IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received October 25, 2021, accepted November 3, 2021, date of publication November 10, 2021,
date of current version November 23, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3127482

5G Non-Public Networks: Standardization, Architectures and Challenges

JONATHAN PRADOS-GARZON[1,2], PABLO AMEIGEIRAS[1,2], JOSE ORDONEZ-LUCENA[3], PABLO MUÑOZ[1,2], OSCAR ADAMUZ-HINOJOSA[1,2], AND DANIEL CAMPS-MUR[4]

[1]Department of Signal Theory, Telematics, and Communications, University of Granada, 18014 Granada, Spain
[2]Research Centre for Information and Communications Technologies, University of Granada, 18014 Granada, Spain
[3]Telefonica I+D, 28013 Madrid, Spain
[4]i2CAT Foundation, 08034 Barcelona, Spain

Corresponding author: Jonathan Prados-Garzon (jpg@ugr.es)

This work was supported in part by the H2020 Project 5G-CLARITY under Grant 871428, and in part by the Spanish National Project TRUE-5G under Grant PID2019-108713RB-C53.

ABSTRACT Fifth Generation (5G) is here to accelerate the digitization of economies and society, and open up innovation opportunities for verticals. A myriad of 5G-enabled use cases has been identified across disparate sectors like tourism, retail industry, and manufacturing. Many of the networks of these use cases are expected to be private networks, that is, networks intended for the exclusive use of an enterprise customer. This article provides an overview of the technical aspects in private 5G networks. We first identify the key requirements and enabling solutions for private 5G networks. Then, we review the latest 3rd Generation Partnership Project (3GPP) Release 16 capabilities to support private 5G networks. Next, we provide architecture proposals for single site private networks, including the scenario in which the radio access network (RAN) is shared. Afterwards, we address mobility and multi-site private 5G network scenarios. Finally, we identify key challenges for private 5G networks.

INDEX TERMS 5G, non-public networks (NPNs), private 5G networks, architectures.

I. INTRODUCTION

Fifth Generation (5G) is here to accelerate the digitalization of economies and society. Over the last decade, the combined efforts from academy and industry have materialized in matured 5G standards that will bring services with data rates, latency, reliability, connection density, and security constraints never seen before, thus opening up innovation opportunities for verticals. Ericsson has identified more than 200 industry digitization use cases enabled or substantially enhanced by Fifth Generation (5G) technology [1]. Typical use cases can be found in disparate sectors such as agriculture, tourism (e.g., museums), transportation, healthcare, education (e.g., convention centers), retail industry (e.g., shopping malls), transport hubs (e.g., ports and airports), sport facilities (e.g., stadiums), energy industry, military bases, and manufacturing. In particular, 5G is acknowledged as a key enabler for Industry 4.0 [2], [3].

Many of the networks of the above mentioned use cases, including the industrial sector, are private networks. A private 5G network, also termed NPN by Third Generation Parnetship Project (3GPP), is a 5G network deployed for non-public use. In contrast to Public Land Mobile Networks (PLMNs) that offer mobile network services to public subscribers, NPNs are intended for the exclusive use of an enterprise customer, such as an industry vertical or a state-owned company. There are two basic options to deploy a 5G NPN: i) SNPN, which does not rely on PLMN-provided network functions, and ii) PNI-NPN, whose deployment is supported by a PLMN. Whereas SNPNs enables the enterprise customer to retain full control of the NPN, PNI-NPNs represent a reduced entry barrier due to Capital Expenditure (CAPEX) and Operational Expenditure (OPEX) reduction.

5G NPNs are gaining momentum across Industry and Academia. As a concrete evidence of this, there are some ongoing European projects, such as 5G-CLARITY, 5GROWTH, AFFORDABLE-5G, and FUDGE-5G, working on 5G NPNs up to date and many research works addressing questions and issues related to 5G NPNs (see Table 1). Table 1 includes a survey on the research literature related to 5G NPNs. Please note that the survey only includes peer-reviewed works (e.g., articles published in journals and

The associate editor coordinating the review of this manuscript and approving it for publication was Stefano Scanzio.

TABLE 1. Related research literature on 5G Non-Public Networks (NPNs). The right column labeled as "E" indicates whether the respective work reports experimental results.

Work	Description	E
Ordonez-Lucena *et al.* [17]	This work considers seven dimensions to qualitatively compare the 5G NPNs DOs, namely, Quality of Service (QoS) customization, autonomy, isolation, security, NPN management for verticals and entry barriers.	
Rostami [18]	This paper and decouples the DO and operation model concepts for 5G NPNs. Then, it discusses and compares four DOs and four operation models for 5G NPNs thoroughly.	
Aijaz [3]	This article motivates the need for 5G in Industry; revisit the spectrum options, use cases and DOs for 5G NPNs; and identifies design aspects and challenges for 5G NPNs.	
Trakadas *et al.* [4]	This article proposes a management architecture for SNPNs that leverages and integrates data analytics, machine learning, infrastructure slicing and cross-domain coordination. It also revisits use cases and enablers for 5G NPNs.	
X. Li *et al.* [5]	This paper describes the pilots of 5G-GROWTH project and the requirements imposed by them. It also presents a novel AI-assisted management architecture for SNPNs with Radio Access Network (RAN) slicing and multi-domain support.	
X. Li *et al.* [19]	This work proposes multi-domain solutions to interconnect multiple 5G NPNs through public networks. It provides experimental results to show the feasibility of these solutions.	✗
Guimarães *et al.* [6]	This article explores the use of 5GGrowth architecture for two industrial use cases related to metrology and quality control. It experimentally evaluates the service provision time and performance (latency and throughput) of the proposed 5G solution.	✗
Camps-Mur *et al.* [20]	This work briefly describes the architecture proposed in 5G-CLARITY project and its key innovations like the integration of 5G New Radio (NR), Wi-Fi, and Li-Fi for enhanced throughput, reduced delay and precise localization.	
Taleb *et al.* [7]	This paper identifies novel use cases and enablers for industrial 5G networks. It also presents a 5G network slicing framework tailored for Industry 4.0. Last, it provides experimental measurements of the slice provision time.	✗
Soós *et al.* [8]	This paper revises the DOs, identifies the primary players in Industry 4.0 and business opportunities, and analyzes the business and technological risks.	
Filin *et al.* [9]	This work investigates the use of 5G NPNs to serve outdoor use-dense environments with high throughput demand. It describes a trial for this use case and includes preliminary results on the observed backhaul capacity.	✗
Godor *et al.* [10]	This article covers the requisites, standardized capabilities and open issues related to time synchronization in industrial 5G networks.	
Poe *et al.* [11]	This work discusses and identifies challenges on how to manage the traffic in PNI-NPNs considering isolation requirements and architectural aspects.	
Kang *et al.* [15]	This work addresses the integration of 5G with Time-Sensitive Networking (TSN) and IEEE 802.11 technologies.	
Jerichow *et al.* [16]	This work puts the emphasis on the security aspects of 5G NPNs.	

conferences proceedings). However, it is fair to say that other types of documents, such as white papers or technical specifications, laid the foundations of 5G NPNs and most of the scientific literature, including this work, is based on them. We reference this non peer-reviewed literature throughout the text. The topics addressed in the research works can be classified into five major categories, namely, use cases & requirements, enablers, DOs, management & orchestration, and experimentation in 5G NPNs. The primary observations and conclusions extracted from the related works revision are discussed next.

Some works identify specific use cases and their associated requirements in the context of 5G NPNs [3]–[11]. Part of the use cases covered in the literature are based on those described in [12]–[14], and, remarkably, many of them target smart factory scenarios. This is likely due to the manufacturing sector imposes the most stringent requirements for 5G NPNs. Also, the discussed requisites derived from these use cases are centered around Key Performance Indicators (KPIs), while functional and operational requirements receive less attention. Concerning the 5G NPNs enablers, i.e., technologies, paradigms and aspects that enables or facilitates the adoption of 5G NPNs, many of them are separately covered in [3], [4], [7], [10], [15], [16]. Nonetheless, a more complete review encompassing all of them is missing from the literature. Furthermore, in the literature, a clear distinction is not drawn between the 3GPP standardized capabilities and key solutions orthogonal to the standards to enable 5G NPNs.

The 5G NPNs DOs are discussed in [3], [8], [17]–[19]. DOs refer to the alternatives to roll out a 5G NPN in order to cover the necessities of the different vertical use cases. DOs do not specify details on the realization of the 5G NPNs, but only more high-level features like the location (on-premises versus out-of-premises) of each component of the 5G System (5GS) and the management plane, the spectrum option chosen (e.g., unlicensed spectrum), the ownership of each component (public versus private), and who manages the network. The related research work is centered around the four pioneering DOs proposed by 5G Alliance of Connected Industries and Automation (5G-ACIA) for industrial scenarios [2].

Recent articles propose solutions related to the management and orchestration of the 5G NPNs [4]–[6], [19], [20]. These works highlight the importance of data analytics and Artificial Intelligence (AI) to automate the management of the network slices in SNPNs. The interaction and integration between NPNs and PLMNs to enable, for instance, multi-domain private networks is another field of interest in the literature.

Regarding experimental performance results offered by 5G NPNs, there are four works reporting some of them from trials and proof-of-concepts [6], [7], [9], [19]. Interestingly, three of them provide measurements related to the service provision time in 5G NPNs [6], [7], [19]. In addition, [19] provides measurements for the throughput and latency of the 5G NPNs data plane for both single site and multi-site scenarios.

The authors conclude that the delay degradation associated with the multi-domain interactions is considerably low. Last, the throughput demands in the backhaul for an outdoor private use case are measured in [9].

Given the current interest within the research community, in this work we provide an overview of 5G NPNs. Our goal is to provide a better overall understanding of this emerging field. For that purpose, in this overview we cover the following aspects. We gather the key requirements for NPNs from the enterprise customer viewpoint, which helps understanding the demands to be fulfilled by NPN designs. We give an overview and discuss key enabling solutions for NPNs, such as spectrum access options, deterministic networking, integration with legacy private networks, positioning, O-RAN, on-premises edge computing, and security and privacy features. These enabling solutions are expected to play a decisive role for NPNs to provide 5G services to vertical industries. We provide a summary of the 3GPP Release 16 specifications support for NPNs and network sharing, which helps getting the picture of the 5G NPN capabilities as allowed by the specifications. Moreover, we provide a proposal of the architectures to realize SNPNs and PNI-NPNs. Furthermore, we provide the description of the architecture for NPNs leveraging network sharing. Besides single-site NPNs, we present other scenarios not addressed in the literature. On the one hand, NPNs might spread across multiple sites, e.g., several enterprise branches. On the other hand, various private use cases involve devices that need to move out of the private venue, which requires mobility in NPNs without service interruption. Last, we identify additional challenges and research directions for realizing 5G NPNs to those proposed in the literature.

