SAMSUNG

Technical White Paper

Private Networks Vol.2

Architectures and Features for Industrial Scenarios

Oct 2021

Contents

Abbreviation

3GPP	3rd Generation Partnership Project
5GC	5G Core
AI	Artificial Intelligence
CAG	Closed Access Group
CBRS	Citizen Broadband Radio Service
CoMP	Coordinated Multi-Point
COTS	Commercial off-the-shelf
CU	Centralized Unit
CUPS	Control User Plane Separation
CW	Contention Window
DL	Downlink
DNN	Data Network Name
DoA	Direction of Arrival
DU	Distributed Unit
eMBB	enhanced Mobile Broadband
EPC	Evolved Packet Core
ID	Identifier
IEEE	Institute of Electrical and Electronics Engineers
IIoT	Industrial IoT
IoT	Internet of Things
LAA	License Assisted Access
LAN	Local Area Network
LBT	Listen Before Talk
LTE	Long Term Evolution
MCS	Modulation and Coding Scheme
MEC	Multi-access Edge Computing
MIMO	Multiple Input Multiple Output
mMTC	massive Machine-Type Communication
mmWave	millimeter Wave
MNO	Mobile Network Operator
MOCN	Multi Operator Core Network
MORAN	Multi Operator RAN
NID	Network ID
NPN	Non-Public Network
NR	New Radio
NR-U	NR Unlicensed
NSA	Non-Standalone
PDCP	Packet Data Convergence Protocol
PLMN	Public Land Mobile Network
PNI-NPN	Public Network Integrated NPN
PRS	Positioning Reference Signal
RAN	Radio Access Network
RTT	Round Trip Time
QoS	Quality of Service
SA	Standalone
SDN	Software Defined Network
S-NSSAI	Single Network Slice Selection Assistance Information
SNPN	Standalone NPN
SR	Scheduling Request
ToA	Time of Arrival
TSN	Time Sensitive Networking
UE	User Equipment
UL	Uplink
URLLC	Ultra-Reliable Low-Latency Communication

Introduction

Industries and businesses are undergoing an unprecedented digital transformation driven by the adoption of cloud-native applications and services, internet of things (IoT), analytics, artificial intelligence (AI), augmented reality and blockchain. While the degree of implementation of these technologies varies across each industry or business, one common factor stands true across the board - the need of mobility while providing a fast and stable network.

A 'private network' is a corporate network that provides communication connections to users or devices belonging to a private enterprise or organization, while offering specific application services tailored to each business needs. For industrial applications, the ability to design mobile networks to meet the reliability, latency, and security requirements of critical applications is fundamental to the new wave of cyber-physical systems known as Industry 4.0 – industrial IoT (IIoT). The stringent requirements of each industry cannot be met via traditional Ethernet or Wi-Fi, which are technologies accepted across the industry. Wired Ethernet is economical and stable in terms of performance and quality but limited in mobility since it is wired. Wi-Fi is easy to build and operate, but in terms of communication performance - such as connectivity distance, latency, mobility, and security - it is not enough to meet the requirements for enterprise digital transformation.

Considering this existing mode of operations, a mobile communication network that can overcome the limitations of traditional Ethernet and Wi-Fi networks gives private networks the competitive edge to optimize their business. Further, the importance of the private network allows its requirements to be addressed directly by the 5G specifications. It enables the technology to meet the requirements of private networks and facilitates innovation, competitiveness and agility in the enterprise business.

One of the biggest motivators that private '5G' attracts attention over the previous generation of mobile communication is that the appearance of new 5G frequencies to establish private 5G networks in enterprises have been introduced. These are allocated separately for private networks, not a licensed 5G frequency that governments have sold to mobile operators at high prices through auctions. The new 5G frequencies for private networks uses are expressed in various terms such as unlicensed, private, local or shared frequencies like the citizens broadband radio service (CBRS) as a primary example.

Moreover, key use cases of 5G technology represented by ultra-reliable low latency communication (URLLC), enhanced mobile broadband (eMBB), and massive machine-type communication (mMTC) drive the 5G innovation into industries such as smart factory, transportation, logistics, smart hospital and so on. Network slicing, which is one of most significant features of 5G, creates a variety of logical networks dedicated to the needs and use of private networks that may be different from public networks, enabling the creation and provision of services optimized for the private network. The virtualization and cloudification of network functions in 5G enables 5G networks to run via software on general purpose hardware. The mobile netwoks implemented with software – that are not tied to expensive dedicated hardware equipment - make it possible for private network customers to reduce the cost and increase efficiencies in deployment and operations.

5G continues to innovate in the radio access domain and system architecture to better meet the requirements of high-performance industrial applications. Various use cases of a private 5G network and its benefits can also be seen in [1]. The purpose of this white paper is to show that the private 5G network can achieve predictable and reliable performance which Samsung has the capability to build for its private network enterprises. To that end, this paper explores the ways in which enterprises and organizations can deploy and operate private networks, and introduces the innovative 5G technologies that enable the deployment and high performance required in private networks. Then, we describe Samsung's Private 5G Solution, which provides an end-to-end solution for private networks

Architectures of Private 5G Networks

A public mobile network is typically deployed and operated by public mobile network operators (MNOs) on licensed spectrums. In the case of a private network, however, the ownership of deployment and operation can be transferred from the MNOs to the enterprise that requires the network and can be deployed even on unlicensed spectrums, independent of the public network. Deployment types of the private 5G networks are largely divided into the following two categories depending on whether or not there is dependency on the public network.

Independent network - standalone private networks that are isolated from a public network

Dependent network - private networks deployed in conjunction with a public network as the following

① Private Network Sharing RAN

② Private Network Sharing RAN and Control Plane

③ Private Network Deployed in Public Network

Independent Network

A private network is deployed as a standalone network that is – physically and logically - isolated from a public network, in this deployment scenario. Moreover, the standalone private network can be completely isolated from the public network using local 5G spectrum rather than an MNO's licensed spectrum. If specific use cases are needed or there are regulations to abide by, it is also possible to use licensed spectrums.

All the network functions such as gNB, 5G core control plane, and user plane are deployed in the premise of the enterprise - factory or building – as shown in Figure 1. Once an enterprise has an independent 5G network with all the functions at its disposal, it can apply all the innovative 5G technologies relevant to the enterprise, on premise, without being limited to the traditional wired Ethernet or wireless LAN solutions.

Typical advantages of a standalone private network are summarized as follows.

