



5G PPP Technology Board

Non-Public-Networks – State of the art and way forward

Version 1.0

Date: 2022-11-17

Version: 1.0

DOI 10.5281/zenodo.7230191

URL <http://doi.org/10.5281/zenodo.7230191>

Contents

1	<i>Vision</i>	3
2	<i>Background</i>	4
2.1	<i>NPN and Type of NPNs</i>	4
2.2	<i>NPN Technology Gap Analysis</i>	5
3	<i>Deployment scenarios and Use Case requirements</i>	8
3.1	<i>Deployment scenarios</i>	8
3.1.1	Architectural considerations for NPNs.....	8
3.1.2	SNPN category	10
3.1.3	PNI-NPN category	12
3.2	<i>Use case requirements</i>	14
4	<i>Enabling Technologies for implementing an NPN</i>	20
5	<i>Impact of NPN on 5G Ecosystem</i>	38
6	<i>List of Editors and Contributors</i>	40
	<i>References</i>	43

1 Vision

The integration of 5G with verticals has been positioned as the most significant shift in service orientation compared to previous generations of the mobile sub-system. Many of the new capabilities, such as ultra-low latency, edge computing, and others aim at accommodating the many vertical use cases that the 5G community has identified [1]. 5G has not only seen capabilities developed with verticals as targets but has also developed architectural concepts, most prominently around the **Service-based Architecture** (SBA) [2], which allow for much greater adaptability to, and integration with the vertical customer's communication and service infrastructure. Key here is the realization that *network functions* (NFs) are best realized as network-level services through well-known and tested Internet invocation protocols (HTTP) over a generic communication substrate, such as the Internet. It enables the 5G system to be decomposed, distributed and, more importantly, integrated into the vertical industries' existing **enterprise service architectures** (ESA) in a manner that the operation of the 5G network becomes an integral part of the overall services provided within the vertical ESA.

Non-Public Networks (NPNs) push this integration capability a step further by not only offering the integration of service capabilities specific and tuned towards verticals but building an entire concept of **infrastructure provisioning** around verticals. This is achieved by extending the architectural alignment (of SBA and ESAs) to the capability of provisioning 5G hardware infrastructure, down to base stations in vertical industry sites. The use of **private site-specific spectrum**, utilized for 5G infrastructure, can be complemented by the possibility to utilize roaming into operators' wide-area connectivity, if needed for the specific use case. The use of local spectrum disconnects NPNs entirely from previous operator-dependent deployment models. *Ultimately, the vertical customer's extended ESA is now realized as a distributed data centre that spans its various sites albeit with the ultra-low latency and service-centric capabilities that are enabled by 5G.*

2 Background

2.1 NPN and Type of NPNs

As the roll-out of private LTE networks is getting mature into carrier networks, new challenges are at the forefront when considering the applicability of 5G technology on private networks. Following 3GPP terminology, these private networks are referred to as Non-Public Networks (NPNs). An NPN is a 5G System (5GS) deployed for the sole use of a given customer (e.g., vertical customer, government, industry...) and is designed to support services for non-public use, including infrastructure services, communication services and other digital services.

Starting from Release 16, 3GPP 5G Phase 2 specifications provide requirements, capabilities and solution sets for the support of NPNs, at functional (3GPP SA2) and management (3GPP SA5) layers. According to [6], NPNs can be classified into the following categories:

- **Stand-alone NPN (SNPN).** It is an NPN that does not rely on network functions provided by a Public Land Mobile Network (PLMN). An SNPN is identified by a combination of a PLMN ID and a Network IDentifier (NID). The User Equipment (UE) registered in an SNPN might access PLMN services, if required, by carrying out another registration with a PLMN using the SNPN User Plane, while the SNPN is playing the role of an untrusted non-3GPP access network. A symmetric scenario is allowed to access SNPN services when camping on PLMN. 3GPP Rel-16 specifications do not include support for interworking with the Evolved Packet Core (EPC), i.e., the 4G core network, emergency services in SNPNs as well as roaming and handover between SNPNs.
- **Public Network Integrated NPN (PNI-NPN).** It is an NPN deployed with the support of one (or more) PLMN(s). For the provision of a PNI-NPN, two solutions have become normative: a PNI-NPN as a dedicated Data Network Name (DNN); and a PNI-NPN as a network slice. In the first case, which is an evolution of 4G APN (Access Point Name) solutions, the PLMN defines a mobile pipe to convey NPN traffic to a dedicated mobile gateway, in charge of dispatching traffic towards a local area data network (LADN). In the second case, the PLMN provisions a dedicated slice, with resources allocated for the exclusive execution of non-public services. Typically, the private UEs will only have access to the PNI-NPN within a limited coverage area. However, network slicing does not include any mechanism for limiting the PNI-NPN footprint. To overcome this issue, 3GPP standards specify the Closed Access Group (CAG), which defines a list of subscribers who are allowed to access the cells associated with it. In other words, CAGs serve to apply access control to the UEs depending on their geographic position, thus preventing UEs from accessing the network in areas where they are not permitted to access the network slice implementing the PNI-NPN.

3GPP release 16 covers the ability to identify, discover, select and implement access control for NPNs. Meanwhile, 3GPP supports also the interworking between NPN and PLMN, such as service continuity between NPN and PLMN, architecture enhancement to access the SNPN services via PLMN and vice versa. In 3GPP release 17, more NPN architecture features are supported based on the dedicated requirements from the NPN user [26] [19] [20], which include:

- Enhancements to support SNPN along with credentials owned by an entity separate from the SNPN. Here the separate entity could be either a 3GPP entity such as UDM/AUSF (Unified Data Management / Authentication Server Function) or a non-3GPP entity such as an AAA (Authentication, Authorization and Accounting) server.

- Support on service continuity and simultaneous service from both SNPN and PLMN. This aspect is especially useful for video, imaging and audio for professional applications
- Support for IP Multimedia Subsystem (IMS) voice and emergency services for SNPN
- UE onboarding (i.e., to enable 3GPP connectivity) and remote provisioning (i.e., provisioning of credentials to allow access to NPN services).

2.2 NPN Technology Gap Analysis

Non-public networks based on 5G technology are implemented to replace existing proprietary radio networks or fixed Ethernet networks. NPN networks are also needed to enable automation to deliver the Industry 4.0 paradigm on large geographical areas. Motivations to implement NPNs may vary, but common shortcomings in current network implementations can be overcome by using NPN technology. Yet, we also recognize gaps in current NPN technologies with respect to the roadmap projections and the needs expressed by different stakeholders.

The proliferation of the NPN technology is expected to profoundly change the owner ecosystem. If with the current public networks, by definition, the network and equipment owners were a rather small group of either privately or state-held public mobile network operators (MNOs), of an order of 3-4 per country, plus some special operators, like e.g. railroad companies using their own GSM-R conformant installations for signalling and communications with and between trains, the central promise of NPN is to render the same technology attractive and usable for a wide range of stakeholders in the vertical industries. This typically includes:

- different types of production industry (factories, plants, power generation, etc.)
- power transport and distribution companies (smart grid, etc.)
- agriculture (farms, swarm management, etc.)
- road authorities, automotive and transport industry (diverse V2X scenario, fleet management, etc.)
- health sector (hospitals, medical devices, emergency vehicles, etc.)
- local facility providers (gas, water supply and infrastructure management, etc.)
- local event organizers with high density requirements (sport events, stadiums, etc.)
- small and medium size enterprises (SME) of all kinds (Wi-Fi and Ethernet cable replacement).

Overall, the move to NPN yields an unprecedented mix of technology stakeholders of strongly varying sizes, with functionally very different use cases and radically different enterprise cultures, sensitivities and resulting requirements (additional functional requirements, functional safety, resilience, security, etc.).

In the sheer diversity of such new potential stakeholders, there is indeed one common, novel trait, as depicted in Figure 2-1. In a sharp contrast to the so far predominant MNOs (Figure 2-1, left), who, by regulation, have to precisely log any network access and, therefore, insist on large-scale service with a reliable and precise mobile session management plus accounting (per second, per byte, etc.), typical new stakeholders (Figure 2-1, right) seek to enable their own end-to-end (E2E) services through their own network using NPN technology. In other words, since the new stakeholders are not primarily interested in providing service to third parties (mobile subscribers, over-the-top services, etc.), the focus of 5G NPN stakeholders is on the **end-to-end enterprise application performance** vs. the incurred costs (CAPEX/OPEX) with that technology.



Figure 2-1: In contrast to MNOs, typical NPN users combine the network and service in one authority

At the same time, NPN coverage generally is not limited to some local islands and rather should be expected to range from as broad as for the current MNOs (e.g., all country road infrastructure providers of V2X services; large electrical transport and distribution grid operators, etc.) to NPNs as small as one single base station.

NPN functionality is usually related to at least one application that has specific requirements in terms of reliability, performance, lifecycle management, security or costs. To be able to meet these requirements, NPN needs to have frequency coordination, high global sales volumes and scalable design to drive CAPEX down. The technology has to be easy to use and to operate and should support a long lifecycle to drive OPEX down.

In most cases, NPN will not be a greenfield implementation, but will rather be implemented to become part of an existing IT architecture. This means that integration and network planning are crucial along with common deployment, configuration, monitoring, performance and security of the mixed communication and information systems. While an NPN is implemented with certain applications in mind, and these applications have to work reliably in a given environment, the NPN owner obtains a high degree of technical freedom, which however comes with the responsibilities of network providers, in that it needs to cover network infrastructure, network planning and application integration.

In this light, analysing the current 5G technology and especially 5G NPN technologies, we recognize the following gaps in the state-of-the-art NPN products:

Scaling down - Compared to other technologies like Wi-Fi, which use a very simplistic notion of session or “connection” and do not mandate any core network functionality, both the deployment of and the connection to the actual service end-point (cf. “local breakout”) is complicated.

Ease of use - The typical NPN users ultimately seek a more reliable and more cost-efficient enterprise service realization. Yet, in particular, it is unnecessarily difficult to deploy an end-to-end application and to provide stable services from the connected UEs.

MNO-driven architecture - Current NPN technology uses the 5G Core (5GC) network built as per MNO-centric 3GPP SA1 requirements. While 5GC can be customized (e.g., through network slicing, particular UPF instances and application functions), it is limited to control and management plane services typical for the operators, yet, even with customization options, the used core network does not support end-to-end enterprise application deployment. In its minimal manifestation, 5GC already represents a non-negligible complexity in both the initial configuration and setup and in the latter maintenance, increasing OPEX. The configuration of user profiles, possibly with the corresponding SIM cards in the UEs, might make it a no-go for many SMEs and roaming users.