Besides providing an overview, we identify the following main novel contributions of this paper:

- Reviewing 3GPP Release 16 specification capabilities to support 5G NPNs, including features such as Local Area Data Network (LADN), Closed Access Group (CAG), Data Network Name (DNN), and Multi-Operator Core Network (MOCN) sharing architecture.
- Discussing the PNI-NPN architecture, analysing their technical options and implications, including an archetypal architecture. We additionally include simulation-based performance results for three PNI-NPN configurations in a campus network.
- Proposing a MOCN based sharing architecture for NPNs. Network sharing is also a key trend in 5G, as it enables notable costs reduction and maybe a key lever to reduce the entry barrier for some enterprise customers interested on deploying 5G NPNs. In addition, it also fits the necessities of many private venues that cannot accommodate the deployment of several infrastructure networks due to physical space limitations or aesthetics.
- Covering the mobility in 5G NPNs, discussing the associated issues, and identifying solutions. For the related scenarios, the service continuity when a device leaves the private premises must be ensured with the support of a PLMN.
- Addressing the multi-site 5G NPN scenarios, discussing their issues and identifying deployment alternatives. For such scenario, the support of a public network is needed to provide connectivity among the remote locations while ensuring the required performance and security levels.
- Identifying new challenges for the realization of 5G NPNs.

The remainder of the article is organized as follows. In sections II and III, we provide an overview of the key requirements and enabling solutions for 5G NPNs. In section IV, we review the 3GPP specifications to support NPNs. In section V, we address the single site NPN architectures, whereas in section VI we address the mobility and multi-site NPN scenarios. Finally, in section VII we provide a summary of key challenges for 5G NPNs, and in section VIII we draw the main conclusions.

II. KEY REQUIREMENTS FOR 5G NPNs

This section covers the key requirements for 5G NPNs from the enterprise customer viewpoint. The primary requirements are listed below:

- **Guaranteed QoS**: it refers to the ability to assure the critical QoS parameters on a 24/7 basis to prevent any degradation on the targeted use case. Critical QoS parameters for 5G NPNs include throughput, latency, delay variation (jitter), and availability, among others. The enterprise customer might have a level of demand for just one QoS parameter or a combination of them. The performance requisites of some 5G NPNs use cases are more stringent than those imposed by public services in PLMNs. For instance, the cyber-physical control applications in manufacturing impose stringent requirements in terms of throughput (500 Mbps per device), high connection density (100 devices/m^2), high positioning accuracy (centimeter (cm)-level), and service availability (six 9's). [12]–[14].
- **Customization**: it refers to the need for flexibility to include (and configure) add-on features to the 5GS in order to meet the customer's needs in terms of functionality and performance. Unlike the PLMNs, where 5GS is built with components and configuration settings that allow accommodating traffic/subscriber growth from user-centric services, in NPNs, the 5GS shall be designed to cope with the specificities of customer use cases. For example, to satisfy stringent QoS constraints [17], the private 5GS can be provisioned with radio resource scheduling strategies (at the RAN side) and 5G QoS Identifier (5QI) values (at the Core Network (CN) side) that are not typically available in the solutions used for carrier networks. Likewise, for those use cases requiring value-added functionality (e.g. security, analytics, and localization), the private 5GS can be enriched with value-added Rel-16+ 5G Core

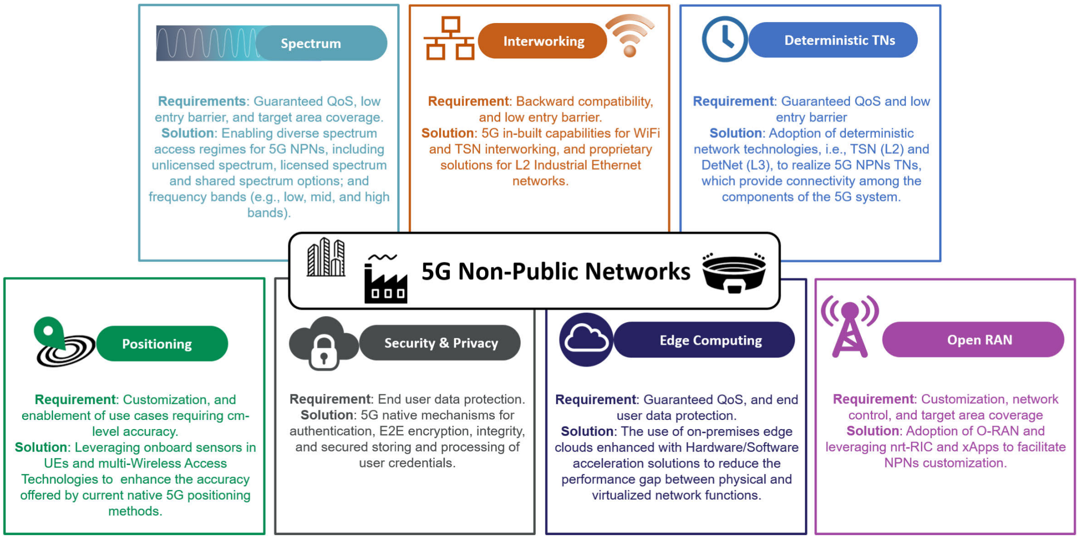

Spectrum
Requirements: Guaranteed QoS, low entry barrier, and target area coverage.
Solution: Enabling diverse spectrum access regimes for 5G NPNs, including unlicensed spectrum, licensed spectrum and shared spectrum options; and frequency bands (e.g., low, mid, and high bands).
Interworking
Requirement: Backward compatibility, and low entry barrier.
Solution: 5G in-built capabilities for WiFi and TSN interworking, and proprietary solutions for L2 Industrial Ethernet networks.
Deterministic TNs
Requirement: Guaranteed QoS and low entry barrier
Solution: Adoption of deterministic network technologies, i.e., TSN (L2) and DetNet (L3), to realize 5G NPNs TNs, which provide connectivity among the components of the 5G system.
5G Non-Public Networks
Positioning
Requirement: Customization, and enablement of use cases requiring cm-level accuracy.
Solution: Leveraging onboard sensors in UEs and multi-Wireless Access Technologies to enhance the accuracy offered by current native 5G positioning methods.
Security & Privacy
Requirement: End user data protection.
Solution: 5G native mechanisms for authentication, E2E encryption, integrity, and secured storing and processing of user credentials.
Edge Computing
Requirement: Guaranteed QoS, and end user data protection.
Solution: The use of on-premises edge clouds enhanced with Hardware/Software acceleration solutions to reduce the performance gap between physical and virtualized network functions.
Open RAN
Requirement: Customization, network control, and target area coverage
Solution: Adoption of O-RAN and leveraging nrt-RIC and xApps to facilitate NPNs customization.

FIGURE 1. Key aspects and enabling solutions for 5G NPNs.

(5GC) network functions, following a plug-and-play approach.

- **Network Control**: it represents the desire of some enterprise customers to retain (certain) control of their networks, e.g., configuration management of certain network functions, and deciding on traffic flow policies. PLMNs are categorized as mission-critical infrastructure, and hence it is not acceptable for the PLMN-Operator to allow 3rd parties to reach out to Operation and Service Subsystem (OSS) and network assets freely. In fact, any misconfiguration injected by the customer can put at risk the stability of the entire PLMN, and thus the performance and integrity of public user services. If the customer wants to take a proactive role in network management, the only solution is to go for NPNs, either SNPN or PNI-NPN, with the PLMN-Operator providing necessary capability exposure mechanisms for PNI-NPNs.
- **Data protection**: it stands for the need of customers to ensure that unauthorized entities do not have read and write access to sensitive data, including operational data (e.g., configuration information, logging, trace data), subscriber data, and business-related data (e.g., charging information). Assuring the data is properly secured might entail applying the appropriate security mechanisms (e.g., encryption, secondary authentication), deploying some network functions on-premises (e.g., Unified Data Management (UDM), and User Plane Function (UPF)), and providing a certain level of redundancy. The criticality of the data to be conveyed by the NPNs in some scenarios demands add-on protection mechanisms beyond the 3GPP built-in security capabilities applied in PLMNs.
- **Target area coverage**: the enterprise needs radio coverage in a specific geographical area and guarantees the radio signals are confined on-premises to avoid interference with public subscribers and to secure the private communications further. It is remarkable that some enterprise use cases might require a guaranteed coverage (say Reference Signal Received Power (RSRP) > -80 dBm for 99% of the time) across their entire target coverage area, while some might tolerate periodic fluctuations or poor-quality at the edge of the target coverage area. It is important to state that the QoS is only guaranteed in the areas where the enterprise requires the coverage. What is more, NPN coverage beyond the target area is undesirable due to the reasons previously mentioned.
- **Backward compatibility (brownfield environments)**: many private use cases require the integration of the 5G NPN with current legacy private networks technologies (e.g., Wi-Fi and Industrial Ethernet). In this way, the entry barrier is reduced as the enterprises can deploy the NPN incrementally while keeping some parts of the existing private network unchanged.

III. KEY ENABLING SOLUTIONS FOR 5G NPNs

This section reviews key aspects for 5G NPNs (see Fig. 1):

A. SPECTRUM ACCESS OPTIONS

One of the key ingredients for the success of 5G private networks is to make spectrum a handy resource for enterprises. We can distinguish three options considering the commercial terms for spectrum access:

- **Licensed Spectrum (LS)**: A portion of the available spectrum is acquired for exclusive use within a given geographical area. LS is the preferred choice for supporting private Ultra-Reliable Low-Latency Communication (URLLC) services due to it offers the highest predictability. The NPN owner has two ways to acquire LS: i) to sub-lease it to a PLMN-Operator (PLMN-Op) upon establishing an agreement, or ii) to acquire it directly from national regulators. For the second case, national regulators are setting spectrum aside for verticals. For instance, Germany is releasing 3.7-3.8 GHz frequencies for industrial private 5G networks [21].

- **Shared Spectrum (SS)**: Third-party users share spectrum bands licensed to incumbent users (primary users) by means of database-assisted spectrum sharing models. For example, the Spectrum Access System sharing model enables the sharing of the Citizens Broadband Radio Service (CBRS) band in the USA.
- **Unlicensed Spectrum (ULS)**: Specific frequency bands might be used free of charge at any location and without access rules or restrictions, thus reducing the entry barrier for enterprise customers that want to deploy SNPNs. 5G supports two options for utilizing ULS, namely Licensed Assisted Access (LAA) NR-U and stand-alone NR-U [22], [23]. LAA NR-U enables combining ULS with other LS or shared spectrum acting as anchors. On the other site, stand-alone NR-U only uses ULS at either 5 or 6 GHz band, not requiring LS.

Besides the variety of options for spectrum access, the ranges of spectrum available might substantially affect the performance and the deployment of the private network. Millimeter waves (26 GHz and above) offer higher throughput, lower latency, and easier to confine their signals within private premises boundaries than mid-band spectrum (1 - 7 GHz). However, they require a high number of radiating points, which translates into denser radio deployments than mid-band.

