial networks, each use case has different requirements on latency, aggregation, packet loss, time synchronisation etc. These requirements should be laid out together by the enterprise and the provider of the private networks.

Network Slicing Requirements

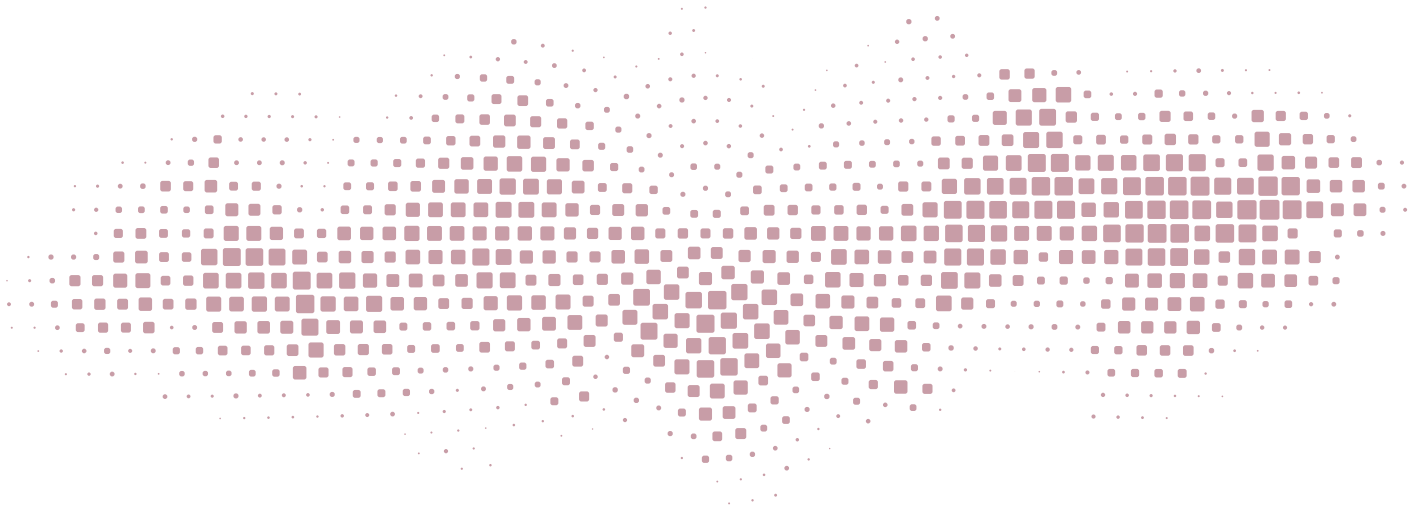
From the configuration of a network slice to its maintenance, ensuring QoS requires a KPI range for latency, bandwidth and other parameter requirements. The enterprise and network provider must discuss use cases and possible network slice type and monitoring options etc. The GSMA has published a document guideline on end-to-end network slices **[19]**. Section 3.7 of this document discusses industry customer management and section 3.4 talks about API exposure options. Network function virtualisation orchestration (NFVO), network slice management function (NSMF) and network slice subnet management function (NSSMF) facilitate isolation of multi-tenancy in such a manner that individual slice customers are able to operate their network slice instances with complete independence. The industrial customer may use different network slices for different types of network operations bounded by different KPI requirements on bandwidth, URLLC and TSN requirements. MNO-provided slices should be secured end-to-end with a 3GPP-defined authentication mechanism.

Device access and addressing

The device ecosystem for industrial private 5G networks has yet to develop. The devices need to consider registration with private networks (local private and/or MNO) and should be able to auto-configure with minimum human interaction. Device access to a SNPN or PNI-NPN are subject to authentication and authorisation on the respective networks and their sub-networks. Role-based authentication may also be required.

SNPN-enabled devices are also configured with subscription data for their usage on behalf of the organisation and they are either configured with the network-ID(s) of the SNPN or they should be able to automatically select a SNPN through the network operator's RAN. The device registration information may stay with the SNPN only or the device could have double registration with the SNPN and PLMN network. A SNPN device may be configured to access multiple SNPNs at different times.

Device addressing should be assigned by the private operator's 5G network core functions and the user database or the device addresses are assigned by the PLMN network for the private network in the PNI-NPN model. Details of device address management are defined in section 5.8.2.2 of 3GPP TS 23.501.