Typical cost and licensing models applied by 5GC vendors still target the MNOs with their tens of thousands of base stations, and might be unfit for most of the new types of stakeholders. Overall, current 5GC design reflects the particular needs of the MNOs only. In spite of the often-claimed support for the vertical

industries, there is no core network dedicated to any vertical industry. “*One size fits all*” clearly does not hold here.

Specific mobile network skillset with enterprise IT - While NPN targets enterprises, it lacks noticeable means of integration with the typical enterprise IT systems. Consider, for instance, directory integration: this typical pain point might be aggravated in NPN, which comes with its own 5GC Home Subscriber Server logic, stipulating particular interfaces and a particular access control logic based on subscriber profiles. The existing enterprise directories might both use incompatible interfaces and a completely different understanding of the whole service access control logic, e.g., by application, by location, by load, etc.

NPN with public networks - NPN can be deployed as “Public Network Integrated NPN” (PNI-NPN). Beyond RAN sharing, discussed below, such integration covers the question of control plane sharing by the public network, which can be implemented by the public network providing access to some of its control plane network functions to the NPN users, NPN RAN or by a network slice from the public network providing a whole and seemingly isolated NPN control plane, if required. This is highly interesting to limit NPN deployment costs and to assure service continuity, since the terminal/UE can be connected to both NPN and PLMN at the same time. However, having both on-site, NPN-own and remote PLMN network functions available, there should be a dynamic way of selecting the serving control plane. This has been recently successfully demonstrated for reliability purposes [3], yet requires a particular integration effort by all involved stakeholders (vendor, NPN owner and public network owner). There should be a way of selecting the whole serving network on a per-service basis (e.g., data over this, call & VPN over that other, URL-based routing, etc.). Ideally, there should be a more fine-grained and standard way to dynamically select network function (NF) instances according to the immediate service quality needs (e.g., based on current network function instance load, latency of the NF instance response, etc). Besides, the integration of NPN with PLMN does not have to be a one-way road only. Having NPN 5GC on site, in principle, a network slice could be deployed in the NPN to provide PLMN type of services locally as well. While the generic slice template (GST) – defined by the GSM Association (GSMA) – could be used for this, the current GST does not yet support all NPN attributes [16].

NPN with other NPNs - Interconnecting NPNs is not yet supported today. Not even basic roaming is specified for 5G NPNs so far. More particular needs, like network function sharing and reuse, inter-NPN slices, etc., are not supported either. These would appear suitable and interesting for use cases such as connecting factory floors, stadiums, educational institutes, etc.

Efficiency, OAM and sustainability - There is no end-to-end resource control, beyond the air interface, as current 3GPP standards are resource-agnostic. When deploying flexible distributed networks with potentially several RANs and several core networks (or one core network spread over several locations), to meet the performance requirements of the enterprise services (robustness, quality, availability, service success rates, etc.), a better resource control for all service-relevant resources would be required. While potential solutions exist, for example IETF ANIMA [4], these are not yet integrated with the 3GPP standards framework. In, ETSI ZSM [5], ANIMA is considered as one of the crucial enablers for zero touch service management.

3 Deployment scenarios and Use Case requirements

3.1 Deployment scenarios

NPNs can be deployed in a wide variety of forms, depending on the use cases to be supported as well as the regulatory issues in place. In an attempt to simplify this casuistry, the 5G Alliance for Connected Industries and Automation (5G-ACIA) has defined four baseline deployment scenarios for NPNs [6]. These four scenarios, captured in Table 3-1, have become de-facto in the industry 4.0 sector, and have been used as reference for further discussion in other works, including academia [27] [28], industry fora [29] [30] and even government institutions [31].

Table 3-1: Mapping of 5G-ACIA scenarios with 3GPP NPN categories

5G-ACIA scenario	3GPP NPN category	Comments
#1: Isolated NPN	SNPN	All 5GS functions are owned by the enterprise customer, and deployed on-premises.
#2: Shared RAN	SNPN	Scenario #1 with RAN sharing in-built, so that the gNB can serve non-public subscribers (e.g., enterprise customer's subscribers) together with public subscribers (e.g., UEs from one or more PLMNs).
#3: Shared RAN and CP	PNI-NPN	The network functions shared in 5GC CP depends on the specific use case and vertical customer requirements
#4: NPN hosted by the public network	PNI-NPN	PLMN allows for E2E connectivity, from non-public subscribers to the LADN.

The state-of-the-art work mentioned above is mainly focused on factories of the future, without capturing the rest of scenarios where NPNs may also apply, and that are of interest for operators. Examples of these non-industry 4.0 scenarios include transportation hubs (e.g., airports, seaports...), private venues (e.g., stadiums, shopping malls...) and large-sized infrastructures (e.g., university campus, government ministries...). GSMA has recently published a Public Reference Document (PRD) on 5G industry campus [7] that aims to capture all these scenarios. Leveraging 3GPP progress and outcomes from vertical industry alliances (notably 5G-ACIA and 5G-MAG), together with the guidelines from the MNOs (e.g., standardization readiness, case studies and lessons learnt), this GSMA document lays out the key factors that may influence the NPN deployment choices and operator strategy rollouts.

In the following, we provide an overview of the different deployment models for NPNs. Based on a set of architectural considerations (Section 3.1.1), we will present representative scenarios for both SNPN (Section 3.1.2) and PNI-NPN (Section 3.1.3) categories.

3.1.1 Architectural considerations for NPNs

In an archetypal deployment, an NPN is a 5GS formed by the following functional components:

- **3GPP 5G radio access network (RAN)**, deployed with one or more gNBs. A gNB is a 5G base station providing new radio (NR) based connectivity towards the end device.

- **3GPP 5GC user plane:** it consists of one or more instances of User Plane Functions (UPF), with optional deep packet inspection (DPI) capabilities built-in. We refer to 5GC user plane as UP.
- **3GPP 5GC control plane:** it consists of cloud-native network functions providing signalling and packet core functionality, such as Session Management Function (SMF), Access and Mobility Management Function (AMF), Policy Control Function (PCF) and Network Slice Selection Function (NSSF). We refer to 5GC control plane as CP.
- **3GPP 5GC subscriber data management (SDM):** it consists of cloud-native network functions that allows authenticating and authorizing end devices based on stored subscription data. Examples of this functions include Unified Data Management (UDM) and Unified Data Repository (UDR).
- **Service/enterprise applications,** providing service/business logic. These applications are hosted in cloud execution environments, with optional multi-access edge computing (MEC) capabilities built-in.

Depending on the considered use case, the NPN can be enriched with other complementary (and non-5G-specific) functionalities, including Wi-Fi access and time-sensitive networking (TSN) technology. While the combination of Wi-Fi and NR allows higher throughput aggregation and enhanced reliability on the access side, the TSN provides determinism and zero-jitter behaviour on the transport network.

There are several factors that may have a huge impact on how an NPN can or shall be deployed for a given NPN. This includes, but is not limited to the *location of the enterprise customer site*; the *maximum admissible latency that the connected devices can have*; the *level of redundancy required*; and the *security requirements of the enterprise customer*. Decision-making should be done based on these technical factors, with the most economical approach when possible, optimizing CAPEX and OPEX as needed.

3.1.2 SNPN category

Figure 3-1 illustrates representative deployment flavours for the SNPN category.

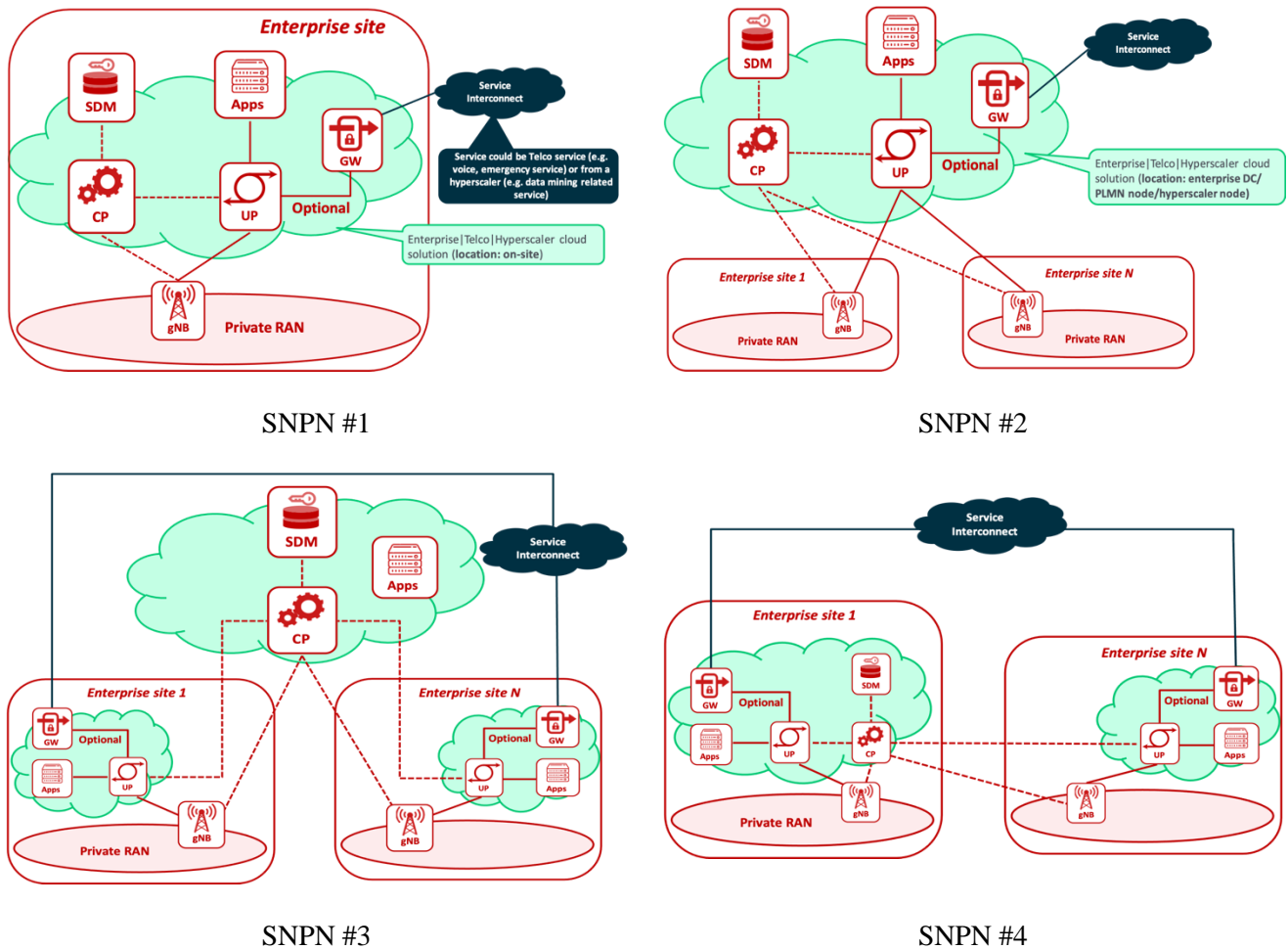


Figure 3-1: SNPN deployment models

SNPN #1 represents a deployment flavour where all the NPN components are deployed on premises. This usually is due to security reasons, high availability requirements, or to avoid control and data traffic thromboosing via the public 5GC. The complete separation of this NPN from PLMN is manifested in three facets. First, the assignment of dedicated spectrum to the gNBs¹, either private spectrum (i.e., obtained from the local regulator) or licensed spectrum (i.e., leased from the MNO). Secondly, the gNBs are for exclusive use of non-public subscribers, thereby representing the concept of private RAN. Thirdly, the lack of presence of PLMN functions along the entire data path, from access to local data network, all NPN components are owned by the enterprise customer. For those NPN components deployed as virtualized/cloud-native workloads (i.e., VNF/CNFs), the cloud service platform hosting them is an on-premises solution from the enterprise or provided by a 3rd party, either a telco operator or a hyperscaler.