B. INTEGRATION WITH LEGACY PRIVATE NETWORKS

Current factory networks are based on isolated Ethernet environments to connect devices such as sensors, actuators and controllers, and Wi-Fi deployments to support non-critical services, e.g., Radio Frequency Identification (RFID) readers. The integration of 5G with today's legacy private networks is essential to allow incremental updates of certain parts of the network, while others remain unchanged, thus lowering entry barriers for verticals. Also, it enables specific use cases as not all the devices (e.g., industrial controllers) will be connected wirelessly.

On the one hand, the integration of 5G with Wi-Fi has been addressed in 3GPP Releases 15 and 16 by means of the Non-3GPP Interworking Function (N3IWF). This function abstracts the complexity of each Wi-Fi access point making it appear as a single Next Generation NodeB (gNB) towards the UPF. On the other hand, the integration of 5G with wired networks might be particularly challenging. Whereas 5G can be easily integrated with IP L3, the interworking with L2 has to deal with critical aspects. For example, several approaches have been proposed in [24] for the transparent integration of 5G with L2 bridged networks. The integration of 5G with TSN [15], [22], [25], which is expected to replace Industrial Ethernet in tomorrow's industrial domains [26], exemplifies one of these approaches (refer to Section V-A for further details), where the 5GS acts as a set of virtual switches. For the integration with L2 non-bridged networks, which is not subject to 3GPP standardization, proprietary solutions are needed [24].

C. DETERMINISTIC TRANSPORT NETWORKS

The provision of URLLC services requires all the network domains have the ability to handle deterministic QoS sensitive traffic, including the Transport Network (TN). The TN is the domain in charge of providing connectivity among the distinct 5G components and out of the scope of 3GPP. There are two key requirements for TNs in NPNs [27], [28]:

- The TN shall support deterministic QoS provision, i.e., the ability to establish a multi-path connection over the network for streams transport with assured performance levels in terms of delay, jitter, frame loss, and reliability.
- The same TN infrastructure shall be able to accommodate all the heterogeneous private 5G services in order to lower costs.

TSN and Deterministic Networking (DetNet) [29] meet the requisites referred to above and are, therefore, appealing solutions for connectivity in NPNs. TSN is a set of standards specified by IEEE 802 aiming to define a converged layer 2 (L2) network technology that ensures the deterministic transport of the streams via IEEE 802 networks. On the other side, DetNet can be regarded as an extension of TSN to provide routes with deterministic QoS over Layer 3 (L3) routing segments. In fact, DetNet mainly relies on TSN standards to provide performance guarantees up to L2, though it is able to run over other underlying network technologies different from Ethernet.

D. POSITIONING

Positioning functionality enables the network to determine the geographic position and, optionally, the velocity of the User Equipment (UE). 5G includes built-in functionality to estimate the UE location based on Next-Generation Radio Access Network (NG-RAN) (i.e., network domain realizing the radio-related functions in the 5GS) radio signals measurements either at the UE or some NG-RAN nodes. Specifically, the propagation time, the direction, or the strength of the radio signal are used to estimate the UE position [30].

The UE positioning is especially important to enable manufacturing automation use cases like Augmented Reality (AR) applications, motion control, and Automated Guided Vehicless (AGVs) in factories. These use cases require UE localization with cm-level precision. Nonetheless, the 5G native positioning methods offer positioning errors below 3 m indoors and 10 m outdoors. Although upcoming 5G standard releases are expected to enhance the positioning accuracy, for the time being, we can only harness the onboard sensors in UE, e.g., cameras, Light Detection And Ranging (LiDAR), barometric and motion sensors, and laser reflectors, to meet the positioning requisites of the specific use case. 5G architecture includes Location Management Function (LMF) (see [31]) in the 5GC that could collect all the measurements from different sensors and sources to perform location estimations precisely, for instance, using sensor fusion techniques. In this way, with 5G we can provide a positioning solution that can be leveraged across technologies.

E. ON-PREMISES EDGE COMPUTING

Cloud adoption among enterprises continues to gain momentum. In the journey towards digital transformation, many enterprises now depend on the scale of the public cloud. They have learned to leverage a rich set of innovative cloud services, including databases, analytics, Internet of Things (IoT), and AI, to streamline and better manage their business processes. However, there exists a number of critical issues that make it difficult for enterprises to migrate their workloads and data to the public cloud. Most of them are related to security; in fact, these enterprises may have compliance, residency, and privacy constraints preventing data from leaving the premises. Other restrictions are related to functionality (e.g., the need to connect directly to onsite equipment) and performance (e.g., strict latency requirements or impossibility of transferring massive amounts of data to the cloud due to time constraints or available network bandwidth). On-premises edge computing solutions can be used to cope with the issues mentioned above.

On-premise edge computing is a concept that allows onsite workloads to benefit from cloud innovation. In 5G NPNs, these include telco functions and applications that need to run on-premises due to latency constraints (e.g., UPF), local data storage (e.g., UDM), or local data processing needs (e.g., AI/Machine Learning (ML)-based applications). Unlike the telco edge or public cloud, built with generic infrastructure capabilities that are enough to support most of the virtualized services, solutions for on-premises edge computing need to be right-sized and tailored to the specificities of targeted workloads in terms of computing capacity and features. For example, a UPF in charge of processing packets for critical industrial services requires a high level of QoS (e.g., throughput, latency, jitter) as well as predictable performance. However, this is not something that can be achieved by using traditional virtualization solutions (e.g., deploy the UPF as a Virtual Network Function (VNF) on commodity hardware), as the UPF packet-processing performance is significantly degraded due to technology limitations imposed by virtualization overheads. Another example is the AI/ML-based applications, which require high computation and memory capabilities and have a high-power consumption profile. The performance of these applications is also dependent on the available set (amount/diversity of data, data refreshing frequency) and how fast the existing model is re-trained with the new data set.

To meet the performance expectations of the onsite workloads while ensuring maximum utilization of infrastructure, on-premise edge computing solutions might need to build upon acceleration technologies (e.g., Smart Network Interface Cards (NICs), Peripheral Component Interconnect express (PCIe) cards, Field-Programmable Gate Array (FPGA), Graphics Processing Units (GPUs), etc.) [32] that complement x86 based environment. Compute-intensive tasks can be offloaded to software/hardware accelerators, with the rest of the workload operations performed by the Central Processing Units (CPUs) of general-purpose servers.

F. SECURITY AND PRIVACY FEATURES

Industrial networks have specific security requirements that are described in the IEC 62443 series of specifications [33], [34]. This standard defines four levels of security for different threat models spanning from SL1- protecting from any Internet user, to SL4 - protecting from government organizations. The introduction of 5G technology in Operational Technology (OT) industries needs to conform with these requirements.

5G leverages an advanced security toolbox, including mutual authentication between devices and the network and support for hardware security modules. In particular, 5G includes three authentication mechanisms: 5G-AKA, EAP-AKA' and EAP-TLS. The first two require a Universal Integrated Circuit Card (UICC) module in the client device (i.e., an (e)Subscriber Identity Module (SIM) module). The EAP-AKA' mechanism can be used by non-3GPP access networks such as Wi-Fi. In the case of EAP-TLS, no UICC module is required, which facilitates the introduction of this technology in IoT devices.

In SNPNs, the private network operator (PN-Op) that manages the NPN is in charge of authorizing devices, which can be done through any of the authentication mechanisms above. In PNI-NPNs, the PLMN-Op managing the NPN can only use the first two authentication mechanisms above for authorizing the devices against the public network. In addition, 3GPP Release 16 has defined a second level of authentication based on EAP [35] that allows private network operators to provide their own access control in a PNI-NPN scenario implemented with a network slice.

Additionally, industrial networks have traditionally been physically isolated forming a single trust domain within their perimeter. However, in the case of PNI-NPN, the PLMN-Op represents a separate trust domain. This requires means that guarantee the privacy of the OT network data. Such means may include end-to-end encryption and integrity protection, as well as isolation of operational and subscription information.

From Release 16 on, 3GPP defines advanced security and privacy mechanisms for the support of NPNs [16]. These mechanisms provide solutions related to device-to-network communications, including device authentication (with the possibility of the enterprise customers to implement a second authentication in the local Data Network), end-to-end traffic integrity and encryption (at both user and control planes) and device credentials management. Additionally, other infrastructure related solutions should be considered. Examples include remote attestation (ETSI NFV-SEC defined transitive mechanism ensuring trust and liability for the VNFs and underlying infrastructure) and proof-of-transit (allows for external verification in the compliance of traffic forwarding policies, ensuring packets traverses processing nodes as mandated) [36].

G. OPEN RAN

The O-RAN Alliance [37] is defining an architecture to deploy 5G networks based on disaggregation and open interfaces. The main innovations introduced by the O-RAN architecture are as follows:

i. Standardized fronthaul interface between the Remote Unit (RU) and the Distributed Unit (DU).
ii. Standardized control plane interfaces (E2) between a new entity known as the near real-time RAN Intelligent Controller (nrt-RIC), and the control plane of the Centralized Unit (CU) component of the 5G base station.
iii. The possibility of plugging in additional control plane functions in the nrt-RIC, known as xApps.
iv. An interface to allow a management plane entity, known as the non real-time RIC, to police the behavior of the xApps running in the nrt-RIC.

The previous O-RAN innovations impact the deployment of NPNs in different ways. First, standardized interfaces between RUs and DUs contribute to opening the supplier ecosystem, which is key to lowering the price of NPN deployments. Second, the introduction of the nrt-RIC and the concept of xApps is a key feature to enable customization of NPNs in industrial environments. For example, one could imagine a factory floor where the handover offsets or neighbor tables delivered to a mobile robot are tailored to the trajectory followed by the robot (see O-RAN use cases and deployment scenarios in [38]). Finally, the introduction of the non real-time RIC opens the door to creating mobile network related data lakes that can be interconnected with other industrial data spaces and fed to Machine Learning algorithms to enhance end-to-end efficiency of industrial processes, as envisioned by Industry 4.0.

IV. 3GPP RELATED STANDARDIZATION

In this section we provide an overview of the 3GPP Release 16 capabilities to support NPNs and network sharing.

A. 3GPP SUPPORT FOR NON PRIVATE NETWORKS

According to 3GPP specifications [22], NPNs are categorized into SNPNs and PNI-NPNs:

1) STAND-ALONE NPN

It is a NPN that operates without dependency on a PLMN, i.e., not relying on network functions provided by a PLMN. It requires a 5GS separated from the PLMN, and NPN devices must have a subscription to the SNPN in order to access it. An SNPN is uniquely identified by the combination of a PLMN ID and a Network ID (NID). Thus, UE is configured with the tuple {PLMN ID, NID} to access an SNPN. The PLMN ID may be a private network ID (e.g., based on mobile country code (MCC) 999 as assigned by ITU for 3GPP), or the ID of a PLMN that is operating that SNPN. The NID could be self-assigned (i.e., chosen by SNPN at deployment time) or coordinated assigned (universally managed NID) [22].