- Security: An independent network that is completely separated from the public network ensures security and privacy by preventing leakage of internal traffic and subscriber related information.
- Ultra-low latency: With all network functions located on premise, the network delay between the device and the application server is short, enabling ultra-low latency services such as motion control applications.
- Customized quality of services: Network configurations of private networks can be customized to meet the requirements of the enterprise applications, unlike the typical configuration of the public network. The configuration includes all parameters that can affect the key performance of data rate, reliability, latency, as well as uplink/downlink frame structure.
- Autonomy: The given nature of a standalone private network guarantees its independent operation, even if any failures (e.g. network downtime and performance degradation) occur on the MNO's public 5G network.

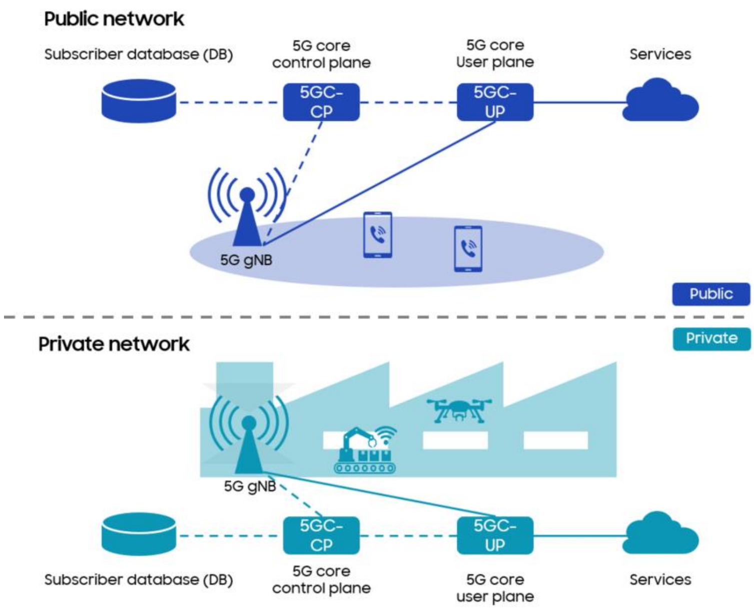

Figure 1. Standalone private 5G network isolated from public network

However, purchasing and deploying an entire 5G network, which contains wireless technologies, may be a challenging alternative solution for enterprises that don't have enough experience and know-how of telecommunication technologies. That is why it is importat to select a vendor like Samsung that had the knowledge, experience and services support to effectively implement and customize the 5G network for your enterprise.

Dependent Network

①Private Network Sharing RAN

In this scenario, a private network shares part of the RAN – especially gNB – with the public network, while other network functions are deployed on the enterprise premise and remain separated from the public network, as shown in Figure 2. The sharing between the private network and the public network is based on the functionality of 'RAN sharing', detailed in 3GPP TS 23.251 [2]. This deployment scenario is further divided into two sub-scenarios depending on whether the private network uses local private spectrums or uses the operator's licensed spectrum, which is shared with the public network. The former and latter sub-scenarios are based on multi-operator RAN (MORAN) and multi-operator core network (MOCN) of RAN sharing, respectively.

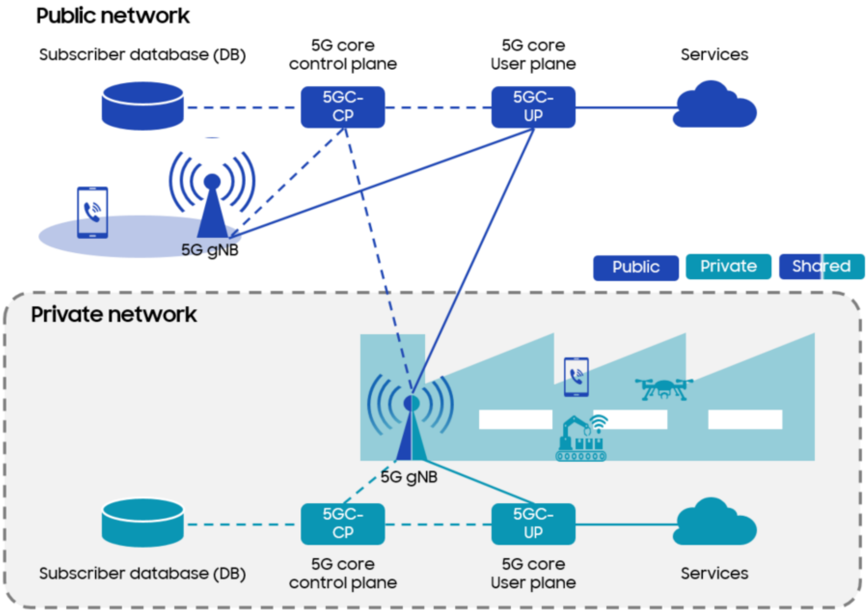

Figure 2. RAN sharing between private and public networks

This scenario works much like a standalone private network, except that in this scenario, the private network and public network share parts of the RAN. Data traffic of the private network – private slice of Figure 2 - is delivered to the private's 5G core user plane in the enterprise, while data traffic of the public network – public slice of Figure 2 - is delivered to the 5G core use plane in the mobile operator's public network. Here, the private 5G core control plane is also deployed in the enterprise, so that subscriber and operation information of the private network do not leak outside. Therefore, the security and privacy of the private network can still be guaranteed, despite parts of the RAN not being fully separated.

In addition, under this model, all network functions are located in the enterprise premises, providing ultra-low latency communications. In this scenario, however, failures in the RAN node may cause failures of the private network.

②Private Network Sharing RAN and Control Plane

In this scenario, the private network and the public network share the same RAN, while the control of the network is handled by the public network. The overall architecture of private and public networks and their components are shown in Figure 3. Functions on the control plane for the subscribers of a private network, such as authentication or mobility, are performed in the control domain of the mobile operator's network, along with the control of the public network subscribers. In other words, devices of the private network are, by definition, subscribers of the MNO's public network. This allows devices of the private network to directly access the public network services, and provides service continuity by roaming when the private network devices move between the private network and the public network, and vice versa. However, interworking with the public network and its management leaves security concerns such as operational information and subscription information of private network devices being stored on a mobile operator's server, rather than being stored on the premise.