¹ The private gNB can be a small cell gNB (when the enterprise site is for example a Factory) or a traditional gNB (when the Enterprise site corresponds to a campus).

SNPN #2 represents a deployment flavour where all virtualized/cloud-native workloads are moved out of the premises. This model is appropriate for small enterprise customers which are not interested in having an on-site cloud service platform, either because high upfront costs or simply because they do not have in-house compute capacity. By getting workloads hosted by 3rd party compute nodes, the customer transfers all the integration efforts to the 3rd party (e.g., telco operator, hyperscaler...), which ultimately results in CAPEX and OPEX reduction. However, this is done at the cost of allowing traffic to leave the enterprise customer site. The user traffic, signalling and packet core traffic and subscription data are transferred to the 3rd party node. Figure 3-1/SNPN #2 illustrates the applicability of this deployment flavour to multi-site scenarios, although single-site scenarios are also valid.

SNPN #3 represents a hybrid deployment flavour, with some workloads instantiated on-site (i.e., UP and mission-critical applications²) and the rest hosted by a 3rd party node (i.e., SDM, CP and non-critical applications³). This setup allows keeping all user traffic on premises, while having a centralized control and data subscription management. As illustrated in Figure 3-1/SNPN #3, it represents a trade-off solution between SNPN #1 and SNPN #2. On the one side, the motivation for a customer to go from SNPN #1 to SNPN #3 is typically a sustainable, cost-efficient scalability support. This flavour allows the customer to extend NPN service footprint to multiple sites without incurring additional costs. On the other side, the motivations for a customer to go from SNPN #2 to SNPN #3 are typically security reasons, and latency constraints between devices in the same location. In SNPN #3 it is assumed that the customer is able to operate a cloud service platform on-site.

SNPN #4 is similar to SNPN #3, with the exception that off-site workloads are now moved in-house. The transition from SNPN #3 to SNPN #4 allows the customer to have everything on-site, so nothing flows out of the premises. This is done at the cost of increasing OPEX and integration efforts at the customer side, who is now responsible for the E2E lifecycle of NPN, from capacity design to run-time operation.

In addition to the above descriptions, it is worth mentioning that:

- For all deployment flavours, there exists the possibility for the SNPN to connect to the PLMN, if needed (e.g., when non-public subscribers need to gain access to PLMN exclusive services like voice services, emergency services). In such a case, Non-3GPP Interworking Function (N3IWF) based solutions for SNPN-PLMN connectivity [19] are applied.
- All deployment flavours are eligible for making small gNBs available for RAN sharing, with the enterprise customer playing the role of neutral host. The neutral host represents a role whereby the enterprise customer invests in on-premises network infrastructure, which is used for its own purposes, and also leased to different MNOs. In this scenario, the leasing can include cell site infrastructure sharing – i.e., passive RAN sharing – and Multiple Operator Core Network (MOCN) – i.e., active RAN sharing. The neutral host model is beneficial for both the neutral host and the MNOs. The enterprise customer (neutral host) monetizes the in-house infrastructure by selling mobile coverage solutions to the different hosted MNOs. On the other hand, the MNO can increase its coverage area without the need to invest in on-site equipment, thus expanding its service footprint at a lower cost.

² Mission-critical applications are deployed on Local Area Data Network (LADN), and typically have stringent latency requirements

³ Non-critical applications can be deployed on traditional Data Networks, just behind the PDU Session Anchor UPF (PSA-UPF). They typically behave as trusted Application Function (AF).

- Some of these SNPN models correspond to the 5G-ACIA scenarios described in [6]. SNPN#1 corresponds to the 5G-ACIA scenario #1 (“Isolated NPN”), while neutral hosting model correspond to the 5G-ACIA scenario #2 (“RAN sharing”).

3.1.3 PNI-NPN category

Figure 3-2 illustrates representative deployment flavours for the PNI-NPN category.

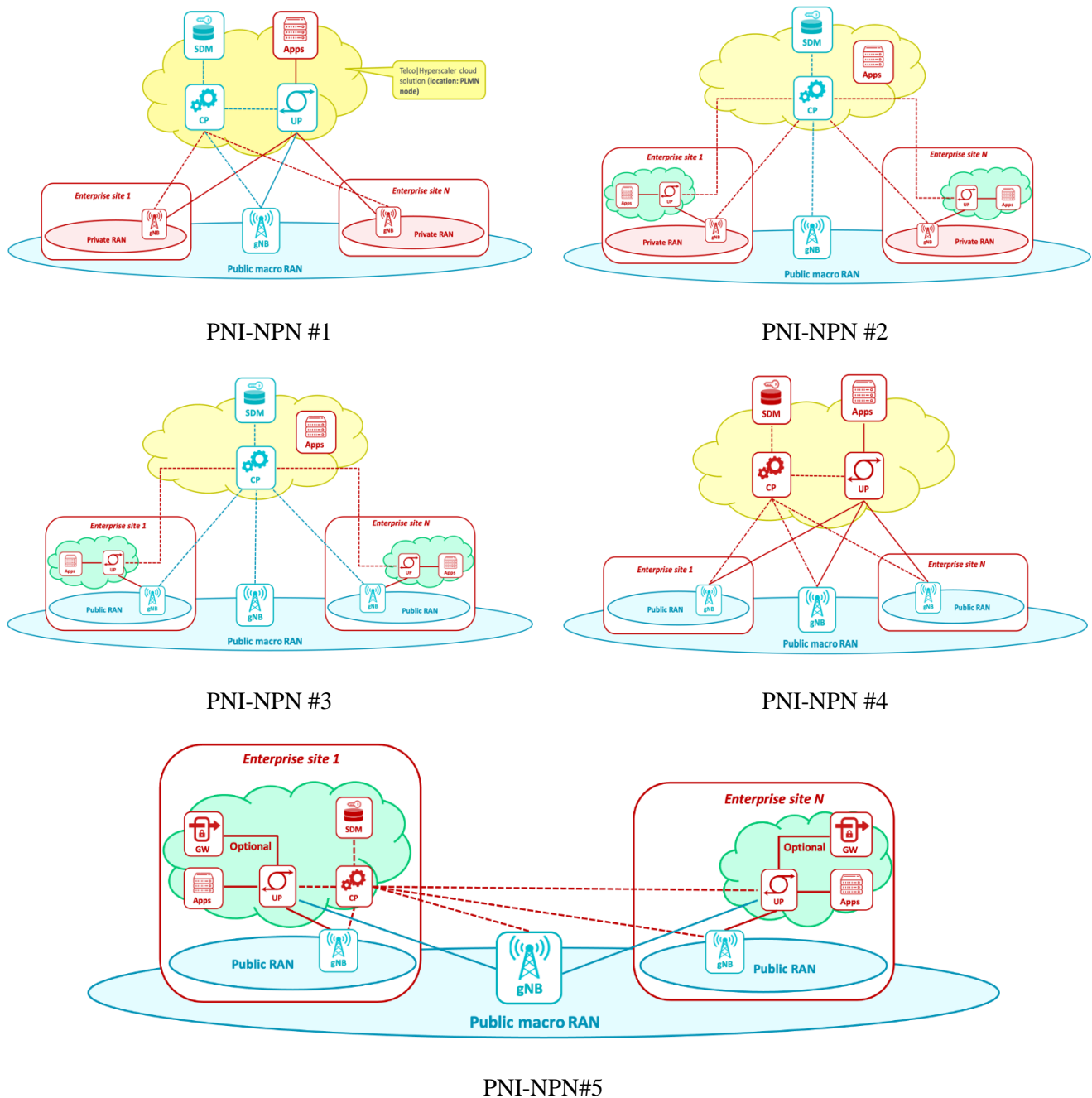


Figure 3-2: PNI-NPN deployment models

PNI-NPN #1 is a deployment flavour whereby the NPN is fully integrated with the MNO commercial network, with the exception of the radio access, which is located on enterprise customer premises and is based on public spectrum. The UP, CP and SDM components from the PLMN are used to process PDU sessions corresponding to public and non-public subscribers. To keep traffic segregation between public and non-public PDU sessions, solutions based on Data Network Name (DNN) [19] or network slicing can be applied. When using network slicing for the provisioning of the PNI-NPN, the MNO shall apply the necessary policies to ensure the slice is only accessible by non-public subscribers. Such a policy is for example linking Single – Network Slice Selection Assistance Information (S-NSSAI) list with Conformance Agreement Group (CAG) identifiers.

PNI-NPN #2 is similar to PNI-NPN #1, with the exception that user traffic is kept on premises, by moving UP and mission-critical applications to the customer premises. The decision for a customer to go for PNI-NPN #2 instead of PNI-NPN #1 is typically due to security reasons, latency constraints between devices in the same location, or to reduce throttling of data into the MNO hosted UP and then back again into the local applications.

PNI-NPN #3 is the result of replacing private RAN with public RAN coverage in PNI-NPN #2. This scenario is interesting for enterprise customers who do not want to invest in RAN equipment, nor want to manage RAN related aspects. Instead, they rely on MNO's proven experience to get the gNB up and running inside every site. Examples of where the scenario can apply, include hospitals and similar venues.

PNI-NPN #4 is the result of replacing private RAN with public RAN coverage in SNPN #2. The motivation is the same as described in PNI-NPN #3.

PNI-NPN #5 is the result of replacing private RAN with public RAN coverage in SNPN #4. The motivation is the same as described in PNI-NPN #3.