There are situations in which an UE needs to obtain PLMN services while camping in a SNPN, e.g., access to data and voice services. For these situations, 3GPP has defined a procedure that allows the SNPN registered UE to perform another registration to the PLMN through the NPN user plane. A symmetric scenario allows to access SNPN services from a PLMN. This procedure is an ‘‘over-the-top’’ solution consisting of two steps. In a first step, the UE uses the NPN subscription to get a data connection to the Internet. Then, the UE uses the PLMN subscription to get access to the 5GC of the PLMN using the architecture for ‘‘untrusted non-3GPP access’’ defined in [22], for example, by establishing an IPSec tunnel with an N3IWF (Non-3GPP Interworking Function) node of a PLMN.

2) PUBLIC NETWORK INTEGRATED NPN

It is a NPN deployed with the support of a PLMN. NPN devices must have a subscription to the PLMN in order to access the PNI-NPN. According to [22], a PNI-NPN may be provided by a PLMN by means of a dedicated Data Network Name (DNN) or by deploying network slices allocated for the NPN.

- Provision as a DNN: In this case, the PNI-NPN is provided as a data network, which is used for hosting the NPN services and applications. The DNN identifies the data network, and whenever the subscriber executes the NPN application, the UE triggers the establishment of a Protocol Data Unit (PDU) session to the NPN DNN. As typically NPNs provide services within a limited coverage area, the 3GPP has standardized the concept of Local Area Data Network (LADN), which enables access to the DNN in a given area (e.g., stadium or museum), but not outside. The LADN service area is defined as one or several Tracking Areas (TAs). A TA is a group of cells where a user can move around without updating the Access and Mobility Management Function (AMF). When the UE is inside the LADN service area, it can request a PDU session establishment for the LADN DNN, and the network will grant such PDU session. The PLMN-Op can use the UE Route Selection Policy (URSP) rules to control the PDU session request from the UE when this is inside (or outside) the LADN service area.
- Provision as a network slice: Network slicing is a technological solution that provides isolated logical networks with diverging performance requirements over a common network infrastructure. A 5G network slice is composed of the 3GPP 5GS network functions (e.g., gNBs, AMF, UPF, Session Management Function (SMF), etc.), it is identified by a Single Network Slice Selection Assistance Information (S-NSSAI), and it consumes a certain amount of radio resources in each cell. A PLMN-Op can use network slicing to provide public network services, or NPN services,

i.e., a PNI-NPN. The PLMN-Op can deploy one or several dedicated network slices for the PNI-NPN, if NPN isolation or specific QoS treatment is desired. The customer can consume the received slice directly, or optionally extend it with additional features (e.g., device on-boarding, secondary authentication). Using network slicing for the PNI-NPN allows to control the access to the NPN because the subscriptions to the dedicated S-NSSAIs can be restricted to the NPN devices. In PNI-NPNs, the UE needs to be pre-configured with the S-NSSAI to access the slice. The PLMN-Op can also use the URSP rules for this purpose.

A relevant requirement of a NPN is that it can control the access of NPN devices to the network in areas in which they are not permitted to. However, as in the case of LADN service area, network slices are set on a per TA basis [22]. That is, neither LADN nor network slicing allow the possibility to prevent UEs from automatically selecting and accessing specific cells within a TA. Closed Access Groups (CAG) may optionally be used in NPNs for this purpose. A CAG defines a list of subscribers who are allowed to access a CAG cell associated with it. A CAG cell is a cell that only UEs supporting CAG can access. Hence, CAG can be used in PNI-NPNs to prevent unauthorized UEs to access specific CAG cells inside a private venue (e.g., stadium or museum). Please note that CAGs are independent from any network slice.

B. NETWORK SHARING

Network sharing is a key technical feature in 5G. 3GPP specifications for 5G provide support only for Multi-Operator Core Network (MOCN) sharing architecture [22]. In the MOCN architecture, the NG-RAN segment (including RAN infrastructure, functionality, and spectrum carrier) is shared among multiple independent network operators, while the 5G Cores are owned by each of them. The NG-RAN sharing functionality has been extended in Rel-16 to support MOCN scenarios involving NPNs [22]. Specifically, the supported scenarios allow to share the NG-RAN among any combination of PLMNs, SNPNs, and PNI-NPNs (with CAGs).

In MOCN architecture, each cell of the shared NG-RAN must radiate the PLMN IDs and NIDs of the available PLMNs and SNPNs, respectively, through the Broadcast System Information (BSI) for selection by UE. Additionally, the PLMNs and/or SNPNs must be the same for all cells of a TA. The BSI also includes additional parameters per PLMN, such as cell ID, TAs, and CAG IDs. In the current version of 3GPP specifications a cell ID may only be associated with one of the following options: one or several SNPNs, one or several PNI-NPNs (with Closed Access Group (CAG)), or one or several PLMNs [22].

V. SINGLE-SITE NPN ARCHITECTURES

This section presents the architectures for single-site NPNs.

A. STAND-ALONE NPN ARCHITECTURE

The baseline SNPN consists of a private 5GS, comprising a NG-RAN and a lightweight 5G Core (5GC). The NG-RAN includes a set of gNBs providing indoor 5GNR coverage. The 5GC follows a Service Based Architecture (SBA) with control and user plane separation, i.e., it is designed with a 5G Core Control Plane (5GC-CP) decoupled from UPFs that build up the user data path. While the UPFs are always deployed on-premises with edge computing (see Subsection III-E), the 5GC-CP might be partially executed off-premises. The 5GC-CP can be hosted off-premises by 3rd party cloud providers, typically hyperscalers (e.g., AWS). Please note that some of these cloud providers also offer to bring their infrastructure and services on-premises (e.g., AWS Outposts), which could facilitate the complete SNPN deployment on-premises.

In SNPNs, the enterprise customer or a delegating company may take the role of NPN operator, thereby acting as a μ Operator [39]. Alternatively, the enterprise customer may ask a PLMN-Op to take the NPN operator role.

One of the main use cases for an SNPN is a smart factory with industry 4.0 services that leverages 5G wireless connectivity capabilities. Figure 2 captures an archetypal architecture of this SNPN. To better clarify the decoupling between functionality and infrastructure resources, the figure has been split into two separate strata: the infrastructure stratum and network function stratum (lower and upper figure side, respectively).

On the one hand, the infrastructure stratum represents the on-premise physical network substrate that hosts the SNPN. It comprises a set of wireless access nodes and a clustered NFV Infrastructure (NFVI), with a transport network providing TSN connectivity along the entire data path (see Subsection III-C for further details on deterministic transport networks). The wireless access nodes include gNBs providing small cell 5GNR connectivity and Wi-Fi access points. Optionally, gNBs functional split could be considered if required. To that end, NFVI could be enhanced with hardware/software acceleration solutions for real-time processing of the virtualized gNB functions (see Subsection III-E).

On the other hand, the network function stratum represents the different functional components building up the SNPN. Note that the SNPN includes four different network segments: 5GS (i.e., NG-RAN, UPF, 5GC-CP), Wi-Fi, TSN and the local data network. In the *5GS*, UPFs and 5GC-CP are executed as VNFs on the edge cluster, while NG-RAN consists of gNBs deployed as physical network functions. The *Wi-Fi* segment, with technology features provided by underlay Wi-Fi access points, combined with the N3IWF, complements the 5GNR connectivity capabilities provided by gNBs. This segment allows increasing the reliability and throughput at the access side leveraging on multi-access connectivity features (e.g., traffic offloading, bandwidth aggregation), as well as enables the integration with the legacy network (see Subsection III-B for further details on interworking with

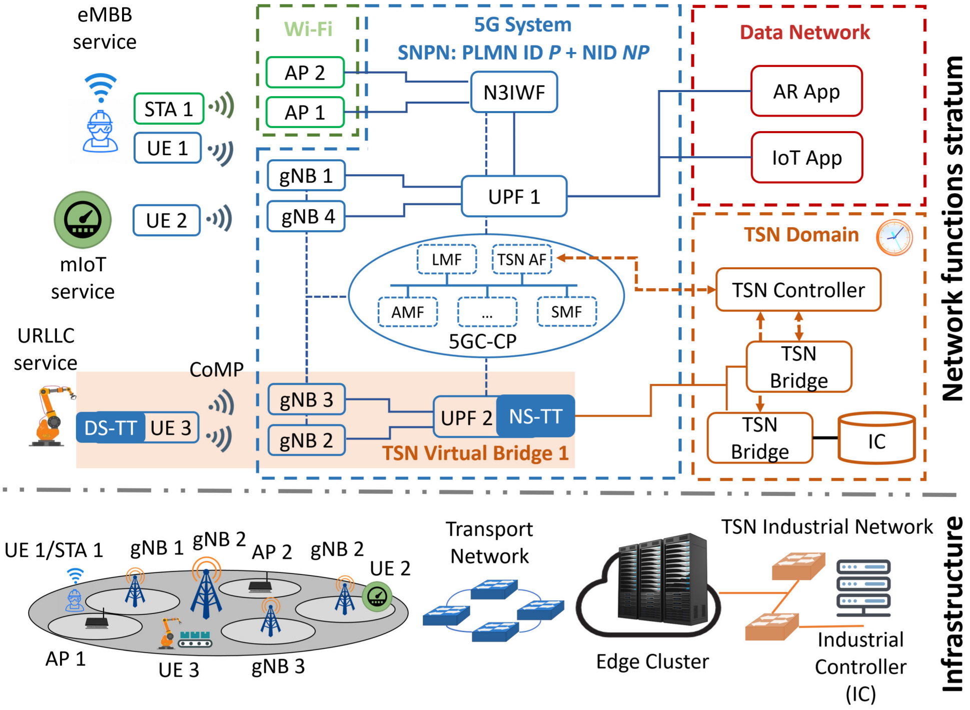


FIGURE 2. SNPN architecture.

legacy networks). The *TSN* segment (domain) allows providing deterministic QoS wired access in the SNPN, which is key for typical URLLC-type industry 4.0 services where a wireless station (e.g., industrial robot) is operated by an industrial controller (IC) connected to the TSN industrial network. For these services, the 5GS behaves as a set of TSN bridges (one per UPF). The integration of 5GS and TSN requires the use of TSN translation modules (e.g., Device-Side TSN Translator (DS-TT) and Network-Side TSN Translator (NS-TT)) at the 5G entities interfacing with the TSN network, i.e., UE and UPF. The TSN controller transparently configures the 5GS as if it is a TSN bridge through the TSN AF. For more information on 5G-TSN interoperability, refer to [22], [25]. Finally, the *local data network* allows hosting the applications (e.g., IoT app, AR app) that provide the service logic.

Although not captured in the figure, it is worth noting that network slicing can be used in SNPN to differentiate traffic from different industry 4.0 services.

B. PNI-NPN ARCHITECTURE

PNI-NPNs represent a reduced OPEX/CAPEX deployment option compared to SNPNs as they may leverage the PLMN-Op's infrastructure, spectrum, and know-how. As described in Section IV-A2, the PLMN-Op may provide the PNI-NPN by means of a DNN or a dedicated network slice.