Dual SIM and eSIM profile considerations

The eSIM working group in the GSMA keeps updating the eSIM specifications to satisfy the market needs. They have started working on in-factory profile provisioning of consumer and IoT devices and the first requirement specification will be available later in 2023 as SGP.41. In-factory profile provisioning will help with simplifying the provisioning of profiles during the manufacturing device process.

A dual SIM may be used for the devices that access multiple private networks but, for cost efficiency and automation, an eSIM is recommended as an eSIM currently allows to store multiple profiles and switches between the profiles as required. Additionally, option such as a dual USIM may be available from some providers. Dual USIM is programmed with two profiles and it can switch to the appropriate profile when it moves to a network with different PLMN-ID or SNPN-ID.

Scalability considerations

Scalability is always a design choice for private networks. Virtualisation in a 5G system, including separation of RAN data and control units, can support scaling. The bandwidth of the available spectrum must also be considered when increasing capacity and serving a number of demanding applications in an industrial private network.

Isolating different types of applications' usage and using AI/ML technologies to understand network usage of these applications may be useful when planning how to scale the network.

Mobility inside private networks and access

Private networks are often used to connect mobile devices (such as cameras, AGVs, trolleys and wearable 5G devices) which will move from place to place within a factory and may require access to public networks.

Depending on the use case, a private network can have its own mobile network code (MNC) to enable it to operate standalone using shared licences from an MNO. As discussed previously, a standalone network can handle traffic locally, provide a URLLC capability on-premises and local data storage through a private cloud for data privacy and integrity. For example, in the mining sector, automated drills may only need to operate in a designated coverage area and require local access to datasets. However, autonomous vehicles may require access to multiple sites of the mine. These sites can belong to the same MNC and use the same data path as other sites. Where devices require both private network and PLMN network access, multi-profile eSIMs can support these use cases.

Mobility of IoT devices between a private and public network will require either a dual SIM (one registered for private networks and another for the PLMN) or dual USIM with multi-profile (one for private and another for public networks), which will be auto-switched during the transition. In future, multi-profile eSIM will be appropriate for the device mobility.

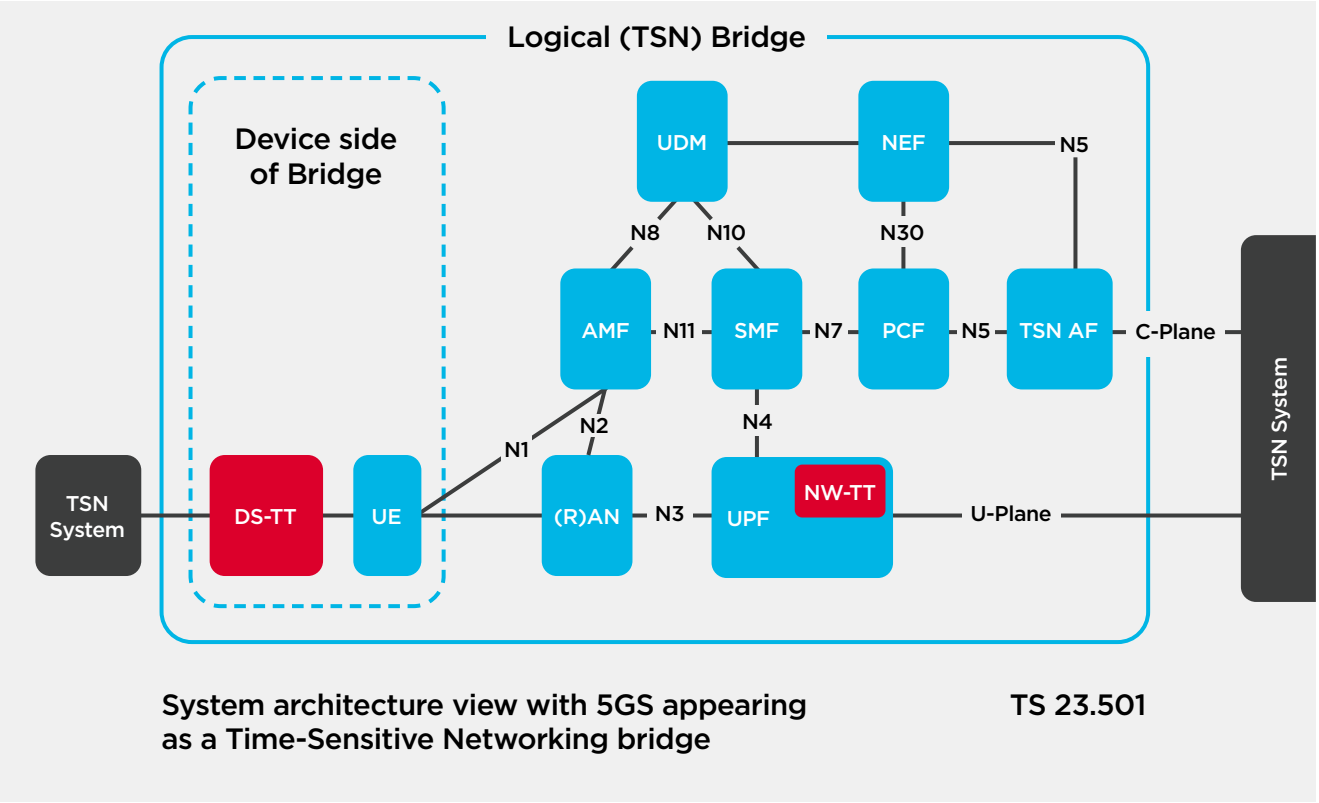
If mobility takes place within the campus network under the umbrella of the SNPN network, then the user equipment will need to selectively attach with the radio base station for destination SNPN NID, among the list of available and approved SNPN NIDs.