In addition to the above descriptions, it is worth mentioning that:

- In the different deployment flavours, it is not unusual that the customer claims for mobility solution out of its own premises (to guarantee service continuity when moving from one enterprise site to another enterprise site) or an emergency solution in the case of complete break-down of the on-site infrastructure. To cover these scenarios, public RAN is used as an alternative. In fact, when a device moves out of private RAN coverage it will try to connect to the public RAN. During that connection, the CP will treat this device as a roaming user, and will contact the SDM for device authentication and access parameters. To allow for this migration from private RAN to public RAN, the MNO needs to enforce the following two conditions: (a) the use of a public international mobile subscriber identity (IMSI) range for the NPN; and (b) the use of a specific PLMN ID for the NPN configured in the SIM as preferred ID.
- Some of these PNI-NPN models correspond to the 5G-ACIA scenarios. In particular, PNI-NPN #1 corresponds to the 5G-ACIA scenario #4 ("NPN hosted by the public network"), and PNI-NPN #2 and #3 correspond both to 5G-ACIA scenario #3 ("Shared RAN and CP"). The concept of RAN sharing in PNI-NPN scenarios is different from the one applied in SNPN scenarios. In the first case, it is based on the use of CAGs to enable non-public subscribers to access the corresponding slice. In the second case, it is based on the use of active or passive sharing mechanisms to allow for neutral hosting.

3.2 Use case requirements

A wide variety of use cases for 5G-NPNs have been identified across different 5G PPP projects. These use cases feature a diverse range of network and radio requirements, as well as deployment and configuration options. These requirements and options represent a very high innovation and business impact for the private 5G network market, thus expanding the business opportunities for all involved stakeholders. These stakeholders could be from different sectors, such as media & entertainment (M&E), Public Protection & Disaster Relief (PPDR), eHealth, Industry 4.0, Smart Cities, Energy and Train Transportation.

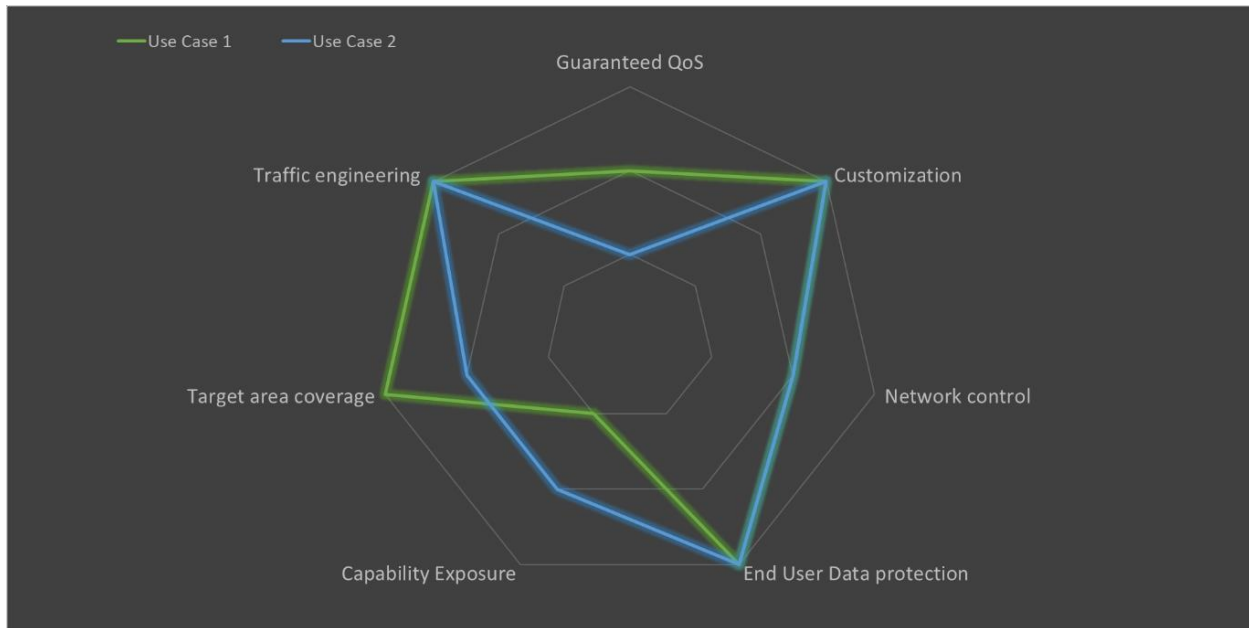


Figure 3-3: The "Why NPN" Spider diagram

The spider diagrams in Figure 3-3 represent different levels of importance of specific requirements for two exemplary enterprise use cases, that could be satisfied with a deployment of an NPN. In the diagram the vertices represent the factors which necessitate a private network. The severity of the requirement is shown in three levels for the two exemplary use cases. The definition of the identified requirements is presented below:

1. **Guaranteed QoS:** Refers to performance parameters such as Latency, Jitter and Throughput (Uplink and Downlink) or a combination of them. The enterprise has a level of demand for a set or even just one of the QoS fields. For example, it may need very high guaranteed throughput, or a millisecond order latency guaranteed by the network.
2. **Customisation:** Refers to the features needed by the enterprise to meet its business needs. This includes but is not limited to **Time Synchronization, Localization Accuracy, 5GLAN support, Integration with remote cloud** or the support for a **High Density of UEs**.
3. **Network Control:** Refers to the enterprise desire for E2E control over the network management, resources and services encompassing the information, data, operations and communication technology (IT, DT, OT and CT).
4. **End User Data protection:** Refers to subscriber data protection level, such as type of encryption, storage location (UDM deployment) and level of redundancy.
5. **Capability exposure:** Refers to the mechanisms for exporting relevant network information and features to the verticals. For example, exposing the network KPIs to an Industry 4.0 vertical that

wants to have real time performance monitoring information about all the components in the manufacturing environment.

6. **Target area coverage:** Refers to the enterprise need for radio coverage in a specific geographical area. It needs to be highlighted that some enterprise use cases might require a guaranteed coverage (for example Reference Signal Received Power > -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.
7. **Traffic Engineering:** Refers to the mechanism to steer and isolate the traffic according to the technical and business needs.

We argue in Figure 3-4 that NPNs are the ideal choice to meet the diverse requirements of the verticals highlighted in Figure 3-3.

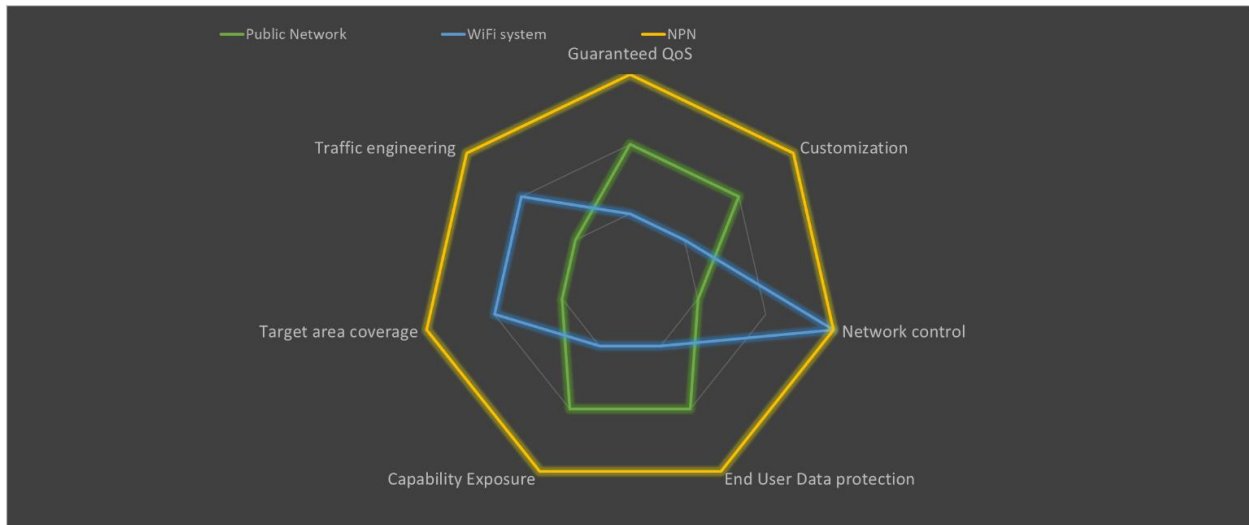


Figure 3-4: Technological Choices to meet the use case demands

Table 3-2: Mapping of network capabilities to use case requirement levels

	Level 1	Level 2	Level 3
Guaranteed QoS	No E2E QoS guarantees	Support for different classes of Service but no guarantees	Guaranteed QoS
Customization	Limited add on features even if fully customisable	Good amount of add-on features available but only few can be provisioned	All available add-on features are possible
Network control	Connection service	Controllable connection service	Owned infrastructure
End User Data protection	Weak protection within the whole system even with full control over the data	Strong protection within the whole system but limited control over the data	Strong protection within the whole system including full control over the data

Capability Exposure	Limited capabilities to expose even if fully customisable	Good amount of capabilities are available to be exposed but only few can be exposed	Rich set of capabilities to expose available and possible
Target area coverage	Best effort	Can be covered but without exclusivity	Exclusive coverage of any given area possible
Traffic engineering	No TE means available	Some TE can be chosen	Support for any typical TE method

In the following we provide a brief description and use cases for selected vertical sectors for which the deployment of NPN is justified.

Media & Entertainment

The flexible use of the network bandwidth, through network slicing, assuring a guaranteed value and the capability of the network to provide ultra-low latency will impact the media & entertainment M&E industry, specifically the live production area. With the deployment of NPNs, the network is fine tuned to the meet the requirements of the specific use case, maximizing the network assets capacities exploitation.

- **Live Audio Production** showcasing the integration of audio capturing devices, 5G RAN and a production site in a standalone NPN deployment.
- **Multiple Cameras Wireless Studio** where a set of cameras and sound capturing devices will be transmitting audio-visual content continuously to a production room by leveraging a public network integrated NPN.
- **AR/VR Media Delivery** to provide immersive media content delivery blending the real and the virtual work (AR), by layering computer generated images on top of the existing reality. Or by providing 360-degree computer generated simulation of real-life-like environment (VR) on user terminals.

Public Protection and Disaster Relief

Communication is critical for saving lives and protecting infrastructure during emergencies and disaster situations. The agencies responding to those events cannot function without robust support of wireless communication. Non-public networks designed for PPDR operations, not only provide the indispensable communication, but also provide robust and reliable means to support coordination between agencies like police, fire, ambulance and armed forces. Most of the Use cases rely on SNPNs, with the possibility of PNI-NPNs, if the public infrastructure is available.