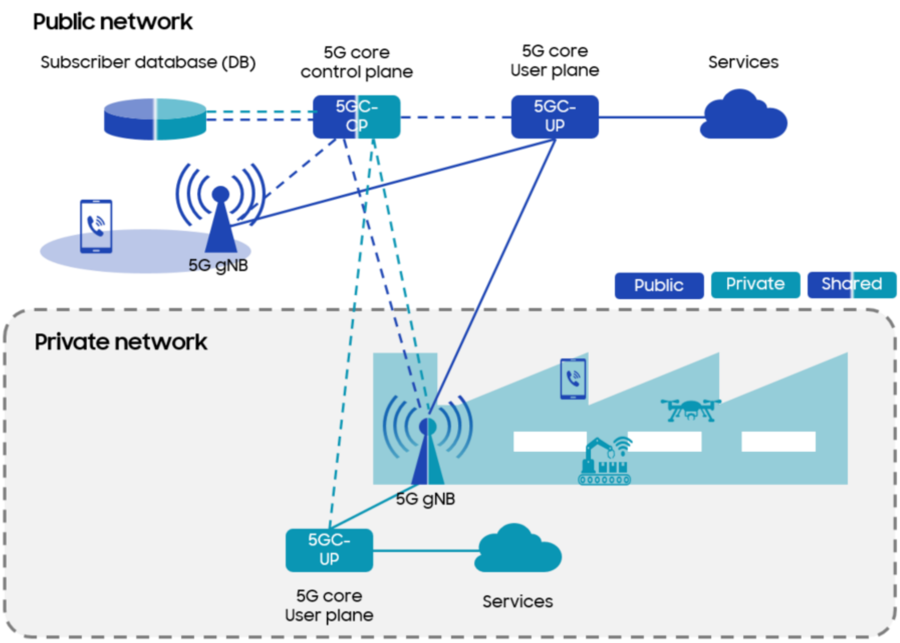

Figure 3. RAN and control plane sharing between private and public networks

Data traffic between the private and the public network can be separated by means of 3GPP defined technologies such as network slicing [3]. The separation between the networks is performed using different network slice identifiers. Data traffic of the private network is delivered to the 5G core user plane in the enterprise with its identifier, while data traffic of the public network is delivered to the 5G core user plane in the mobile operator's public network as shown in Figure 3.

This scenario also guarantees ultra-low latency via introduction of multi-access edge computing (MEC) in the enterprise. The ultra-low latency communication between device-gNB-5GC-MEC enables the enterprise to apply ultra-reliable and low-latency communication (URLLC) applications such as autonomous driving and real-time robot control.

③Private Network Deployed in Public Network

Figure 4 shows a private network that is hosted entirely on the public network. In this scenario, only the gNB is deployed on the enterprise grounds and all other network functions are shared with the public network. All data traffic of the private and public networks flows through the public network located outside the enterprise, but the traffic of each network can be logically independent of one another, due to the separation using end-to-end network slicing.

In this scenario, the service provider will have full control of security and privacy because the deployment scenario is completely dependent on the public network and the failure of the public network leads directly to the failure of the private network. In addition, it may be difficult to utilize low latency services such as URLLC under the model. Since the MEC is also constrained to the mobile operator's network, the round trip time (RTT) of the network can greatly increase depending on the distance between the enterprise and the edge cloud of the operator where the MEC is located.

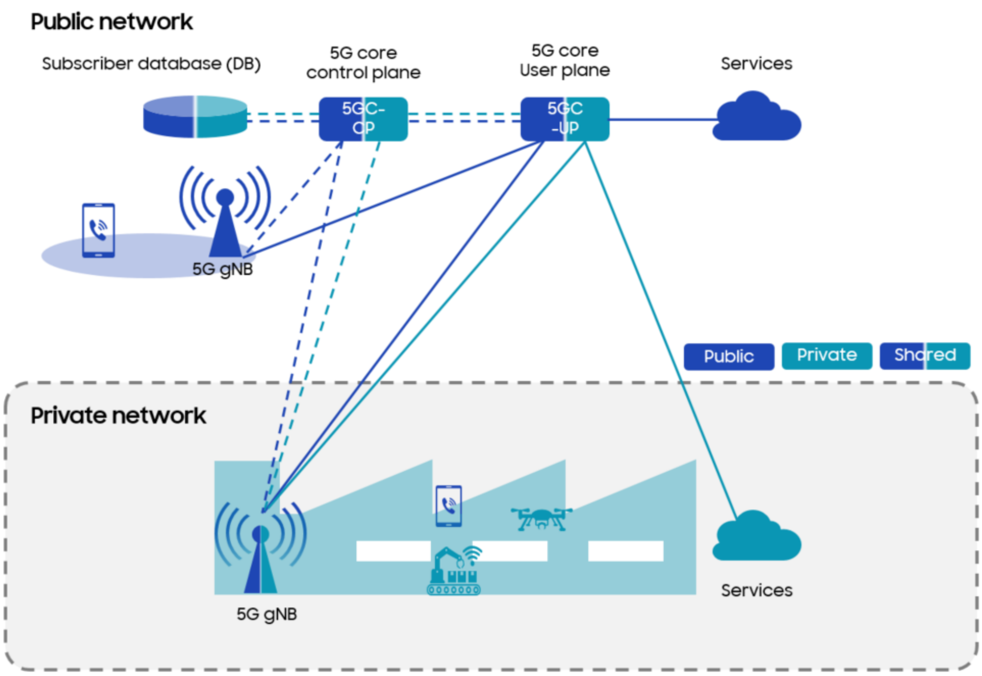

Figure 4. Private network deployed in public network

This deployment scenario is hosted on the operator's network, which makes this solution an operating expense to the enterprise, compared to other scenarios where the network functions need to be built within the enterprise. Also, much like the scenario above, service continuity can be guaranteed through roaming when devices move between the private and public networks.

Private 5G Network Features

A private network is different from a public network from deployment purpose or configuration standpoints. All functions necessary for configuring a public network can also serve as components for a private network. Figure 5 shows software features for a private network. It will better meet the stringent requirements of private networks.

Category	Features
Architecture	1) RAN Sharing ① MoRAN ② MoCN 2) Network Slicing 3) Private Network Identifier ① NPN ID (NID) for standalone NPN (SNPN) ② Dedicated Data Network (DNN) for deployed in public network ③ Network Slice Selection Assistance Information (S-NSSAI) for network slicing
Industrial IoT	1) NR-U 2) Time Sensitive Network 3) Mobile Edge Computing 4) Ultra Reliable Low Latency Communication 5) Accurate Positioning

Figure 5. Features for Private 5G Network

This section, in particular, presents the required features necessary to deploy the private network scenarios described in the section above. Further, this chapter depicts the key features being defined and studied to satisfy the stringent requirements of private networks, especially that of the Industry 4.0.

1. Architecture

1) RAN Sharing

RAN sharing allows multiple participating operators to share resources of a single shared network according to agreed sharing policy. 3GPP has defined several approaches for the RAN sharing such as MORAN and MOCN, shown in Figure 6.