Mobility is easier to handle for devices in the PNI-NPN deployment model because the mobility of the device can be triggered the right radio network.

TSN Requirements

Time synchronisation and time-sensitive communication is an important feature in industrial networks. TSN is used over ethernet in industrial applications today and, with the help of TSN translators, a 5G system can act as a bridge (see Figure 27) to carry legacy TSN packets to the 5G-enabled devices or the mechanism can support communication between two different legacy TSN devices or controllers.

Figure 27 | TSN enabled devices connecting to the TSN system over 5G acting a bridge



Source: 3GPP TS 23.501 **[12]**

Private Network security requirements

A 5G network has in-built security and private network security has been considered in TS 33.501. 5G-ACIA **[6]** has published a paper on industrial security as well.

Traditionally, manufacturing environments are isolated physically and wireline connected; thus, it is secured from outside access.

With a 5G and wireless environment, factories and industrial private networks can be isolated logically through filtering, radio shielding and firewalling from outside attacks. Network operators and service providers have mechanisms to restrict access to the RAN using a closed access group for permitted users and devices.

There are also different separation domains with private networks, such as a production domain, an IT domain and a public domain, which can each operate their own security policies.

A SNPN configuration may also protect data because it does not go out of the campus. However, SNPN configuration needs to make sure there is no leakage of spectrum outside the premises. It also assumes there are adequate physical controls for site access.

PNI-NPN (option 1 – fully remote managed service) uses network slicing, which can be protected by the end-to-end network slice security in 3GPP R16. Thus, a network operator's network is maintained with high security for each enterprise operation. With virtualisation, it is possible to apply different security policies in isolation for each private network service. Some countries require lawful intercept and emergency connectivity for the NPNs, which are usually well covered by private networks offered by MNOs.

PNI-NPN (option 2 – some on-site deployment) also keeps the network data and storage on the premises and it does not go out of the enterprise production domain. At the same time, the devices are registered securely with 5G authentication mechanisms and it is as private as an SNPN configuration.

However, traditional OT devices and methods of operations should be revisited in light of 5G security requirements and those devices and platforms should be 5G security-enabled and protected from hackers' attacks. Thus, when designing private networks, one should carefully consider the security features of the 5G private network service provider.

Conclusions

Private Network deployment choices

- The roles of OT and ICT should be evaluated during the planning phase based on the size of the industrial enterprise and operational cost. This will determine what kind of service providers are appropriate for a private 5G network.

- Take into consideration the spectrum availability in the region and how much spectrum bandwidth is needed for the proposed operation. For example, mmWave spectrum can carry high-bandwidth data, but it may face interference issues due to the presence of metals in the factory (some operators can mitigate those issues). Normally, mid-band is a safe choice, but it doesn't have as much bandwidth as mmWave. One option is to use mid-band for most industrial applications and then add mmWave for certain operations as needed.

- Isolated SNPN networks may feel secure, but there is typically a practical need to connect to entities outside the premises to support mobile wireless devices. Enabling access to a wireless public network can act as a fallback, or for emergency operation, or for data analytics in the cloud. A combination of SNPN and PNI-NPN will provide convenience and long-term stability of the network.