- **Communication in Disaster Situations** provisioning transparent mission-critical services to the end-user independently of the underlying telecommunication infrastructure. This ensures that first responders can access critical information and communicate with each other during crises, even when public 5G network networks are down or congested.
- **3D Indoor Localisation for Emergency Services** providing ultra-precise 3d localization of operatives when responding to emergencies like building fire, kidnap/terrorism incident, medical emergency, building evacuation in emergencies.
- **Ambulance Emergency Response** When an ambulance is dispatched to an emergency call, it uses an NPN on top of public 5G networks to remain connected. The paramedics can check the patient's

medical history from the emergency response vehicle. The patient is monitored, and the information is uploaded, stored, and viewed at the hospital.

eHealth

5G is a key enabler for the Internet of Things, that will impact a large range of areas, but in particular the eHealth sector. The capability of the network to instant deliver data will revolutionize the healthcare industry. However, the sensitive nature of the data requires that the network is able to ensure the security of it. Non-public networks will be an enabler due to its isolated nature, but also tune up to satisfy the Quality-of-Service needs of the applications. The eHealth use cases are supported for SNPNs, on the medical building premises, and by PNI-NPNs to the emergency response outside the medical building camps.

- **Remote Monitoring in the ward** improving the quality of patients monitoring as well as increasing the frequency of monitoring, by applying devices that can collect data of cardiac and respiratory functions. The collected data is centralized in the hospital network and sent over the 5G non-public network to a monitor centre.
- **Intra-Hospital Patient Transport Monitoring** with the 5G non-public coverage across the entire hospital, monitor moving patients around, when necessary, becomes easier as coverage is highly dependable. Moreover, as it lacks wires and supports high bandwidths/low latencies, it is also a great alternative to existing wired solutions.
- **Telemedicine** enabling the capability of observe report and analyse patients with chronic conditions (diabetes, high blood pressure, dementia, etc), monitor pregnancy or weight loss from any location both for the patient and for the clinician. It also includes medication management and specialist remote consultation provided by secured video and audio communications.

Industry 4.0

The fourth industrial revolution will be based on Cyber-physical systems consisting of modern control systems with embedded software and connected to each other, the so-called smart machines. Industrial communications have stringent communication requirements. NPNs are the perfect solution due to their capability to be fine-tuned to address those requirements, encompassing technologies like TSN or 5GLAN on top of 5G. The wireless nature allows for the replacement of the traditional wired solutions, without compromising performance.

- **High accuracy indoor positioning for industrial IoT** providing precise location of the factory assets, such as forklifts, or parts to be assembled.
- **Telemetry** allowing for monitor all the machinery and equipment, with collecting sensors providing data in real time.
- **Augmented Zero Defect Manufacturing Decision Support System** to automate the quality control process to increase the efficiency of the quality control station within a production site.
- **Digital Twin** supplying plant managers with a virtual reproduction of production plants, feeding it with actual information from the production lines.

Smart City Use Cases

Smart cities consist of the evolution based on the use of digital solutions to improve the traditional networks and services, benefiting the business and inhabitants of the city. The ability to monitor events as they unfold, enables the capacity to respond with faster and lower-cost solutions, that ultimately improve the QoE of the citizens. PNI-NPNs are the natural solution to leverage the city deployed mobile telecommunications infrastructure.

- **Positioning and Flow Monitoring in Large Venues and Dense Urban Environments:** Large venues and shopping areas are characterized by gatherings of large crowds, with complex mobility behavior. This calls for efficient flow and resources management and with complex mobility behavior. This calls for efficient flow and resources management and creates opportunities to maximize QoE.
- **Device-free Localization:** Wireless network radio signals are exploited to monitor objects and people that are not equipped with any location device.
- **Smart Sewage:** with a digital map of the sewage system with monitor equipment installed providing constant monitor of flow and quality of the sewage. With those capabilities, the system gets its operation improved, including maintenance operations and disaster response capacity.
- **Smart Environment:** Real time air quality monitoring system enabled by sensors deployed across the city, as well as monitoring devices deployed to provide waste bins tracking (capacity and location) improving the waste collection efficiency for the city service providers.

Energy

The quality monitor for the distribution network can leverage communication improvements provided by the new mobile telecommunications technology. Due to the critical communications nature, both SNPNs and PNI-NPNs suit the use cases described below:

- **Substation Maintenance** by replacing wired connections between the sensors and the main controller by 5G connections for safety-critical communications leveraging the 5G improvements.
- **Last-gasp:** Explore the low latency provided by 5G to develop a solution enabling meters to use the last-gasp of energy before a power outage to send a message with relevant information.
- **In House Smart Grid** enabled by the monitoring of connected devices energy consumption. It brings benefits both for consumers and for energy suppliers. Consumers will be able to get a full picture of their energy consumption. Suppliers will be able to predict peaks, improve energy distribution and avoid waste.
- **Energy production facilities remote monitoring** for equipment health and readiness, enabling remote configuration and parameter deviation with intelligent alarm management.

Train Transportation

With data networks designed to satisfy specific requirements leveraging the 5G capabilities, the train network will benefit from an improved monitoring quality. It will not only provide lower maintenance costs but also improve the train network users' security.

- **Monitoring of railroad infrastructure:** Provide real-time information from sensors, meters, and cameras to the maintenance teams and to the control centre to facilitate the assessment of the severity impact of the problem they are facing, enabling the deployment of the appropriate measure.
- **Video Surveillance** Including live video streaming of the level crossing sent both to the train driver and to the maintenance team, preventing accidents caused by vehicles trapped between the level crossing
- **Automatic train protection and operation** with communication between trains, between trains and other trackside elements and between trains and the ground systems. The communication allows for broad railroad awareness enabling the improvement of train safety in an autonomous way.
- **Voice communication** including on-train, multi-train, with ground forces and control centre.

The large number of use cases described above rely on independently administrated NPNs. To be able to use such an ecosystem in a coherent manner, there is a need to interconnect different NPNs. The interconnection of different NPNs is required in cases such as to interconnect multiple factory floors, multiple event venues, logistics centres, portable 5G units or to connect different educational institutes.

4 Enabling Technologies for implementing an NPN

This section describes enabling technologies for realising an NPN in all its deployment scenarios. The technologies are categorised into three layers: the infrastructure layer, the platform layer and the service layer. *Enterprise applications* at the service layer are responsible to allow UEs to consume or produce content over the user plane. The NFs of a 5GC are also enterprise services that provide functionality such as service slicing, service lifecycle management and control and service communication proxy as *outsourced* components within an underlying platform layer. Such layering shall be understood from the perspective of each underlying layer, which offers programmability and tenancy to the upper layer. The infrastructure layer offers strictly infrastructure related functionalities. The left side in Figure 4-1 illustrates federated NPN management, which includes functionality that allows the federation of NPNs that logically belong together.

The section focuses on enabling technologies that are of particular importance for the realisation of NPNs and their integration with public networks. It does not intend to provide an overview of enabling technologies for 5G in general. Certain enabling technologies represent incentives for enterprises and other customers to deploy NPNs; where without these the business motivation to consider such solutions would not exist.

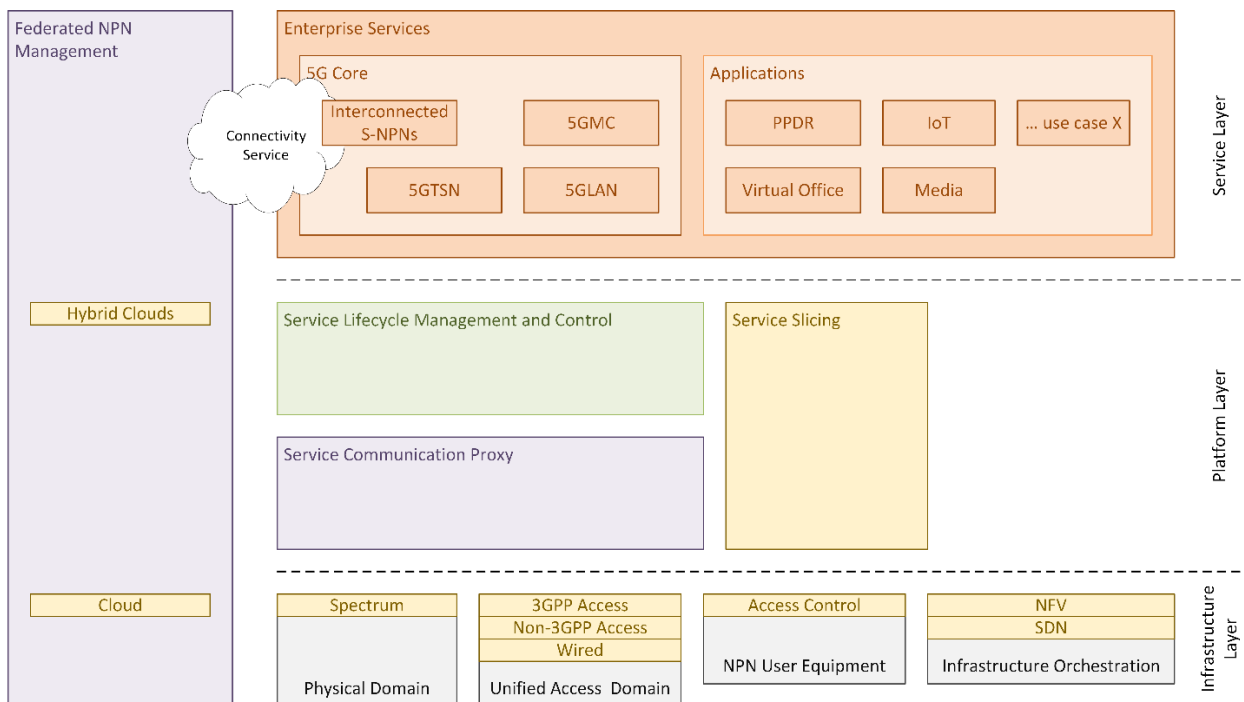


Figure 4-1: Enabling Technologies for flexible NPNs

Network Slicing for PNI-NPN follows the core concept of network slicing in 5G [10]. Considering digital transformation of industries, it plays a pivotal role in this transformation. Network slicing facilitates the evolution from the one-size-fits-all approach to network services tailored to different business and performance requirements for different services. Network slicing achieves customisable services through on-demand deployment of selected network functions and required resources. It guarantees Quality of Service (QoS) through resource isolation and controlled resource sharing. Optimisation of resource management is achieved by the introduction of AI-based online learning [12], or offline training [13]. Resource optimisation is particularly useful for resource-constrained NPNs and mMTC services. Multi-

domain management and orchestration enable E2E network slicing, leading to efficient integration of public networks and NPNs.

Furthermore, network slicing enables the integration of cloud-based resources, either centralized in large datacentres of public service providers or distributed in local datacentres and on-premises infrastructures. This integration enables the provisioning of distinct services, such as ultra-reliable and low latency networks for real-time control systems using local datacentres or on-premises servers in combination with large capacity networks for enterprise resource planning systems deployed on centralized datacentres.