The implementation of the PNI-NPN presents several issues:

- The on-premise 5GNR connectivity: the gNBs deployed in-house can be owned by the enterprise customer (e.g., purchased directly to the network equipment provider) or made available by the PLMN-Op.
- The ability to dedicate and customize the PNI-NPN: the PLMN-Op can configure the PNI-NPN in terms of functionality and capacity according to the enterprise customer's needs by provisioning network and application functions specifically dedicated and adjusted to the NPN requirements. For example, the PLMN-Op may deploy a customer-tailored, lightweight 5GC that includes only the network functions (UDM, AMF, SMF, Network Repository Function (NRF), UPF) and with the specific capacity as required by the private services.
- The location of the PNI-NPN functions: some NPN scenarios require the network functions to be executed on the customer premises, either for performance or privacy reasons (see Subsection III-E). For example, the UPF may be deployed onsite to reduce the latency. The UDM may also be executed on-premises to keep subscription data locally stored (see security and privacy features in Subsection III-F).
- The UE access control: the PLMN-Op can enforce the access control by means of the CAG, LADN, and network slicing mechanisms as described in Section IV.

Figure 3 captures an archetypal architecture for PNI-NPN scenarios realized through network slicing. The figure illustrates two coexisting PNI-NPNs, both provisioned by the PLMN-Op as separate network slices. The gNBs broadcast the PLMN ID for individual PNI-NPNs. One of the slices, whose Slice/Service Type (SST) is URLLC, is destined for

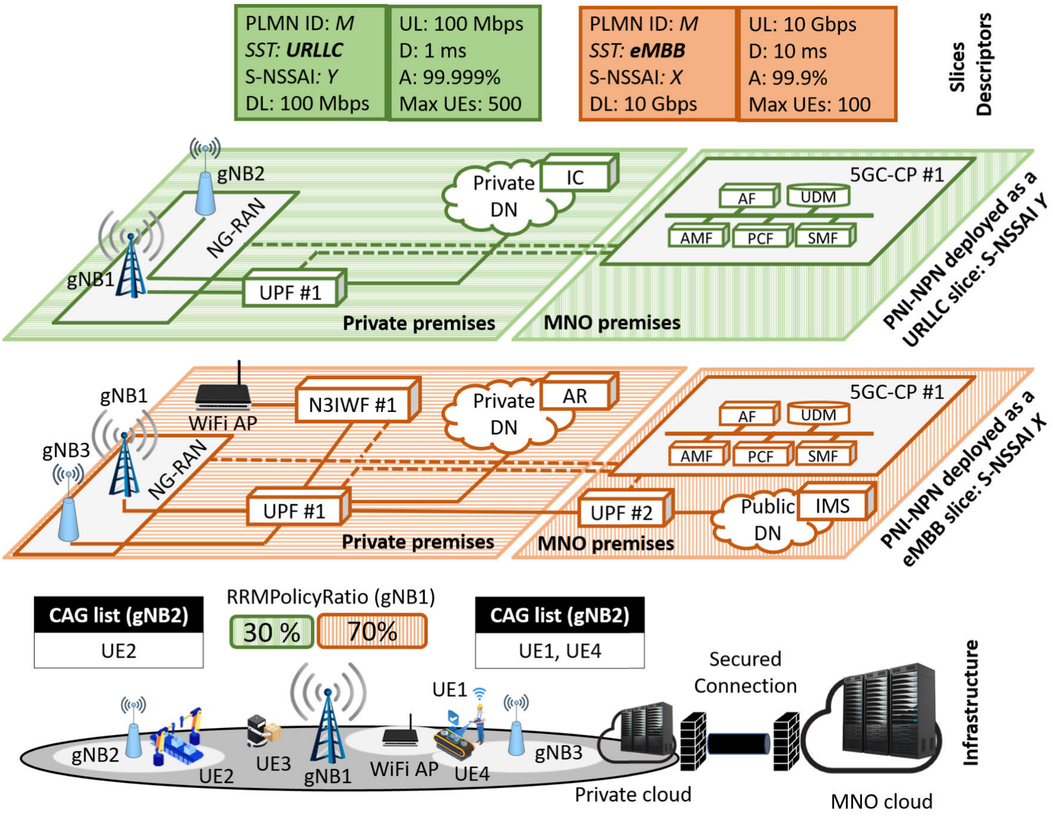
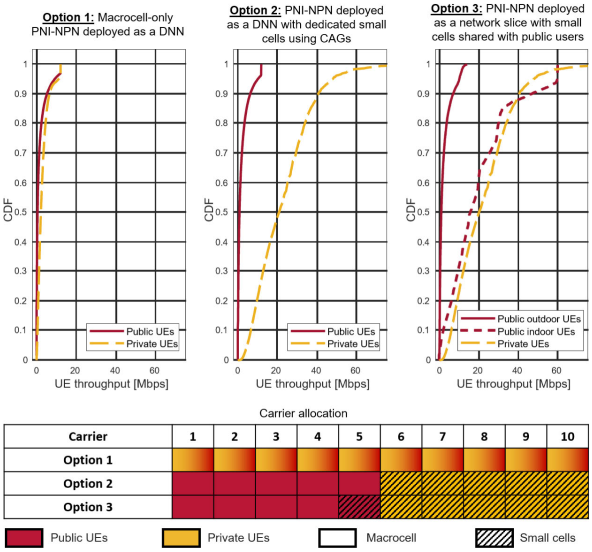


FIGURE 3. PNI-NPN architecture.

industrial critical applications. The second network slice provides access to enhanced Mobile BroadBand (eMBB) services to the workers of the industry. This eMBB slice integrates Wi-Fi access through the N3IWF, which is also located on-premises. The PLMN-Op instantiates a UPF on-premises in the edge cluster and dedicates it to the URLLC slice. In this way, the critical traffic is kept in-house, and its latency constraints can be met. On the other hand, the UPF for the eMBB slice and the 5GC-CP (shared by both slices) are hosted in the PLMN-Op's edge cloud.

For a DNN-based implementation of a PNI-NPN please refer to [40].

Figure 4 shows a comparison of the UE throughput in an industry campus for three deployment options. The setup considers 25 private users located inside three factory plants and 25 public users located inside and outside the factory plants. We consider that UE cannot connect simultaneously to the public and private networks (i.e., they have a single SIM). The deployment options are: 1) all users are served by a macrocell, and a PNI-NPN is deployed as a DNN for the private users; 2) the macrocell serves the public users, whereas private users are served by small cells with CAGs located in the factory plants, and the PNI-NPN is again deployed as a DNN; and 3) the macrocell serves public outdoor users, whereas indoor public and private users are served by the small cells, and the PNI-NPN is deployed as a network slice. The system bandwidth is 100 MHz. It is split into ten carriers of 10 MHz each. Fig. 4 includes the carrier allocation among public and private users.



Carrier	1	2	3	4	5	6	7	8	9	10
Option 1	🟨🟥	🟨🟥	🟨🟥	🟨🟥	🟨🟥	🟨🟥	🟨🟥	🟨🟥	🟨🟥	🟨🟥
Option 2	🟥	🟥	🟥	🟥	🟥	▨🟨	▨🟨	▨🟨	▨🟨	▨🟨
Option 3	🟥	🟥	🟥	🟥	▨🟥	▨🟨	▨🟨	▨🟨	▨🟨	▨🟨

🟥 Public UEs 🟨 Private UEs □ Macrocell ▨ Small cells

FIGURE 4. Throughput achieved by a PNI-NPN in an industry campus network for three deployment options.

As observed, for deployment option 1) the UE throughput is similar for both public and private users. For option 2) the throughput of private UEs significantly increases as they are served by the small cells with CAGs. For option

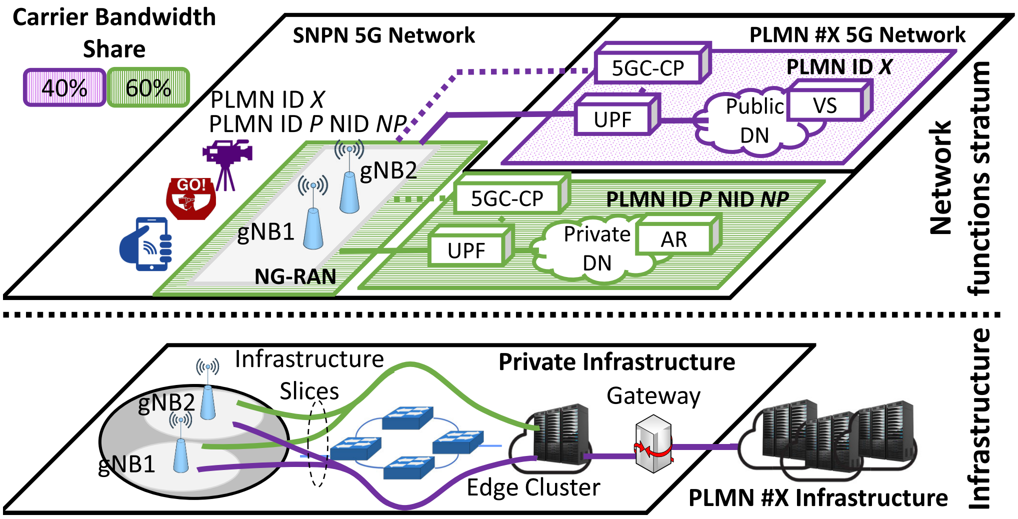


FIGURE 5. On-premises NG-RAN sharing through MOCN architecture.

3), network slicing enables allocating one carrier for public use in the small cells, thus improving the throughput of the indoor public UEs. Note that, in the considered simulation setup, the number of public indoor UEs connected to the small cells is reduced, resulting in the staircase effect observable in Figure 4 (option 3). In particular, changing the actual number of public indoor UEs connected to a small cell (i.e., from 1 to 2 UEs, from 2 to 3 UEs, and so on) causes transitions in the UE throughput (e.g., from 60 to 30 Mbps or from 30 to 20 Mbps). This effect is not observable for private indoor UEs because there are a higher number of them and their slice has a larger bandwidth allocation.

C. ON-PREMISES RAN SHARING SCENARIO AND ARCHITECTURE

In a MOCN architecture for a private venue scenario, a Network Operator (NOP) deploys and operates an indoor small cells infrastructure, and opens this infrastructure and the spectrum to other NOPs for the provision of communication services. We will refer to the first NOP as the Master NOP (MNOP) and the remaining ones as Participating NOPs (PNOPs). Each PNOP, and possibly the MNOP, employs its own 5GC to deploy SNPNs or PNI-NPNs (with CAGs). Additionally, a PLMN-Op may also participate in the sharing with its own 5GC to merely extend the footprint of its public services inside the private venue. For the MOCN scenario, we identify the following possibilities:

- The MNOP is a PLMN-Op. In this case, the MNOP has primary access to a particular licensed spectrum which shares together with its NG-RAN infrastructure with the PNOPs.
- The MNOP is a μ Operator. In this case, the venue owner or delegating company takes the role of MNOP and leases the NG-RAN to the PNOPs. The main difference with the previous case is that the μ Operator does not have primary access to a particular licensed spectrum, and instead it requires a locally issued spectrum license. As mentioned in Subsection III-A, the μ Operator has several alternatives to access spectrum in this situation.