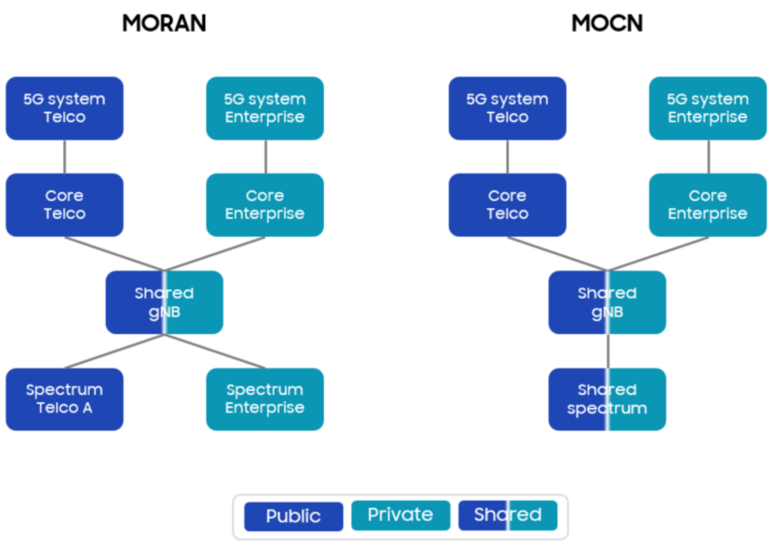

Figure 6. RAN sharing architectures for private networks

The deployment scenario in which a private network shares part of the RAN with a public network is based on the RAN sharing architecture. In such case, the operator that shares the RAN with the public network operator is considered a private enterprise or organization that deploys and operates a private network. With a RAN sharing agreement in place between a public and private network operator, the public network operator allocates shared resources to the private network operator based on current and planned needs, as well as according to service level agreements.

The scope of RAN sharing in 3GPP Rel. 16. has been extended to the NPNs. For example, 5G MOCN supports the following sharing scenarios involving NPNs [5].

- RAN is shared by multiple SNPNs
- RAN is shared by one or multiple SNPNs and one or multiple PLMNs
- RAN is shared by one or more PNI-NPNs and one or more SNPNs
- RAN is shared by one or multiple PLMNs and one or multiple PNI-NPNs

It should be noted that a network slice is defined within a PLMN or SNPN. However, RAN sharing is performed among different PLMNs and/or SNPNs. In the case of RAN sharing, each PLMN or SNPN sharing the RAN defines and supports its specific set of network slices that are supported by the common RAN.

2) Network Slicing

Network slicing in 5G is a key capability that enables flexibility in the network, as it allows multiple logical networks to be created, simultaneously [3]. This, in turn, helps to address the cost, efficiency, and flexibility requirements imposed by the variety of industrial vertical applications in a private 5G network. Vertical applications are very diverse and their requirements are defined by the service characteristics of the vertical segment. Network slicing allows carriers to create logical data pipelines for each of its data type services, thereby assuring the QoS for each service. Through network slicing, 5G is ideal for creating multiple dedicated networks for each vertical application, enterprise, or organization with different service requirements over a single network – i.e. PLMN or SNPN -as shown in Figure 7.

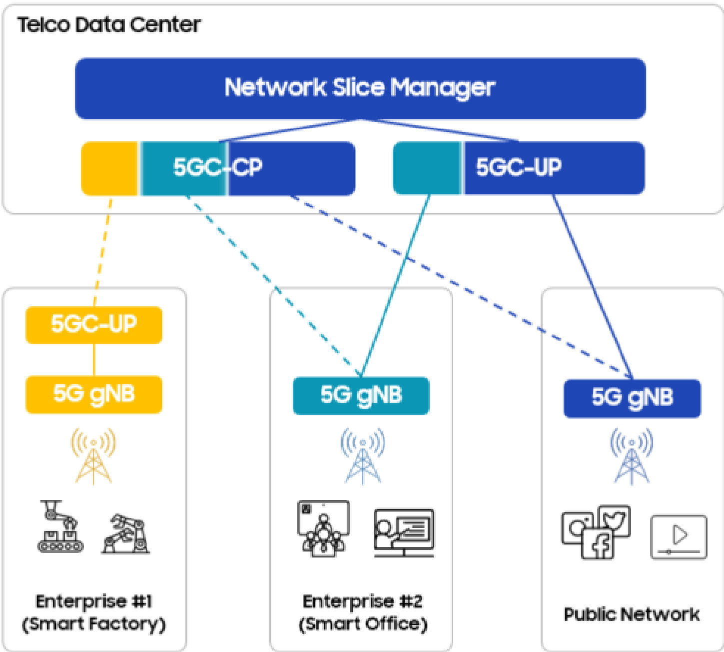

Figure 7. Network slicing for private 5G network

In private networks, in which some of its infrastructure are shared with a public network – PNI-NPN - logical separation from the public network is possible through network slicing. Figure 7 shows examples of private networks deployed in conjunction to a public 5G network of a MNO using network slicing. In the figure, private network for enterprise #1 is deployed 5G gNB and core user plane and it's used 5G core control plane of a public network by network slice manager. The private network for enterprise #2 is entirely hosted on the public network, except gNB. The private networks can provide services independent of the public network and the other private network, owing to the resource isolation within slices.

3) Private Network Identification

The first generation networks based on the 5G system architecture (3GPP Rel. 15) was primarily designed for public use, but the possibility of deploying 5G networks for private use has sprung a wave of interest along with the growing demand for its utilization within the industry. Accordingly, the second phase 5G networks for private use is being handled in the 3GPP and the network can be classified into two categories – public land mobile networks (PLMNs) and non-public networks (NPNs). A non-public network, defined in 3GPP TS 22.261 [4], enables deployment of 5G systems for private use and provides coverage and private services within the enterprise's defined premises. In order for users and devices in the enterprise to discover, access, and select their private network, the private network is identified by a private network identifier called NPN ID and the identification is classified according to the deployment architectures described in the previous section.

A standalone private network, which is a standalone NPN (SNPN), described in the 3GPP specification, is identified by a combination of a PLMN ID and network identifier (NID). The PLMN ID used for SNPN does not need to be unique and PLMN IDs reserved for use by private networks can be used. Otherwise, a PLMN operator can use its own PLMN ID for a SNPN along with a NID, but registration in a PLMN and mobility between a PLMN and an SNPN are not supported using an SNPN subscription given that the SNPN does not rely on the network functions provided by the PLMN.