Network slicing allows the realisation of private communications infrastructures for enterprises with multiple offices or facilities, providing a communication service that is similar to a VPN but with higher flexibility, dynamicity and scalability. Specific scenarios are not possible without network slicing, for example for the deployment of autonomous truck platoons. Currently, no technology provides an alternative to network slicing, which gives access to a private network infrastructure that spans public and private spaces while fulfilling specific network requirements.

Network slicing for provisioning of PNI-NPN deployment scenarios are inspired by [6] [14]. Among various PNI-NPN deployment scenarios, the two specific deployment scenarios which are the most promising and relevant for the PNI-NPN use cases are highlighted in [15].

In the RAN-CP sharing of the PNI-NPN scenario, a dedicated UP NF (UPF) inside the industry premises is used for the data traffic generated by NPN devices using the NPN network slice. The data traffic related to the NPN devices using the public slice may go through one of the UPFs associated to the public slice.

The shared RAN and the shared CP NFs are either physically or logically separated between NPN and public networks. Figure 4-2 illustrates logically separated RAN and physically separated 5G CP NFs for the NPN and public slice. The MNO's 5G CP is deployed at the central cloud, and provides public subscription management. The vertical's 5G CP, deployed at the edge cloud, is in charge of private subscription management. This vertical's *partial* 5G CP, is made available by the MNO for the exclusive use of the NPN and contains only those 5GC NFs that are required for the independent operation of the NPN. The *partial* 5G CP may interact with the MNO's 5G CP for example, it interacts with UDR/UDM of the MNO's 5G CP during a registration procedure. The user data management and control for the NPN is physically separated from other public subscription data and management, and stored securely. This 5G CP split supports better management and control, and satisfies the requirements of NPN in terms of isolation and performance.

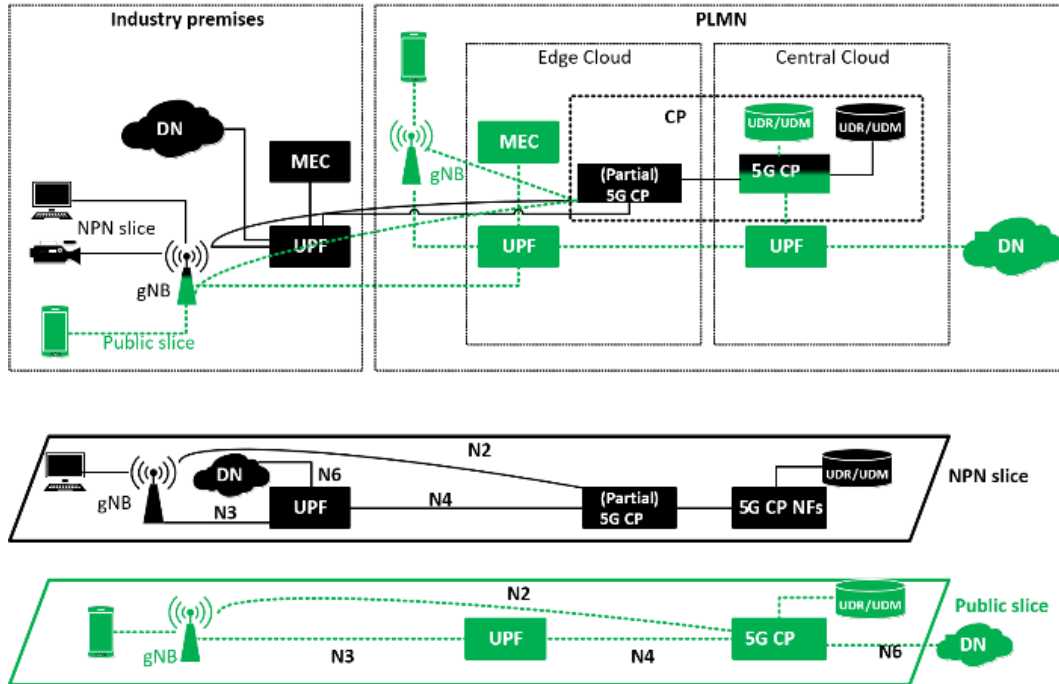


Figure 4-2 RAN-CP sharing of PNI-NPN scenario

In the RAN-CP-UP sharing of PNI-NPN scenario, the user plane traffic generated by NPN and public slices are managed and controlled by the MNO outside the factory premises. RAN, CP and UP are managed and controlled by the MNO for the E2E activities of the NPN and public slices. Figure 4-3 illustrates a logical isolation of RAN, a physical isolation of *partial* 5G CP at the edge cloud, a logical isolation of 5G CP NFs at central cloud and logical isolation of UP.

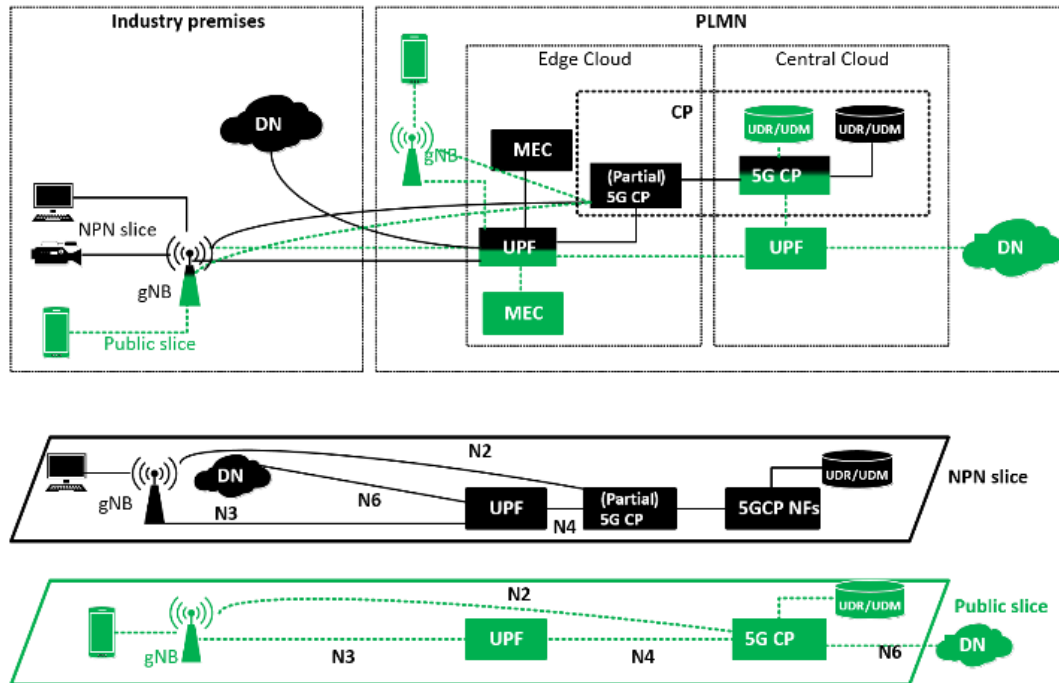


Figure 4-3 RAN-CP-UP sharing of PNI-NPN scenario

Generally, NPNs require more stringent performance agreed in SLAs and which apply to E2E service covering network slice and UE/device level. For this purpose, the GSMA defined Generic Network Slice Template (GST) [16], which contains a set of Network Slice attributes that can characterize a type of Network Slice and can be used to specify the SLA between a service provider and a service customer. Figure 4-4 [17] illustrates the relationship between GSMA GST and 3GPP ServiceProfile and SliceProfile, and how GST attributes are translated into domain specific configuration parameters for the 5GC, the NG-RAN and TN domain.

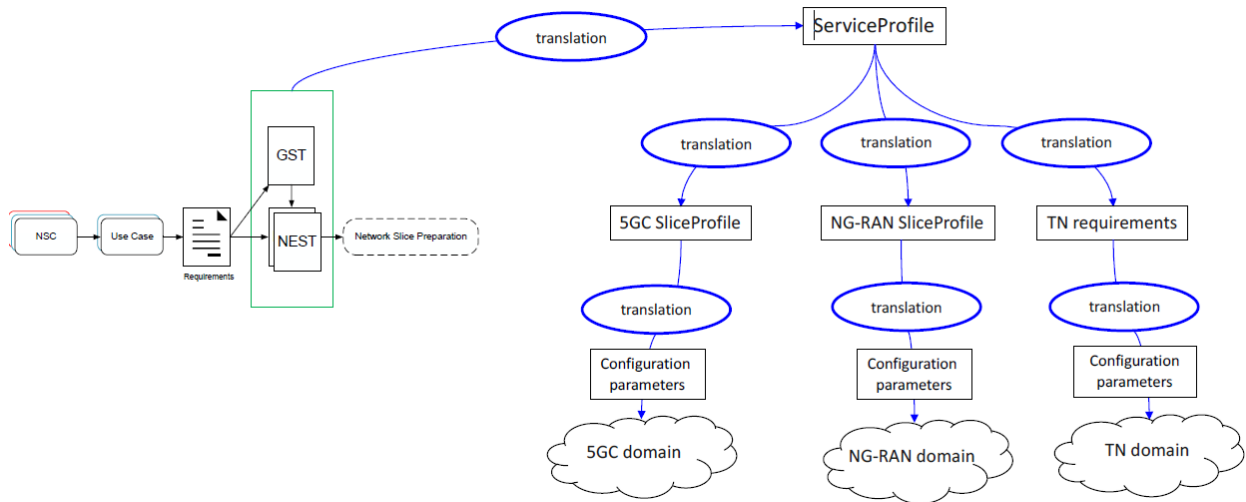


Figure 4-4 Relation between GST and network slice NRM Service Profile [16]

In a SNPN deployment scenario, the NPN CP NFs can control and enforce the slice SLA attributes as specified in [18] [19] and [20]. In a PNI-NPN deployment scenario, the current control and enforcement mechanisms for slice SLA attributes may require enhancements for E2E SLA control across NPN service provider and NPN service customer, in particular between CP NFs of the NPN and the PLMN.

3GPP defines a **Service-Based Architecture (SBA)**, illustrated in Figure 4-5, whereby the control plane functionality and common data repositories of a 5G network are delivered by way of a set of interconnected Network Functions (NFs), each with authorization to access each other's services. SBA represents an enabling technology for flexible NPN deployments allowing for the integration of AFs from enterprises with NFs, following the same design pattern. It allows for exposing network capabilities towards the customer via well-defined interfaces. Through SBA, access to the network data analytics function (NWDAF) can be provided, facilitating advanced analytics functions for the applications.

By way of the Service Communication Proxy (SCP), a controlling mechanism for inter-NF communication is introduced, although a clear separation of concerns between 5GC functionality and communication among 5GC NFs is work in progress, studied in [21].