- Ease of maintenance and managing the 5G networks are essential. Visibility of the private networks and monitoring tools is required for smooth operations.

- APIs are important for connecting OT applications to the 5G exposure system and edge computing infrastructure. Furthermore, tapping into the NWDAF data through an API call may be useful for the industrial enterprise.

- Cost models for the enterprise can be built with the available 5G service provider choices. The model should consider the costs of failure, debugging time, risks of production time loss, and resource and training expenditures in decision-making. Most small- and medium-sized industrial operations will benefit from MNOs' experience in radio coverage and providing private networks-as-a-service.

References

Ref	Document reference	Title
[1]	GSMA Industrial IoT Private Networks - 2020	5G Private and dedicated Industry 4.0 Network
[2]	NG123-v2.0	5G Industrial Campus deployment guideline
[3]	gsma.com/iot/resources/5g-wifi-industry40/	5G for Industry 4.0 Operational Networks
[4]	5gamericas.org/wp-content/uploads/2020/10/InDesign-5G-Technologies-for-Private-Networks-WP.pdf	5GAmericas White Paper on Private Networks
[5]	techblog.comsoc.org/wp-content/uploads/2022/03/Untitled-5-e1647231656808.png	IEEE COMSOC projection
[6]	5g-acia.org/wp-content/uploads/5G-ACIA_WP_5G-for-Automation-in-Industry_SinglePages.pdf	5G-ACIA Whitepaper, 5G for Automation in Industry, July, 2019
[7]	5G-ACIA White Paper, 5g-acia.org/resources/whitepapers-deliverables/	5G for Connected Industries and Automation, ZVEI, November 2018
[8]	5g-acia.org/wp-content/uploads/5G-ACIA_5G_Non-Public_Networks_for_Industrial_Scenarios_09-2021.pdf	5G-ACIA Non-Public Networks White Paper
[9]	3GPP note on 5G-for Industry 4.0	5G for Industry 4.0, May 13, 2020
[10]	3GPP pCR S5-211283rev1	RAN sharing concepts
[11]	5g-acia.org/wp-content/uploads/5G-ACIA_WP_Integration-of-Industrial-Ethernet-Networks_SinglePages.pdf	5G-ACIA White Paper on Industrial Ethernet Integration with 5G introduction
[12]	3GPP TS 23.501	System Architecture for the 5G System
[13]	ofcom.org.uk/manage-your-licence/radiocommunication-licences/shared-access	UK Ofcom shared access model
[14]	5g-ppp.eu/5gcity-enables-smart-cities-with-5g-neutral-host-vran-architectures-based-on-acceleran-drax/	5GPP Neutral host deployment example in a smart city project
[15]	celona.io/cbrs/what-is-a-neutral-host-network-how-to-build-one	Neutral Host Network introduction
[16]	5g-acia.org/whitepapers/industrial-5g-edge-computing-use-cases-architecture-and-deployment/	5G-ACIA Whitepaper, Edge Computing Use cases, requirements and deployment architecture
[17]	GSMA | Industry 4.0 (I4.0) Brownfield Evolution Framework 2023 | Internet of Things	Industry 4.0 (I4.0) Brownfield Evolution Framework 2023
[18]	globalcertificationforum.org/	Global Certification Forum
[19]	E2E Network Slicing Architecture NG.127-v1.0-1	GSMA E2E Network Slicing Architecture

Further reading

Document reference	Title
3GPP note on 5G-for Industry 4.0	5G for Industry 4.0, May 13, 2020
3GPP TS 23.501	System Architecture for the 5G System
3GPP TS 23.502	Procedures for the 5G System (5GS)
5g-acia.org/wp-content/uploads/5G-ACIA_5G_Non-Public_Networks_for_Industrial_Scenarios_09-2021.pdf	5G-ACIA Non-Public Networks Whitepaper
gsma.com/futurenetworks/ip_services/understanding-5g/5g-mmwave/	5G mmWave
gsma.com/futurenetworks/resources/advancing-the-5g-era-benefits-and-opportunity-of-5g-advanced-whitepaper/	5G-Advanced White Paper
globalcertificationforum.org/	Global Certification Forum

GSMA™

GSMA Head Office
1 Angel Lane,
London,
EC4R 3AB,
United Kingdom
Tel: +44 (0) 20 7356 0600
Fax: +44 (0) 20 7356 0601