The MOCN architecture is well suited for private venue scenarios as it enables multi-tenancy in the 5GS network, which makes it possible for various NOPs to provide communication services while sharing the NG-RAN. Some exemplary use case scenarios are a smart stadium, a shopping mall or a hospital, in which several NPNs could be deployed to provide various private localized services.

Figure 5 depicts an architecture blueprint of such a MOCN deployment. The PNOPs act as tenants and interact with the MNOP to negotiate SLAs and request NG-RAN resources on demand. Under such requests, the MNOP has to allocate portions of network capacity to the PNOPs for a particular time period. Therefore, the NG-RAN network resources are to be sliced and delivered to each PNOP. Hereafter, we will refer to these resources as an infrastructure slice. This infrastructure slice comprises the set of wireless, virtualized computing and networking resources of the NG-RAN infrastructure, which are segregated and provided to a PNOP. It is worth noting that the PNOPs, armed with a 5GC, may advertise multiple 3GPP network slices, i.e., S-NSSAI, within their infrastructure slice, with each 3GPP slice having specific requirements in terms of network resources. Additionally, the NG-RAN architecture also has to expose the corresponding interfaces to PNOPs for network resource requests, service monitoring, and network management capabilities.

VI. MOBILITY AND MULTI-SITE NPN SCENARIOS

This section describes, motivates, and explores technical alternatives for mobility between NPNs and multi-site NPNs.

A. MOBILITY IN NPNs

Several promising private applications require the devices to move out of the private premises, such as an unmanned aerial vehicle fleet that needs to monitor crop growth in

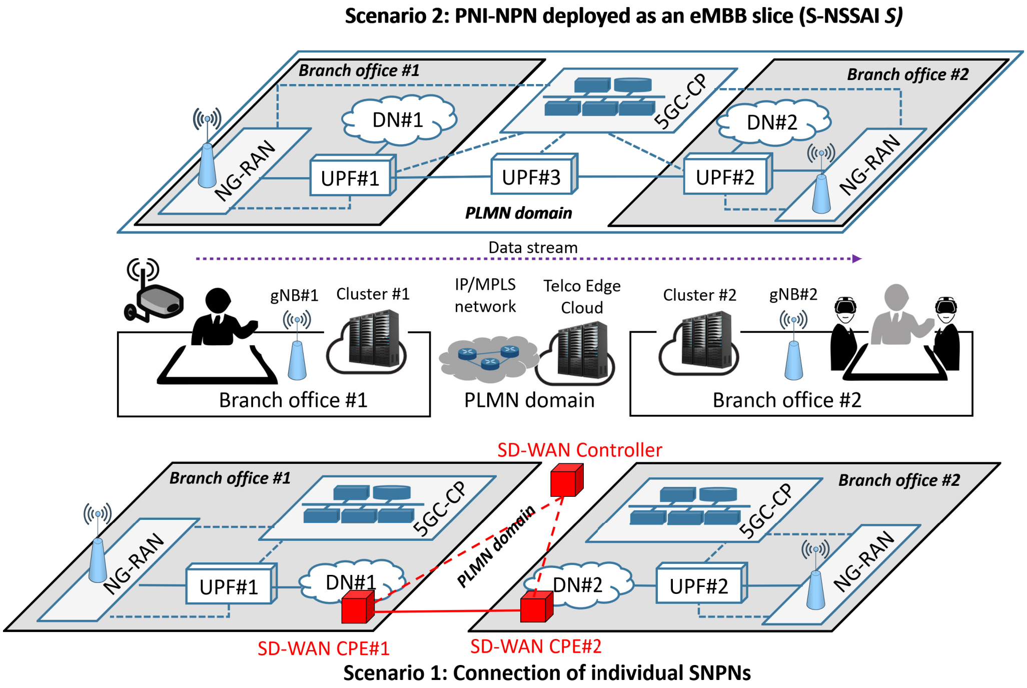


FIGURE 6. Candidate multi-site NPN deployments.

agriculture, deliver a package in logistics, or even move between private sites (e.g., factories). For example, real-time tracking of goods when they are moved between manufacturing, distribution, and retail centers, or even later incorporating those goods into the local factory inventory management system in an automated manner. These scenarios entail a PLMN that supplies wireless access out-of-premises and mechanisms to warrant Session and Service Continuity (SSC), i.e., to provide UEs with a seamless service experience, when devices leave or enter the NPN coverage area.

The specific solution to provide the services referred to above with SSC depends on the NPN deployment option: PNI-NPN or SNPN. For PNI-NPNs, the PLMN furnishes radio access both inside and outside the private premises. Then, ordinary intra-PLMN handover procedures are triggered when the UEs exit or enter the private venue's inner perimeter. These procedures ensure the SSC to the UEs when they cross the private venue borders. Typically, SNPNs only provide radio access on-premises, whereas a PLMN is needed to support 5G connectivity outside. Thus, either the UE has a Dual SIM and a subscription with the PLMN, a roaming agreement between the SNPN and the PLMN is required to enable private UE to maintain the connectivity out-of-premises. Here, we focus on the second option as many commercial mobile end devices, such as most IoT sensors, are equipped with a single SIM.

3GPP Release 16 allows for inter-PLMN mobility procedures with SSC assurance for both local breakout and home-routed roaming scenarios. The same procedures might be used when the private UEs roam from the SNPN to the PLMN. Support of mobility between the SNPN and the PLMN imposes specific requisites on the roaming agreement. For instance, there shall be direct communication between 5GC-CPs in the two networks. On the one hand, the public UDM/Home Subscriber Server (HSS) needs to do an onboarding of the UE subscription data by requesting them to the private UDM/HSS. On the other hand, the public and private 5GC entities must interact to carry out the corresponding handover procedures.

B. MULTI-SITE NPN

A multi-site NPN scenario represents a deployment use case whereby NPN provisioning aims at serving a given enterprise customer whose facility includes two or more sites, e.g., branch offices. Depending on the use case, a multi-site NPN scenario can represent (i) a connection of individual SNPNs, each deployed locally at every branch office; (ii) a single PNI-NPN (see Fig. 6).

The first category is typical for industry 4.0 enterprises, where independent 5G-enabled manufacturing tasks are executed at individual branch offices. The branch offices need to communicate between them to only exchange industry-specific data (e.g file exchange, database accessibility); this means that no signaling/data plane 5G traffic is exchanged among individual SNPNs. For this communication, a plausible solution is to set up an overlay connectivity service (e.g. software-Defined Wide Area Network (SD-WAN), layer 3 virtual private network (L3VPN)) atop the PLMN-Op's underlay substrate (e.g. IP/MPLS). In these setups, the enterprise customer demands the data to be protected when travelling across sites through the transport network. Now that the 3GPP 5G in-built security features no longer apply in this inter-site communication (see Section III-F), the transport network operator needs to find workarounds. One solution is to use LxVPN services (e.g. L2VPN or L3VPN) with IPSec in the underlay, which ensures confidentiality (avoids external visibility on exchanged traffic) and integrity (prevents payload modification, e.g., Denial of Service (DoS) and fraud). This carrier-grade solution, widely used in today's enterprise connectivity services, may remain valid for quite a large portion of customers in the multi-NPN category. However, it is also true that there exists some customers that may demand add-on security features in this connectivity, because of their business requirements. In such cases, more advanced yet costly solutions can be used, for example the use of 3GPP Security Edge Proxy Protection (SEPP) instances on individual sites.

In the second category, it is assumed there exists a single 5GS for the entire facility. Unlike the first category, (i) the traffic across facility sites is entirely protected under the umbrella of 3GPP 5G security framework, and (ii) the 5GS is now partially hosted by the PLMN. Typical layouts in this category consists in having lightweight branch offices, keeping user plane on premises and offloading 5GC-CP complexity towards a PLMN-Op's edge node. The resulting deployment scenario is formed of a set of branch offices, each hosting a CP-less 5GS (i.e., RAN and UPF), and a PLMN-Op's edge node, which hosts 5GC (i.e., 5GC-CP and UPF).

The latter scenario may fit for customers requiring the use of eMBB capabilities among branch offices, for the delivery of 5G media services such as UHD video streaming (e.g., telepresence in council meetings) and XR video experience (e.g., AR assisted supervision on a remote factory). In both cases, the service consists in streaming video traffic from one branch office towards one or more remote offices, leveraging traffic casting (e.g., unicast/multicast/broadcast) mechanisms as needed. The on-premise UPF from source branch office, which performs UL Classifier (UL-CL) functionality, receives incoming IP packets corresponding to video service. Grouped in a PDU session, these IP packets are encapsulated in a GTP tunnel before their delivery to the PLMN hosted UPF. This UPF, deployed at PLMN-Op's edge node and performing the PDU Session Anchoring (PSA) functionality, receives the encapsulated sessions and applies necessary traffic casting policy to route them towards end branch offices, where local UPFs proceed with the GTP tunnel decapsulation, so IP packets can reach end users. In the overall process, participant UPFs are in charge of keeping 5QI-to-DSCP mapping (i.e., translation of 3GPP 5G QoS indicators into IP QoS indicators), so the QoS can be assured along the IP/MPLS substrate which connects the different branch offices.

VII. CHALLENGES

In this section, we identify some of the key challenges and future research directions arising from realizing 5G NPNs. It is worth mentioning that some existing works have also identified additional challenges related to the realization of 5G NPNs [3], [6], [10], [11] to those covered here. In [10], the authors identify the challenges to achieve precise synchronization in 5G to support private use cases. The authors in [11] address the challenges of handling traffic in PNI-NPNs. A brief discussion on the architectural and operational challenges is included in [6]. Finally some challenges related to network slicing resource allocation, 5G and TSN integration, standardization and the adoption of open innovation ecosystems for private 5G are presented in [3]. For example, the need for validation and conformance testing of the programmable hardware is claimed in [3]. We refer the interested reader to those works for further details on the aforementioned challenges.

A. ZERO-TOUCH PRACTICES ON NPN MANAGEMENT

A simplified management of the NPN and a smooth integration in the IT infrastructure of the enterprise customer are key challenges for the success of 5G NPNs. To achieve those goals, NPNs have to embrace full automation in network and service orchestration and implement extensive zero-touch management approaches. The realization of this vision in SNPN leverage two principles: Artificial Intelligence (AI) and Intent-based interfaces. 3rd parties like μ Operator can help enterprise customers to integrate these principles into their management stack solutions.