SBA allows the application of the microservices paradigm for 5G NFs, enabling the instantiation of more than one instance of the same service to handle demand. As a result, lifecycle management of NFs can be automated following a Cloud Native approach.

SBA is an enabling technology for NPNs responding to the demand for a higher degree of flexibility in the instantiation of CP functions. The deployment location of 5GC NFs is transparent for the customer, and seamlessly supported by SBA.

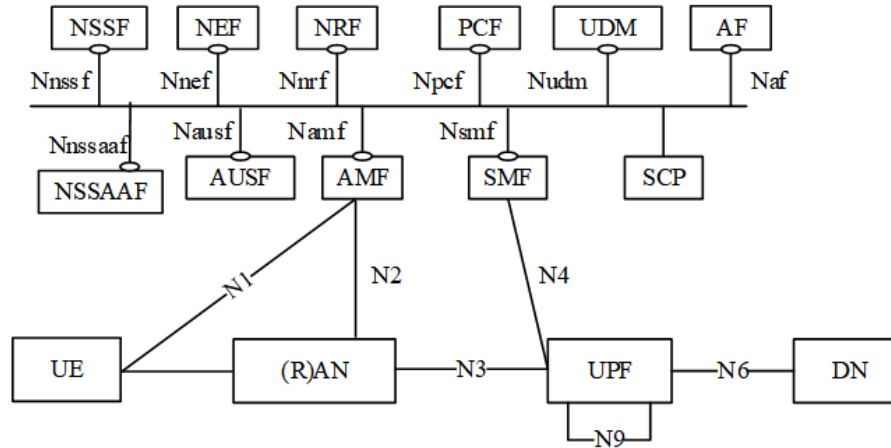


Figure 4-5: System architecture of the 3GPP system, Release 17 [19]

The functions related to **access control, including subscription, authentication and SIM provisioning is a critical aspect of NPNs**, and support an efficient and effective interworking between the NPN and the PLMN. *Roaming* supports the mobility of the subscriber across the home and visited networks. Roaming is supported by commercial agreements and technical interfaces leveraging well-defined 3GPP mechanisms, such as *cell reselection* and *handover*. In the case of cell reselection, the UE receives instructions to switch networks in a deterministic manner; a tight integration of NPN and PLMN is required. In the case of handover, the UE will switch network when it has lost signal and autonomously attempts to find an alternative. However, the coverage areas of the NPN and PLMN may be overlapping, which may cause the UE to remain connected to the PLMN even when it is within reach of its NPN, defeating the purpose of a private network. Currently there is no mechanism to force the UE to switch to the NPN. Handover is a deterministic solution but its application is limited to the cases where the RAN is shared between NPN and PLMN, in order to prevent arbitrary handover attempts by any UE. In both cases (cell reselection and handover), it is not a matter of technical feasibility, rather a business choice, but which can add complexity.

To remove uncertainty regarding radio connectivity, the UE must be able to connect to both networks leveraging latest SIM technology. The following options are possible:

- *Dual IMSI SIM*, in which two SIM identities are stored inside the same physical SIM. The user cannot use both SIM identities at the same time, but can switch between them manually by using an application running on the UE.
- *Dual SIM Dual Standby (DSDS)* UEs allow both SIMs to be “active” simultaneously, with one of them in “standby”.
- *eSIM* technology supports the dynamic installation of SIM profiles. DSDDS phones with eSIM support enable a UE to connect to the NPN and PLMN at the same time.

Service continuity support for a UE moving between multiple NPN sites, is an enabling capability for NPNs. This is the case for example when a truck delivers goods between two subsidiaries of an enterprise, or an Automated Guided Vehicle transports material between a warehouse and an outdoor delivery point.

When a UE moves out of the radio coverage of the NPN, it may wish to continue its ongoing services received from the NPN. In the case of PNI-NPN deployment, this can be realized through the 3GPP handover procedure within a PLMN. In the case of SNPN deployment this can be realised through the 3GPP handover procedure between non-3GPP access and 3GPP access. Depending on the direction of handover, the UE may experience long service interruption due to the switching between 3GPP access mode and non-3GPP access mode as well as additional registration and PDU session establishment procedure in the underlay network. Long service interruption can be avoided or reduced using the following methods:

- For single radio UE, the UE may perform early registration and PDU session establishment in the target network using non-3GPP access before losing the radio coverage of the current network.
- For dual radio UE, the UE can register to the same 5GC and/or register to both SNPN and PLMN at the same time.
- In case the UE can receive the same service from the SNPN and the PLMN, the UE may decide to switch to another network for direct 3GPP access after losing the radio coverage of the current network.

A UE should be able to select the most appropriate mobility option for service continuity support considering the UE radio capabilities and the service continuity requirements of the applications. The network may assist the UE to make a better and timely decision based on the UE location, network deployment, and service agreements.

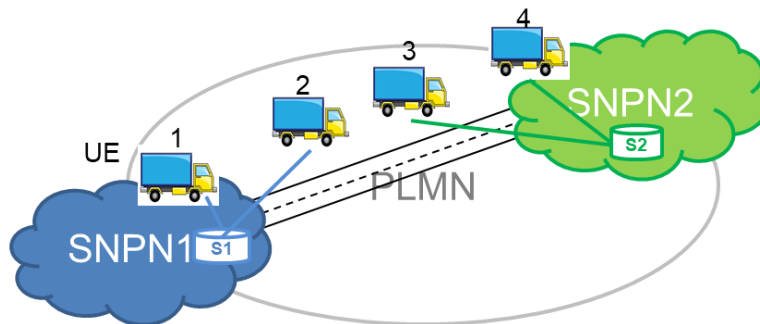


Figure 4-6 Scenario illustrating the requirement for service continuity

The **5GLAN** feature allows the integration of mobile networks as part of an existing IT infrastructure. 5GLAN reduces the need for Ethernet cabling and exhibits similar connectivity properties. In traditional Ethernet communication, a device finds peer devices through discovery mechanisms based on broadcast, for example through the Address Resolution Protocol (ARP) or Universal Plug and Play (UPNP).

In 5GLAN, a UE must obtain the identifiers of other UEs in the same private domain of 5GLAN-type services. The standardisation of 5GLAN is in progress [32], and several issues are listed for resolution, including:

- Network discovery, selection and access control
- Network identification
- System enhancements to support Time Sensitive Networking and time synchronization aspects

- 5G LAN-type services such as group management, service discovery, selection, and restrictions
- 5GLAN communication, including group communication, one to one, one to many communication
- Isolation and security of 5GLAN groups
- Accessing PLMN services via non-public networks and vice versa

Time Sensitive Networking (TSN) is one of the main requirements of certain enterprises in private network settings. TSN support is a motivation for deployment of NPNs, as largely described by 5G ACIA [24]. TSN features enable synchronizing mobile network UEs and can be used to synchronize the mobile network with existing IT infrastructure.

The latest release of 5G specification considers the concept of a TSN bridge and supports the fully centralized TSN configuration model, where a Centralised Network Configuration (CNC) entity configures both Ethernet and 5GS bridges as a unified network. The 5GS should support Medium Access Control (MAC) learning and flooding based forwarding as well as the static forwarding as configured by CNC. 3GPP has defined that a 5GS can be modelled as one or more virtual TSN bridges.

With the standardized support for TSN, a 5G system is modelled as a set of IEEE-compliant virtual Ethernet-TSN bridges when it is deployed in the field. The 5G system consists of 5G core network and radio access network. The 5G User Plane Function (UPF) is a gateway to the wireline network, and the radio access network provides wireless connectivity to the mobile devices. The TSN Translator (TT) function enables interworking between 5G and the wireline TSN network. On the control plane, a 5G bridge provides a management function (the 5G TSN Application Function (AF)) that interacts with a CNC of the TSN network.

The TSN AF reports the 5GS bridge capabilities to CNC such as minimum and maximum delays between every port pair and per traffic class, including the residence time within the UE and Device-Side TSN Translator (DS-TT). Topology discovery information based on IEEE 802.1AB Link Layer Discovery Protocol (LLDP). The TSN AF shall be pre-configured (e.g., via OAM) with a mapping table, which contains TSN traffic classes, pre-configured bridge delays such as delay between UE and UPF / Network-side TSN translator (NW-TT) and priority levels. Based on the capabilities of all bridges the CNC calculates the traffic paths and schedules in the network and provides the bridge configuration to the 5GS through the TSN AF.

Furthermore, a UE must have attached network functions of time stamping and synchronisation through DS-TT. Time synchronization is implemented using gPTP (generalized Precision Time Protocol) Sync or Follow Up messages as defined in 3GPP TS 24.535 [33].

5G-ACIA has investigated the integration options of 5G with TSN for industrial automation [24]. The TSN can be utilized across the levels of enterprise edge cloud, industrial backbone network and local production cell and machine for different time-sensitive communication applications. The 5G-supported TSN is expected to be highly appreciated in flexible manufacturing and process automation settings.

The most discussed application of the 5G supported TSN is the Industrial IoT (IIoT) in industrial automation [22]. In addition, the professional audio/video content production industry – to which the Audio Video Bridging TSN is an important enabler – is also showing an increasing interest in 5G NPN [23].

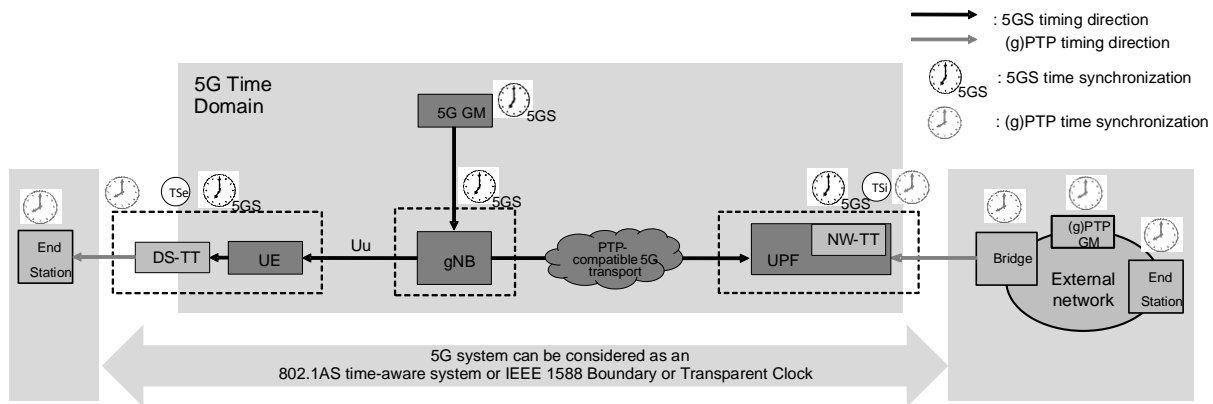


Figure 4-7 5G system modelled as a TSN bridge (Source TS 23.501 [19])

Integration of **non-3GPP access technologies** is a requirement and an enabling technology for **NPNs** because of existing deployments or alternative technology choices based on business considerations or other constraints for example in extremely dense network deployments and in order to increase spectral efficiency and reduce the load on 5G networks. Seamless integration of non-3GPP access technology must support (i) establishment of secure connection; (ii) connection/service continuity; and (iii) careful distribution of network traffic flows.