The private network in conjunction with a public network has been studied as a public network integrated NPN (PNI-NPN) in the 3GPP specification. PNI-NPNs are NPNs made available via PLMNs, by means of dedicated data network names (DNNs), or by one or more network slice instances allocated for the NPN with single network slice selection assistance information (S-NSSAI). Figure 8 shows the network identification of the PNI-NPN hosted by a public network with network slicing, compared with the standalone NPN. For this case, the UEs in the private network have subscriptions to the PLMN. To ensure that UEs separate private and public networks and do not access unauthorized networks, a closed access group (CAG) can optionally identify a group of subscribers who are permitted to access one or more CAG cells associated to the CAG.

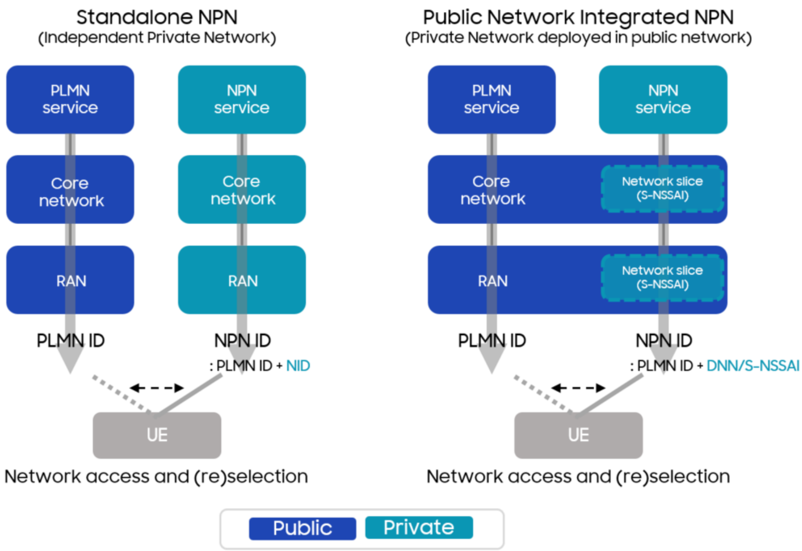

Figure 8. Network identification for private 5G network

2. Industrial IoT

1) NR in Unlicensed Spectrum

Enterprises may choose the appropriate operating frequency spectrum on their decision. However, it can be difficult for an enterprise or organization to operate its private network in a licensed spectrum, because using the licensed spectrum requires a license from the national regulator or an agreement with a license holder, typically an MNO. Thus, licensed spectrums can limit how and where private networks are hosted. Naturally, this brings to surface the need for spectrum options that can be easily and rapidly adopted by private network operators. The NR for unlicensed spectrum (NR unlicensed, NR-U) of 3GPP Rel. 16 provides the potential to alleviate the spectrum conflict in future wireless networks by operating in the unlicensed band.

For industrial deployment on the NR-U, two main scenarios have been defined in the 3GPP. The first is a NR-U deployment with a licensed anchor. This scenario is analogous to LTE's license assisted access (LAA) and is a suitable scenario for the public network to obtain capacity gain by using the unlicensed spectrum. Another scenario for private networks is NR-U deployment in the unlicensed spectrum only, without being anchored to any licensed carrier. This is called standalone NR-U, and is attractive for use in industrial networks since it has no dependency on public networks.

Multiple network operators, by nature, can access an unlicensed spectrum, meaning that when one network tries to use the spectrum, it may already be occupied by another party. Depending on how the spectrum is shared, there are two main modes of spectrum sharing proposed for standalone NR-U. Figure 9 shows the comparison of spectrum sharing modes.

- Asynchronous shared spectrum mode: The NR must follow the existing coexistence rules, which is listen-before-talk (LBT) channel access protocol, when deployed in the unlicensed spectrum. In the channel access, characterized by distributed and asynchronous random access to the radio channel for uplink data transmission, the presence of LBT will degrade NR-U performance in terms of channel access delay and latency due to the LBT requirement for each new transmission.
- Synchronous shared spectrum mode: The synchronous shared spectrum allows overlapping of the contention window (CW) of the node. It offers great advantages over asynchronous mode for more efficient spectrum sharing. It enables advanced technologies such as coordinated multi-point (CoMP) and URLLC to enhance reliability and minimize latency. The synchronous sharing mode may be more suitable for private networks that need to meet stringent requirements of industrial applications. However, this approach requires sharing mechanism such as a common synchronization reference among operators.

Mode	Asynchronous	Synchronous
Spectrum	5GHz	6GHz
Area	Global	Under consideration (U.S. and Europe)
Spectrum Efficiency	Low	High
Benefit	Not Needed time synchronization	Enable to adapt CoMP, URLLC

Figure 9. Comparison for spectrum sharing mode of NR-U

The 3GPP classifies the bands for NR-U into sub 7 GHz and millimeter wave (mmWave) bands. The sub 7 GHz band for NR-U typically includes the 2.4, 3.5, 5, and 6 GHz bands. Meanwhile, in mmWave, 60GHz band is being developed as unlicensed band in the 5G NR-U roadmap. In the US, in particular, the CBRS band has been in the spotlight for the use of private networks. In addition to the mentioned frequency bands, many countries conduct evaluations of the availability of new unlicensed and shared frequency bands for private networks. Figure 10 shows the frequencies which are considered for NR-U.

NR-U Freqeuncy	Legacy Tech
2.4GHz	Bluetooth, Wi-Fi
3.5GHz	CBRS
5GHz	Wi-Fi
6GHz	Wi-Fi 6E, Broadcast
60GHz	Wireless Backhaul

Figure 10. NR-U frequency in the global

2) Time Sensitive Network Support

The 3GPP Rel. 16 enables 5G systems to interwork with existing wired time sensitive networking (TSN), a set of IEEE Ethernet standards foundational for meeting the many demands of time-sensitive applications in Industry 4.0 [4]. The TSN solution can accurately synchronize all devices on a network and use coordinated scheduling to ensure deterministic performance of real-time applications. To support TSN time synchronization, the 5G system is integrated with the external network as a TSN bridge with TSN translators on the device and system sides as shown in Figure 11. The translators map the TSN configuration to the 5G QoS framework, providing efficient transmission over the Ethernet. For TSN synchronization, the entire end-to-end 5G system can be considered as an IEEE 'time-aware system'. In private networks where many industrial applications require micro-second time synchronization, the interworking with TSN allows 5G systems to use common 5G system times to provide accurate synchronization for these applications.