On the one hand, the introduction of AI principles allows for data-driven, self-X network and service management, minimizing the intervention of the NPN operator (i.e. the enterprise customer or the delegating company). Decisions that currently take slow human interactions, based on carrier-grade network characterization and optimization methods, should be autonomously performed by (ML) algorithms with a holistic view of the network, enabling software components to directly contribute into decision-making activities related to the SNPN management. Despite the general applicability of ML-based solutions, their practical application often relies on the possibility to access real-time data to perform analytics and diagnosis. To that end, further research work on data aggregation mechanisms (e.g., model-based streaming telemetry) need to be made.

On the other hand, the design of intent based language will allow the NPN operator to interact with the NPN resources, functions and services using business primitives, instead of low level network configuration. With the use of an intent-based northbound interface, the NPN operator can operate the NPN in an user-friendly manner, by issuing expectations (intents) rather than specific network control/orchestration requests. Before getting this intent-based northbound ready for use, it is needed to understand how business intents are to be described and translated into enforceable goals and actions at resource, network and service layers. This requires further innovation and research work ahead on intent modelling, specially on intent decomposition, intent monitoring and intent assurance. Much of these aspects are still on early discussion, in both industry fora (e.g. TM Forum initiative on autonomous networks) and standardization bodies (e.g. 3GPP SA5 and ETSI Zero touch network & Service Management (ZSM)).

B. MULTI-WAT IN 5G NPNs

Multi-Wireless Access Technology (WAT) is appealing to affordably improve the 5G NPNs performance. Many of the current private networks are based on Wi-Fi deployments for wireless connectivity. Thus, the integration of Wi-Fi with 5GNR in 5G NPNs reduces the entry barrier and enhances their QoS by leveraging the already deployed infrastructure. The integration of 5G with Wi-Fi has been addressed in 3GPP Releases 15 and 16 by means of the N3IWF. This function abstracts the complexity of each Wi-Fi access point making it appear as a single gNB towards the UPF. Nonetheless, it is still required to devise and develop smart mechanisms that allow to easily combine 5GNR and Wi-Fi to provide advanced connectivity with improved reliability and throughput. For example, solutions to decide when switch, split or steer the eMBB traffic through the available WATs according to a given goal or SLA. Besides Wi-Fi, alternatives technologies like Light-Fidelity (Li-Fi) can also be integrated in multi-WAT 5G NPNs to further enhance their performance and increase the security of the wireless communications.

C. ENABLING AND VALIDATING 5G NPNs WITH E2E DETERMINISTIC QoS SUPPORT

One of the primary drivers behind 5G NPNs is the support for private critical services with stringent deterministic latency and reliability requirements, such as connected robotics and closed-loop control systems for industrial processes automation. However, they are still open questions about what is required, besides the URLLC capabilities included in recent 3GPP releases, to provide end-to-end (E2E) deterministic QoS support and which critical private services can be supported by 5G NPNs. In this regard, the E2E user plane operation (e.g., packets handling at every potential bottleneck) shall be deterministic, i.e., it is possible to derive analytical performance deterministic bounds of the E2E QoS metrics (e.g., delay, jitter, packet loss, and reliability). Otherwise, it is not possible to truly ensure that a given configuration of the 5G NPN meets the Service Level Agreement (SLA) of the private critical services. SLA violations might have a highly negative impact, e.g., long production downtimes in the factory or life-threatening in remote surgery. Therefore, the SLA violation probability must be known and kept within the specific safety margins for the particular critical service.

In addition to the data plane aspects, AI-empowered management planes are also a requisite to cope with the complexity of configuring the different domains (e.g., RAN, transport, and core) of the 5G NPNs and provide coherence among them, e.g., to ensure the E2E packet delay budget. However, analytical performance models are still essential to assist the AI algorithms in order to make them fully reliable. By way of illustration, let us assume an action issued by a reinforcement learning agent to configure the network. The feasibility of this configuration, i.e., ensuring that all performance requirements are fulfilled for this configuration, must be done analytically. Please note that corner cases performance is difficult to measure either experimentally or through simulation. Last, it shall be noted that analytical models might help speed up the training process of the ML models.

D. CAPABILITY EXPOSURE IN PNI-NPN

The previous challenges mainly apply for SNPNs scenarios. However, as described above, PNI-NPNs represent a reduced entry barrier option to have an NPN for some enterprise customers such as small and medium-sized enterprises (SMEs) or incumbent digital service providers. In PNI-NPNs, there are situations in which the customer enterprise wants to retain control and management of some specific parts of the network. In such a case, hybrid solutions can be defined, with PLMN-Ops taking the main control and management activities, while exposing needed capabilities to the enterprise customer. These capabilities can be of two types:

- Configuration related capabilities: this group of capabilities defines the ability of an enterprise customer to modify the parameters of certain network functions and infrastructure nodes. To that end, the PLMN-Op needs to characterize the permissions (i.e., isReadable, isWritable, isInvariant, isNotifyable) associated to these parameters accordingly.
- Assurance related capabilities: this second capability group defines the ability of an enterprise customer to subscribe to certain performance measurements and fault alarms, so that the customer can consume them in the format it sees more appropriate according to its business needs (e.g., for performance management, batches vs streaming).

To make capabilities available for consumption by the enterprise customer, the PLMN-Op shall have a business support system (BSS) hosted integration fabric in charge of mediating the request-response messages between the customer and PLMN-Op. It is important for the PLMN-Op to expose these capabilities in a controlled, secure and auditable way. To that end, the solution design for this integration fabric will require the implementation of an Application Programming Interface (API) gateway, together with mechanisms for token-based authentication and non-repudiation. However, how to build this solution is still unclear, and much work ahead is agreed in the telco industry community. On the one hand, it is still not clear for enterprise customers the capabilities they need to consume for their business processes; this is mostly due to their lack of knowledge/expertise with telco and networking issues. On the other hand, the PLMN-Ops need to think about the implementation of this BSS hosted integration fabric, with a particular focus on:

- the control, security and auditability implications of exposing these capabilities to the customer, specially considering multi-tenancy environments, where multiple customers will request the PLMN-Op to consume (potentially) different capabilities.

- the mapping of customer requests into network actions, and the API transformation behind this. In this regard, the PLMN-Op shall define mechanisms to map customer-facing, service APIs into low-level, internal network APIs.

VIII. CONCLUSION

In this article, we have provided an overview of 5G Non-Public Networks (NPNs). First, we have listed the primary requirements of 5G NPNs from an enterprise customer point of view. Next, we have given an overview of the key enabling solutions for 5G NPNs, including spectrum access options, deterministic transport networks, integration with legacy private networks, positioning, Open Radio Access Network (RAN), on-premises edge computing, and security and privacy features. These solutions play a relevant role to fulfill the requirements mentioned above and complement the capabilities defined in 3rd Generation Partnership Project (3GPP) standards to support 5G NPNs. We have also revisited most of these standardized capabilities.

Then, we have proposed and discussed the architectures for three single-site 5G NPNs, namely, Stand-Alone NPN (SNPN), Public Network Integrated NPN (PNI-NPN), and network sharing in NPNs. SNPNs do not rely on a public land mobile network (PLMN)-provided network functions, whereas PNI-NPNs are supported by a PLMN. SNPNs are suited for use cases that require independence from the PLMN. Deploying an NPN as an SNPN allows full-fledged customizability in terms of network functionality and performance, according to the enterprise customer's service needs, without restrictions on PLMN policies. The ability to retain complete control of the NPN behavior comes at the cost of higher CAPEX (e.g., purchase infrastructure resources, acquire 5GS functions) and OPEX (e.g., 5GS functions operation and software upgrades, 24/7 performance, and fault management activities) for the customer. Consequently, SNPNs entail a high entry barrier for most small and medium-sized companies. On the other hand, network sharing is also a key lever to reduce the entry barrier for some enterprise customers interested in deploying 5G NPNs. Moreover, it also fits the necessities of many private venues that cannot accommodate the deployment of several infrastructure networks due to physical space limitations or aesthetics.

Following that, we have discussed mobility in NPNs and multi-site NPNs. Some private-use cases need mechanisms to ensure Session and Service Continuity (SSC) when devices move out-of-premises. To that end, intra-PLMN handover procedures are sufficient in PNI-NPNs. However, in SNPNs, a roaming agreement between the SNPN and a PLMN is needed when the devices (e.g., sensors) are equipped with a single Subscriber Identity Module (SIM). Regarding multi-site NPNs, we have emphasized securing the communications between the remote NPNs. In contrast to scenarios where the NPNs are deployed as PNI-NPNs, the 3GPP 5G security framework does not apply to interconnect remote SNPNs. Thus, LxVPN services with IPSec in the underlay might be used as an affordable solution.

Finally, we have identified and discussed some challenges, such as those related to enabling truly end-to-end deterministic communications to support private critical services, for the success of 5G NPNs to unleash the full potential of the digital transformation in vertical industries.

REFERENCES

[1] *5G for Business: A 2030 Market Compass. Setting a Direction for 5G-Powered B2B Opportunities*, Ericsson, Stockholm, Sweden, Oct. 2019.

[2] *5G Non-Public Networks for Industrial Scenarios*, 5G-ACIA, Frankfurt, Germany, Jul. 2019.

[3] A. Aijaz, "Private 5G: The future of industrial wireless," *IEEE Ind. Electron. Mag.*, vol. 14, no. 4, pp. 136–145, Dec. 2020.

[4] P. Trakadas, L. Sarakis, A. Giannopoulos, S. Spantideas, N. Capsalis, P. Gkonis, P. Karkazis, G. Rigazzi, A. Antonopoulos, M. A. Cambeiro, S. Gonzalez-Diaz, and L. Conceição, "A cost-efficient 5G non-public network architectural approach: Key concepts and enablers, building blocks and potential use cases," *Sensors*, vol. 21, no. 16, p. 5578, Aug. 2021.

[5] X. Li, A. Garcia-Saavedra, X. Costa-Perez, C. J. Bernardos, C. Guimaraes, K. Antevski, J. Mangues-Bafalluy, J. Baranda, E. Zeydan, D. Corujo, P. Iovanna, G. Landi, J. Alonso, P. Paixao, H. Martins, M. Lorenzo, J. Ordonez-Lucena, and D. R. Lopez, "5Growth: An end-to-end service platform for automated deployment and management of vertical services over 5G networks," *IEEE Commun. Mag.*, vol. 59, no. 3, pp. 84–90, Mar. 2021.

[6] C. Guimaraes, X. Li, C. Papagianni, J. Mangues-Bafalluy, L. M. Contreras, A. Garcia-Saavedra, J. Brenes, D. S. Cristobal, J. Alonso, A. Zabala, J.-P. Kainulainen, A. Mourad, M. Lorenzo, and C. J. Bernardos, "Public and non-public network integration for 5Growth industry 4.0 use cases," *IEEE Commun. Mag.*, vol. 59, no. 7, pp. 108–114, Jul. 2021.

[7] T. Taleb, I. Afolabi, and M. Bagaa, "Orchestrating 5G network slices to support industrial internet and to shape next-generation smart factories," *IEEE Netw.*, vol. 33, no. 4, pp. 146–154, Jul./Aug. 2019.