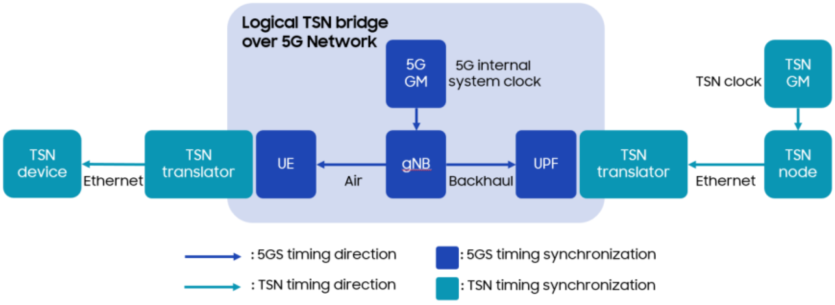

Figure 11. TSN support in the 5G system

3) Mobile Edge Computing

With the coming of the IoT era and Industry 4.0, connecting vertical applications to a mobile communication network, as well as the smart phone based services, has become a necessity. Many newly emerging vertical applications require ultra-low latency of less than 1 ms and high capacity communication up to several Gbps. However, since using gateways in the 4G core are typically centralized on a few central servers, application servers are physically located far away from devices. The long delay time due to the physical distance makes it impossible to meet the ultra-low latency requirements and the overload of backhaul network traffic makes it impossible to support high-capacity services. These shortcomings have led to the concept of MEC, where application servers are pushed closer to the edge, or near vertical devices and applications. Because 5G is based on control user plane separation (CUPS) which decentralizes the 5G core user plane in charge of user data traffic from the center cloud, MEC can be deployed in regions requiring edge services.

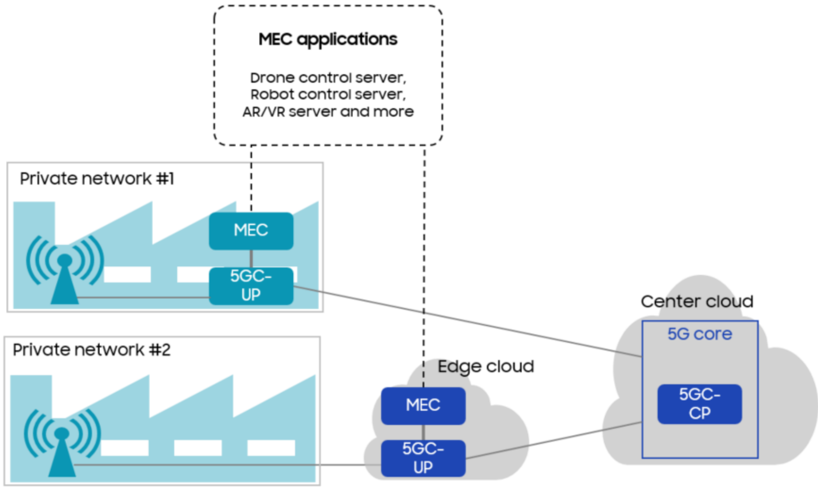

Figure 12. Private 5G networks with MEC

Figure 12 shows an example where MECs are deployed inside or near private networks to satisfy the industrial use cases of the private networks. Private network of enterprise #1 in Figure 12 is a standalone private network, where the MEC is located in the enterprise's premise, enabling ultra-low latency and high capacity communication for enterprise industrial communication. The private network of enterprise #2 is deployed in a public network, meaning the 5G core userplane and MEC are deployed in the edge cloud of the public network, not in the enterprise's premise. In this case, the latency requirement may also be satisfied via the MEC within the edge cloud much closer to private network #2 than the central cloud.

4) Ultra Reliable Low Latency Communication

A growing number of critical applications in private networks have stringent latency performance and reliability requirements. Communications with vehicles, drones, and industrial robots are a few examples of applications where radio access must meet either low latency less than 1 ms or high reliability under 10-5 packet drop rate. The 3GPP has been addressing and improving the URLLC feature set from Rel. 15 to achieve high reliability and low latency.

The URLLC feature set can be divided into features that achieve low latency and features that enable high reliability. First, key features of 5G air interface to achieve low latency are as follows:

- Frequent transmission opportunity: By frequent monitoring occasions for downlink (DL) control channel and frequent uplink (UL) scheduling request (SR), the waiting time in DL/UL transmission can be reduced.
- Flexible transmission duration: Using larger subcarrier spacing and small scheduling units such as mini-slot (Figure 13) can achieve the short transmission duration.
- UE aggressive processing time: To shorten the processing time of UE, aggressive UE processing capabilities have been defined in NR.
- UL configured grant: gNB configures periodic UL resource for a UE without the need for dynamic UL grant. It allows the delay skip from UL SR to scheduling grant as shown in Figure 13.
- DL pre-emption – URLLC packet, which needs to be transmitted urgently, can be pre-empted in the duration of an ongoing enhanced mobile broadband (eMBB) transmission. A pre-emption indicator informs the eMBB UEs about the punctured resources. This is shown in Figure 13.

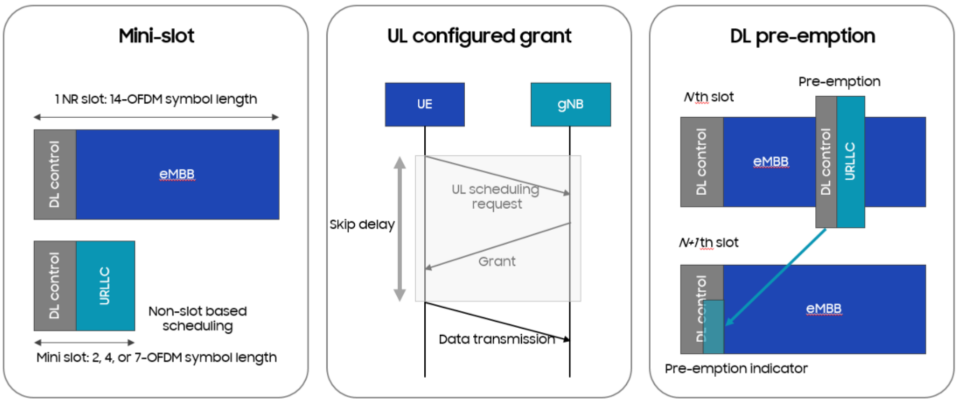

Figure 13. NR features for low latency

On the other hand, Figure 14 shows the key features in 5G air interface for high reliability. This includes slot aggregation, packet data convergence protocol (PDCP) duplication, and new modulation and coding scheme (MCS) tables for low spectral efficiency. In addition, private networks, such as factories and buildings where it is conducive to placing multiple transmission/reception points, can increase the utility of multiple antenna technologies including CoMP and greatly improve reliability.

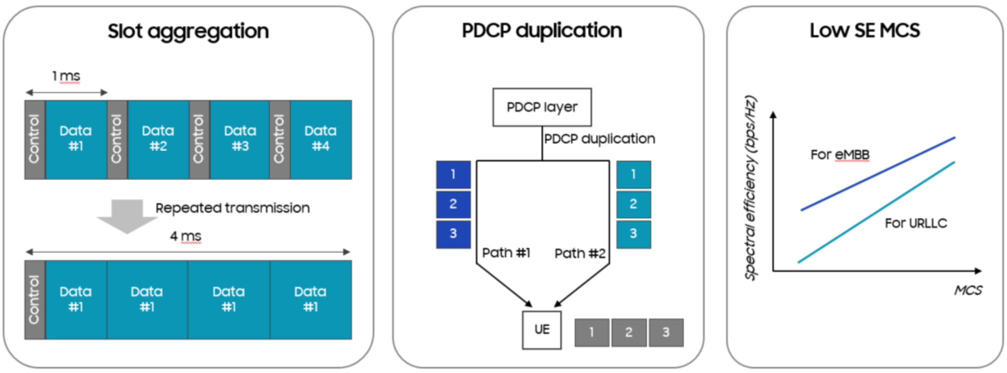

Figure 14. NR features for high reliability

5) Accurate Positioning

Though the requirements for positioning vary depending on applications, the 5G network for Industry 4.0 may require a positioning accuracy of less than 1 m as defined by the 3GPP. As is the case in 4G, the position of a UE can be obtained using a trilateration estimation algorithm based on the direction of arrival (DoA) and/or time of arrival (ToA) from multiple cells to the UE. For the estimation of DoA and ToA, some reference signals including positioning reference signal (PRS) may be used.

5G NR allows an even more precise DoA and ToA, making positioning estimations more accurate. This includes the use of more increased multiple input multiple output (MIMO) antenna arrays. For example, the support of beam sweeping may be one of the major changes for the NR PRS design. In private networks such as factories and buildings, it may be easy to place multiple transmission/reception points, as it offers the possibility of CoMP as shown in Figure 15. In turn, it is possible to secure higher positioning accuracy. Some enhancement technologies related to reference signals such as power control, comb structure, symbol locations within a slot, and beam alignment considerations are also under discussion. In addition, the 5G framework can integrate non-3GPP technology into the hybrid positioning method to ensure that 5G positioning is robust and accurate.

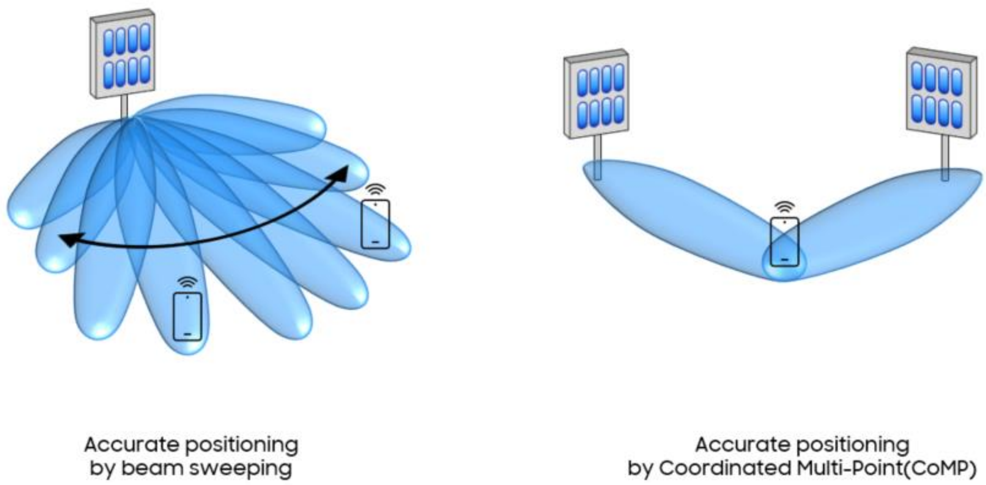

Figure 15. NR features for accurate positioning

Samsung's Private 5G Solution

Complete Private 5G Network Solutions

Samsung offers efficient business-enabling solutions that can embrace any enterprise use case. Figure 16 shows Samsung's private 5G solution, which is a complete end-to-end solution including RAN, core network, switch, management system, and applications for the private network.

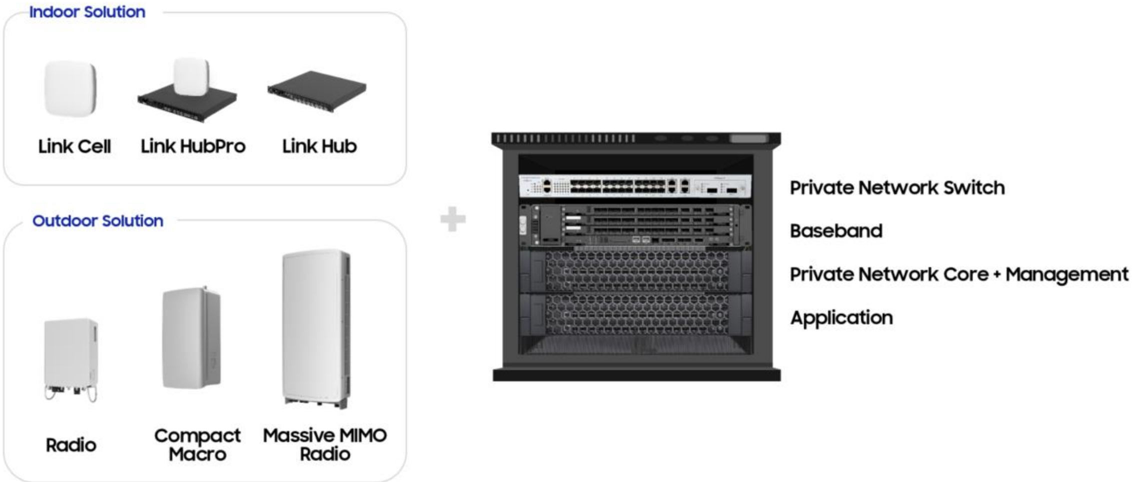

Figure 16. Samsung's end-to-end private 5G solution

Each component of the solution plays a role appropriate to the enterprise's needs for private 5G networks, deviating from the traditional look for telco customers.