[8] G. Soós, D. Ficzere, T. Seres, S. Veress, and I. Németh, "Business opportunities and evaluation of non-public 5G cellular networks—A survey," *Infocommun. J.*, vol. 12, no. 3, pp. 31–38, 2020.

[9] S. Filin, H. Murakami, K. Ibuka, H. Kawasaki, K. Ishizu, and F. Kojima, "5G and B5G technologies to implement private operators supporting high quality video production in dense user environments," in *Proc. 22nd Int. Symp. Wireless Pers. Multimedia Commun. (WPMC)*, Nov. 2019, pp. 1–6.

[10] I. Godor, M. Luvisotto, S. Ruffini, K. Wang, D. Patel, J. Sachs, O. Dobrijevic, D. P. Venmani, O. L. Moult, J. Costa-Requena, A. Poutanen, C. Marshall, and J. Farkas, "A look inside 5G standards to support time synchronization for smart manufacturing," *IEEE Commun. Standards Mag.*, vol. 4, no. 3, pp. 14–21, Sep. 2020.

[11] W. Y. Poe, J. Ordonez-Lucena, and K. Mahmood, "Provisioning private 5G networks by means of network slicing: Architectures and challenges," in *Proc. IEEE Int. Conf. Commun. Workshops (ICC Workshops)*, Jun. 2020, pp. 1–6.

[12] *5G for Connected Industries and Automation*, 2nd ed., 5G-ACIA, Frankfurt, Germany, Feb. 2019.

[13] *Key 5G Use Cases and Requirements—From the Viewpoint of Operational Technology Providers*, 5G-ACIA, Frankfurt, Germany, May 2020.

[14] *Service Requirements for Cyber-Physical Control Applications in Vertical Domains; Stage 1 (Release 16)*, document 3GPP TS 22.104, Version 17.7.0, Sep. 2021.

[15] Y. Kang, S. Lee, S. Gwak, T. Kim, and D. An, "Time-sensitive networking technologies for industrial automation in wireless communication systems," *Energies*, vol. 14, no. 15, p. 4497, Jul. 2021.

[16] A. Jerichow, B. Covell, D. Chandramouli, A. Rezaki, A. Lansisalmi, and J. Merkel, "3GPP non-public network security," *J. ICT Standardization*, vol. 8, no. 1, pp. 57–76, Jan. 2020.

[17] J. Ordonez-Lucena, J. F. Chavarria, L. M. Contreras, and A. Pastor, "The use of 5G non-public networks to support industry 4.0 scenarios," in *Proc. IEEE Conf. Standards Commun. Netw. (CSCN)*, Oct. 2019, pp. 1–7.

[18] A. Rostami, "Private 5G networks for vertical industries: Deployment and operation models," in *Proc. IEEE 2nd 5G World Forum (5GWF)*, Sep. 2019, pp. 433–439.

[19] X. Li, C. Guimaraes, G. Landi, J. Brenes, J. Mangues-Bafalluy, J. Baranda, D. Corujo, V. Cunha, J. Fonseca, J. Alegria, A. Z. Orive, J. Ordonez-Lucena, P. Iovanna, C. J. Bernardos, A. Mourad, and X. Costa-Perez, ''Multi-domain solutions for the deployment of private 5G networks,'' *IEEE Access*, vol. 9, pp. 106865–106884, 2021.

[20] D. Camps-Mur, M. Ghoraishi, J. G. Terán, J. Ordonez-Lucena, T. Cogalan, H. Haas, A. G. Gómez, V. Sark, E. Aumayr, S. van der Meer, and S. Yan, ''5G-CLARITY: Integrating 5GNR, WiFi and LiFi in private networks with slicing support,'' in *Proc. Eur. Conf. Netw. Commun. (EuCNC)*, pp. 1–2. Accessed: Oct. 6, 2021. [Online]. Available: https://upcommons.upc.edu/handle/2117/333746

[21] *5G Spectrum Vision*, 5G Amer., Bellevue, WA, USA, Feb. 2019.

[22] *System Architecture for the 5G System (5GS); State 2 (Release 16)*, document 3GPP TS 23.501, Version 16.5.0, Jul. 2020.

[23] *Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall Description; Stage 2 (Release 16)*, document 3GPP TS 36.300, Version 16.2.0, Jul. 2020.

[24] *Integration of Industrial Ethernet Networks with 5G Networks*, 5G-ACIA, Frankfurt, Germany, Nov. 2019.

[25] *Integration of 5G with Time-Sensitive Networking for Industrial Communications*, 5G-ACIA, Frankfurt, Germany, Jan. 2021.

[26] J. Prados-Garzon, L. Chinchilla-Romero, P. Ameigeiras, P. Muñoz, and J. M. Lopez-Soler, ''Asynchronous time-sensitive networking for industrial networks,'' in *Proc. Joint Eur. Conf. Netw. Commun. 6G Summit (EuCNC/6G Summit)*, Jun. 2021, pp. 130–135.

[27] J. Prados-Garzon and T. Taleb, ''Asynchronous time-sensitive networking for 5G backhauling,'' *IEEE Netw.*, vol. 35, no. 2, pp. 144–151, Mar. 2021.

[28] J. Prados-Garzon, T. Taleb, and M. Bagaa, ''Optimization of flow allocation in asynchronous deterministic 5G transport networks by leveraging data analytics,'' *IEEE Trans. Mobile Comput.*, early access, Jul. 26, 2021, doi: 10.1109/TMC.2021.3099979.

[29] A. Nasrallah, A. S. Thyagaturu, Z. Alharbi, C. Wang, X. Shao, M. Reisslein, and H. ElBakoury, ''Ultra-low latency (ULL) networks: The IEEE TSN and IETF DetNet standards and related 5G ULL research,'' *IEEE Commun. Surveys Tuts.*, vol. 21, no. 1, pp. 88–145, 1st Quart., 2019.

[30] R. Keating, M. Säily, J. Hulkkonen, and J. Karjalainen, ''Overview of positioning in 5G new radio,'' in *Proc. 16th Int. Symp. Wireless Commun. Syst. (ISWCS)*, 2019, pp. 320–324.

[31] *5G System (5GS) Location Services (LCS); Stage 2 (Release 16)*, document 3GPP TS 23.273, Version 16.4.0, Jul. 2020.

[32] G. Yigit and C. Chappell, ''Acceleration technologies: Realizing the potential of network virtualization,'' Analysys Mason, Multinat. Group, White Paper, Jun. 2019.

[33] B. Leander, A. Čaušević, and H. Hansson, ''Applicability of the IEC 62443 standard in industry 4.0/IIoT,'' in *Proc. 14th Int. Conf. Availability, Rel. Secur. (ARES)*. New York, NY, USA: Association for Computing Machinery, Aug. 2019, pp. 1–8.

[34] *Security Aspects of 5G for Industrial Networks*, 5G-ACIA, Frankfurt, Germany, May 2020.

[35] *Security Architecture and Procedures for 5G System (Release 16)*, document 3GPP TS 33.501, Version 16.0.0, Jul. 2020.

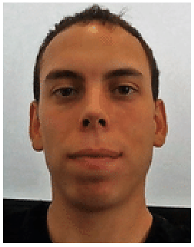
[36] G. Millar *et al.*, ''5G security: Current status and future trends,'' INSPIRE-5Gplus, Eur. Project, Deliverable, 2.1 Version 1.0, May 2020.

[37] *O-RAN Architecture Description 4.0*, O-RAN Alliance, Bonn, Germany, Specification, Mar. 2021.

[38] A. Akman *et al.*, ''O-RAN use cases and deployment scenarios,'' O-RAN Alliance, Bonn, Germany, White Paper, Feb. 2020.

[39] M. Matinmikko-Blue and M. Latva-Aho, ''Micro operators accelerating 5G deployment,'' in *Proc. IEEE Int. Conf. Ind. Inf. Syst. (ICIIS)*, Dec. 2017, pp. 1–5.

[40] *5G Campus Networks LTE and 5G-Technology for Local Company Networks*, TSI GmbH, Aachen, Germany, Nov. 2019.



JONATHAN PRADOS-GARZON received the B.Sc., M.Sc., and Ph.D. degrees from the University of Granada (UGR), Granada, Spain, in 2011, 2012, and 2018, respectively. Currently, he is a Postdoctoral Researcher at the WiMuNet Laboratory, headed by Prof. Juan Manuel Lopez Soler, and the Department of Signal Theory, Telematics and Communications, University of Granada. His research interests include mobile broadband networks, network softwarization, deterministic networking, and network performance modeling and optimization.

PABLO AMEIGEIRAS received the M.Sc.E.E. degree from the University of Malaga, Spain, in 1999. In 2000, he joined Aalborg University, Denmark, where he carried out his Ph.D. thesis. In 2006, he joined the University of Granada, where he has been leading several projects in the field of LTE, LTE-advanced, and 5G systems. Currently, his research interests include 5G and the IoT technologies.

JOSE ORDONEZ-LUCENA received the B.Sc. and M.Sc. degrees in telecommunications engineering from the University of Granada, in 2015 and 2017, respectively, where he is currently pursuing the Ph.D. degree in telecommunications engineering. In 2018, he joined Telefónica I+D as a Core and Platforms Technology Analyst, within the Global CTIO Unit. He is currently involved in technology exploration and innovative activities for 5G/B5G systems through different European research projects, with a focus on mobile network architectures and end-to-end network slicing solutions, considering their applicability for public-private network integration scenarios. He also takes part in standardization activities, acting as Telefónica Delegate in 3GPP SA5, ETSI ISG ZSM, and GSMA 5GJA.

PABLO MUÑOZ received the M.Sc. and Ph.D. degrees in telecommunication engineering from the University of Málaga, Málaga, Spain, in 2008 and 2013, respectively. He is currently an Assistant Professor with the Department of Signal Theory, Telematics, and Communications, University of Granada, Granada, Spain. His research interests include radio access network planning and management and application of artificial intelligence tools in radio resource management.

OSCAR ADAMUZ-HINOJOSA received the B.Sc. and M.Sc. degrees in telecommunications engineering from the University of Granada, Spain, in 2015 and 2017, respectively, where he is currently pursuing the Ph.D. degree with the Department of Signal Theory, Telematics and Communications. He was granted the Ph.D. Fellowship by the Education Spanish Ministry, in September 2018. His research interests include SDN, NFV, and network slicing in 5G radio access network (RAN).

DANIEL CAMPS-MUR received the master's and Ph.D. degrees from the Polytechnic University of Catalonia (UPC), in 2004 and 2012, respectively. He is currently leading the Mobile and Wireless Internet (MWI) Group, I2CAT, Barcelona, Spain. In addition, he is the Technical Coordinator of the 5G-PPP Project 5G-Clarity, which investigates convergence of 5GNR, Wi-Fi, and LiFi. Previously, he was a Senior Researcher at the NEC Network Laboratories, Heidelberg, Germany. His research interests include mobile networks, software defined networking, and communications protocols for the Internet of Things.