- RAN: Samsung provides extensive Radio and Baseband products to offer proper solutions that meet the demands of private network operators. The extensive RAN portfolio from Samsung consists of Baseband, macro/micro Radios including massive MIMO, mmWave, small cell solutions, and indoor solutions. Samsung's RAN portfolio meets the growing interest in private networks in the CBRS, C-band, and local frequency in Japan, and considers the various size and installation environments, enabling rapid time to market.
- Private Network Core: Samsung's Private Network (PN) Core provides a pre-configured set to support various use cases of the private 5G network. The minimum configuration is a network-in-a-box system, which provides single server core and management solution for single small scale enterprise site. PN Core can also be expanded and molded to fit a diverse case of private 5G networks for medium to large scale multi-site enterprises. The PN Core can operate as 4G evolved packet core (EPC), 5G non-standalone (NSA), or 5G standalone (SA) core while enabling a seamless migration without hardware replacements.
- Private Network Switch: Samsung's private 5G solution provides the connection to the transport network with the PN Switch optimized for private networks. The PN Switch supports a compact-sized data center switch to connect virtualized servers, and delivers the enterprise switch function that supports wired/wireless integration, including Wi-Fi. It can also support Samsung's software-defined network (SDN) solution, which is an all-in-one solution supporting automated, integrated management of mobile transport, and enterprise's data center network equipment optimized for private 5G networks.
- Private Network Management System: Samsung's Private Network Management System (PNMS) provides easy distribution, easy scaling, and integrated management for various local and remote sites. PNMS can be included in the PN Core which consists of a single server or be deployed as a separate system if the enterprise requires remote management to manage multiple sites. PNMS provides an easy and powerful portal for management, and plans to provide closed-loop automation by interacting with analytics systems for more automated lifecycle management and network slicing.
- Application: Samsung's private 5G solution delivers applications to provide various services. The applications are loaded in a single server and managed via PNMS. Currently, the supported applications are following: IP multimedia subsystem (IMS); mission critical push-to-all (MCPTX); video surveillance platforms; drone and IoT solutions. Additional applications are planning according to enterprise's needs.

The complete end-to-end solution provides various configurations based on the enterprise's size and business needs. And the configurations are standardizied to several options that can meet various demands for coverage and capacity of private 5G customers, from a cost-effective one-box solution to a large-scale expandable solution. With the standard configuration portfolio, enterprises can reduce the time and effort to build and operate their private 5G networks for both independent and dependent deployment architectures.

More detailed descriptions of Samsung's private 5G solution and the benefits it brings can be explored further in another white paper about Samsung's solution [1].

Synergy with Virtualized RAN

In addition to the features above, Samsung's vRAN, which plays a leading role in RAN virtualization, can serve as a suitable solution for rapid adoption of private networks. Private networks can be deployed in various environments depending on the purpose of the network. It can be placed indoors or outdoors, and be configured as macro, micro, or small cells, requiring a wide range of network capacity. Samsung vRAN supports flexible deployment that increases resource efficiency by using only the resources that is required by the network, and can meet various capacity needs of private networks.

In addition, one of the biggest reasons why it is difficult for private enterprises and organizations to directly operate its own private network is that, in general, mobile communication technology requires very high expertise in deployment and operation, something that is hard to come by in average enterprise IT departments. Deployment and operation of various types of hardware equipment, repairs in case of failure, introduction of new network features, and replacement of outdated equipment can be high entry barriers for the private enterprise that does not had long experience in telecommunications. To overcome this, Samsung vRAN converts telco technology to IT technology, which enables deployment, maintenance, repair, and upgrade with software, making it easy for private enterprises to operate their own mobile networks.

In addition to the network functions such as core, centralized unit (CU), and distributed unit (DU), applications required by private networks, including MEC, can be operated on the same platform – commercial off-the-shelf (COTS) server or cloud platform - avoiding equipment specific deployment and management. Also, when standard changes and new technologies are introduced, easy and cost-effective upgrades facilitate performance guarantees at the level of public networks. Samsung is collaborating with the public cloud vendor for deployment of Samsung's vRAN, vCore and MEC technologies. It can accelerate 5G expansion for enterprises and help them deploy private 5G networks faster.

Summary

More than ever, today's industries and enterprises are demanding private networks where various devices requiring different communication capabilities such as robots, drones, sensors, as well as user terminals can be seamlessly connected. Most use cases involving such devices have high performance requirements in terms of availability, reliability, latency, and security, which have led to the need for integration of 5G technology in private networks.

To accelerate the deployment and operation of private 5G networks, several technologies have been brought up for discussion and been specified in the 3GPP. In order to deploy private networks that are partially or completely isolated from public networks, technologies that allow the private and public networks to share some of its networks are required. Access to unlicensed or shared spectrum that are not occupied by public operators can be one of the keys to deploy private network without dependencies on the public network. Many technologies for achieving high performance requirements, such as increasing reliability and lowering latency, are also applied to satisfy the high demands of private networks.

Samsung has the portfolio and capability to build reliable private networksand is constaly working on new technologies and features to improve the 5G experience. . Samsung provides a complete end-to-end private 5G solution including RAN, core network, switch, management system, and applications for enterprise wireless networks, and is designed to fit in any deployment architecture with different business purposes. Private network customers can also take advantage of quickly deploy compact solutions for their private networks with the standardizied but fully functioning Samsung private 5G solution.

References

[1] Samsung, “Transforming Private Networks with Samsung 5G”

[2] 3GPP TS 23.251, “Network Sharing; Architecture and functional description”

[3] Samsung, “Network slicing”, https://www.samsung.com/global/business/networks/solutions/network-slicing/

[4] 3GPP TS 22.261, “Service requirements for next generation new services and markets”

[5] 3GPP TS 23.501, “System architecture for the 5G System; Stage 2”

[6] Doodle labs. “Industrial Private Wireless”

[7] Global TD-LTE Initiative. “LTE 5G NR Private Networks WHITE P APER V1.0”

[8] MDPI, “Future is Unlicensed: Private 5G Unlicensed Network for Connecting Industries of Future”

About Samsung Electronics Co., Ltd.

Samsung inspires the world and shapes the future with transformative ideas and technologies. The company is redefining the worlds of TVs, smartphones, wearable devices, tablets, digital appliances, network systems, and memory, system LSI, foundry and LED solutions.

Address : 129 Samsung-ro, Yeongtong-gu, Suwon-si Gyeonggi-do, Korea

ⓒ 2021 Samsung Electronics Co., Ltd.

All rights reserved. Information in this leaflet is proprietary to Samsung Electronics Co., Ltd. and is subject to change without notice. No information contained here may be copied, translated, transcribed or duplicated by any form without the prior written consent of Samsung Electronics.

Homepage & Insight

www.samsungnetworks.com

www.samsung.com/global/business/networks/insights

Youtube

www.youtube.com/samsung5g