Secure tunnels between the 5G core and a UE that is connected to a non-3GPP based private network can be established via either N3IWF or TNGF depending on whether the non-3GPP network is listed as untrusted or trusted, respectively. When a UE establishes a connection to the non-3GPP access network, it also sets up a secure tunnel against N3IWF or TNGF which is then mapped to a per-user, per-access network tunnel for the user and control plane interfaces against the 5G core. This can be seen such that N3IWF/TNGF terminates the user and control plane interfaces to the 5G core network.

Integration can also make use of the recently defined access traffic steering, switching and splitting (ATSSS) function for 5G systems as described in [34]. ATSSS enables simultaneous utilization of user plane resources of 3GPP and non-3GPP access network. As its name indicates, ATSSS considers three different procedures, namely:

- **Traffic steering:** selects an access network for a new data flow and transfers the traffic of this data flow over the selected network, which can be 3GPP or non-3GPP network. There are five steering modes described, namely, active-standby, smallest delay, load-balancing, redundant and priority-based. These steering modes can be used to balance/prioritize the load between the access networks or improve reliability by duplicating the traffic flows.
- **Traffic switching:** moves all ongoing data flows from one access network to another. It can be used to provide data traffic continuity.
- **Traffic splitting:** divides the data traffic flows onto 3GPP and non-3GPP access networks. It can be used to aggregate traffic flows to improve throughput by utilizing user plane resources of 3GPP and non-3GPP networks.

The traffic steering, switching and splitting policies are provided by 5G core (generated by PCF, translated to rules by SMF, and pushed by UPF/UE), and they are based on pre-defined values for either all traffic types or some specific traffic type such as UDP/TCP to a specific IP address/port. The ATSSS rules are ordered in a way that as long as a data flow matches a rule, the data flow gets routed according to the rule

and the remaining rules are not considered. The performance of the enforced policies is monitored by path performance measurements. If the targeted service performance is below its threshold, an ATSSS policy/rule change is initiated.

As can be inferred by the different deployment scenarios introduced in section 3.1, the integration of public with private/edge cloud infrastructures into hybrid cloud constellations is a prerequisite for certain use cases. The integration of NPNs in public cloud infrastructures will widen their diffusion, since it makes 5G wireless access technology available to the customer with a simplified installation process. Indeed, when the softwarized mobile core network functions are deployed by a vendor or integrator in the cloud, and made accessible to a customer, the latter just needs to attach the radio access infrastructure via Internet to the remote mobile core instance. Such a deployment allows the creation of localized dedicated 5G coverage, with a comparable effort as for the setup of Wi-Fi. Deploying the core network in the cloud makes it possible to easily leverage its monitoring, self-healing, telemetry, automation, and scaling functionalities. Such a network architecture is particularly adapted to 5G NPNs that interconnect more than one physical site, like different branches of the same company.

Whenever appropriate, a constellation of multiple local access points can be deployed and jointly managed by the non-public core network. Specific core functions (like the UPF) can be distributed at edge nodes, typically collocated with the access points, to enable local steering and routing of traffic within a firewall. This can be exploited to yield deterministic latency, increased security, and improved economics. In this kind of flexible deployments, only the more complex core network functions (like authentication, mobility, etc.) are instantiated in the public cloud and can be shared to simultaneously serve multiple edge nodes.

Positioning and localisation with an accuracy down to the centimetre level are enablers for applications such as AR/VR, self-driving cars, drones and indoors navigation. These applications are on the priority list in the verticals industry 4.0, automotive, and smart logistics among others. The example use case presented earlier, where an Automated Guided Vehicle transports material between a warehouse and an outdoor delivery point supported by capabilities in the NPN, is a good representative of such applications. The customer is then able to locate goods and parcels in transit and within distribution centres.

These applications are enabled by accurate localization techniques that exploit Radio Access Technology (RAT)-dependent and RAT-independent technologies, and applying data fusion from heterogeneous observations [25]. While in outdoors scenarios Global Navigation Satellite Systems (GNSS) are the dominant technology, Ultra-Wide Band (UWB), or Wi-Fi Fine-Time Measurement (FTM) are technology candidates for indoors precise localisation. 5G is being studied as a localisation technology both for indoors and outdoors with the advantage that it can provide connectivity and location in a single package.

Network location was first part of 3GPP standards in GSM (3GPP TS 04.31), and has been part of consecutive generations ever since. Currently, for 5G new requirements have been described for network-based location in 3GPP TR 38.855 [35]. The location providing system architecture is described as an entity with a REST API exposed to the 5G core in 3GPP TS 29.572 and 3GPP TR 23.731.

Even if SNPNs are not designed for public use, users can still be authorized to use both SNPN and PLMN services. **Access to PLMN services via Stand-alone Non-Public Network (SNPN)** as well as access to SNPN services via PLMN is in most cases a self-evident requirement. 3GPP specifications foresee means

for users to access the services offered by PLMN via SNPN and the services offered by SNPN via PLMN. In both directions this works via the deployment of non-3GPP inter working function (N3IWF) functionality. Figure 4-8 represents the reference architecture to provide access to PLMN services via SNPN specified in 3GPP TS 23.501 [19]. The same reference architecture is used to provide access to SNPN services via PLMN when *SNPN CN* is replaced with *PLMN CN* in Figure 4-8.

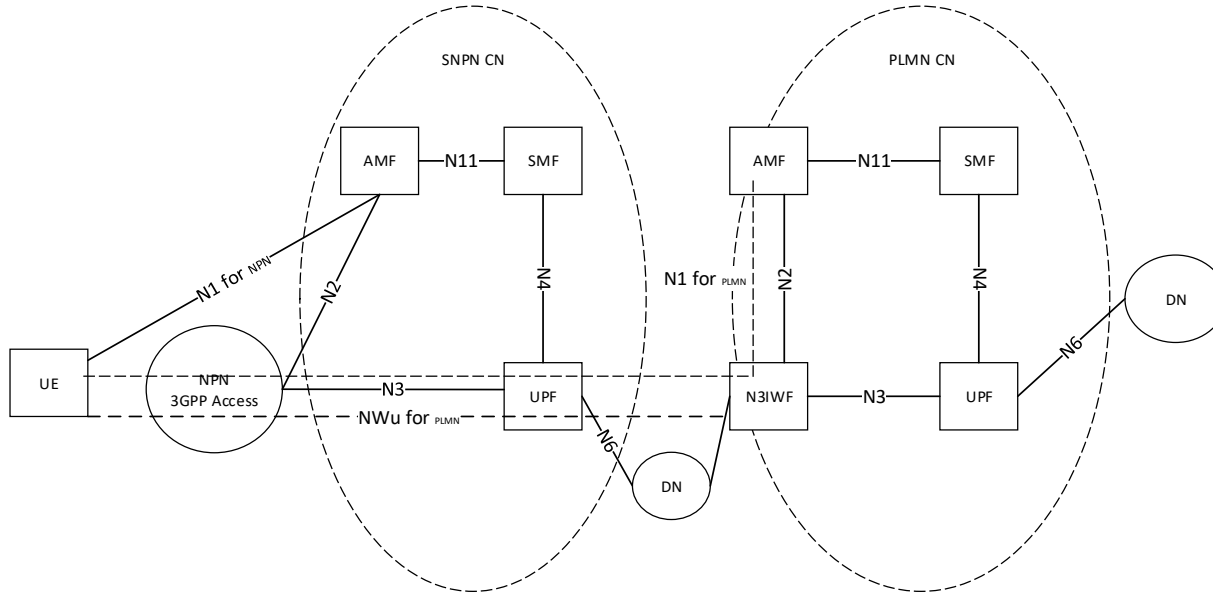


Figure 4-8 Reference architecture to provide access to PLMN services via SNPN [19]

Service continuity can be supported but depends on the UE capabilities as described earlier. Nevertheless, the existing handover procedure between non-3GPP access and 3GPP access can be used to support session continuity as one of the networks is considered non-3GPP access. In case UE has dual radio capability, the existing handover procedure between non-3GPP access and 3GPP access as well as the user plane resource additional procedure for multi-access session is used to support service and session continuity between SNPN and PLMN [19].

Depending on the NPN deployment scenario and based on the vertical needs, there can be cases where a user needs to access services from different NPNs. In such cases, there are requirements on:

- (i) enabling users to access multiple NPNs;
- (ii) authorizing users to efficiently access and move between multiple NPNs;
- (iii) supporting optimized access control and service continuity between NPNs;
- (iv) using the same QoS mapping for uplink and downlink traffic within different NPNs; and
- (v) enabling users to efficiently select NPNs during network selection.

Further considerations on interconnecting SNPNs focus on enabling an SNPN to take the role of PLMN and provide access to another NPN by using the network slicing mechanism. This option may be considered if there is no need for an SNPN user to access PLMN services at all. For example, a CPE is used to deliver/provide specific operation within a factory environment, and the CPE requires to access only services offered by another NPN. Thus, in that case, service/session continuity is crucial between SNPN and SNPN-integrated NPN. A similar consideration applies in case NPNs are deployed as PNI-NPNs. Again, as the network slicing solution can be used to deploy NPNs as PNI-NPN, interconnecting different NPNs that are deployed as PNI-NPN by the same PLMN can be achieved via network slice management/coordination. As in the existing solution on PNI-NPN as a network slice of PLMN,

authorization, optimized access control and service continuity between NPNs can be achieved by configuring S-NSSAIs specific to each NPN.

3GPP TS 23.501 [19] defines a Non-Public Network (NPN) that enables deployment of the 5G System for private use, in particular:

- (i) a Stand-alone Non-Public Network (SNPN), operated by an NPN operator and not relying on network functions provided by a Public Land Mobile Network (PLMN) and
- (ii) a Public network integrated NPN (PNI-NPN), a non-public network deployed with the support of a PLMN.

In a SNPN deployment scenario, the SNPN Network Functions (NF) may need to interact with the PLMN NFs, e.g., the AMF in SNPN needs to interact with a UDM/AUSF in the PLMN, in order to get User Equipment (UE) credentials, so that the UE can access the SNPN, as defined in TR23.700-07 [26].

In a PNI-NPN deployment scenario, the NPN NFs may also need to interact with the PLMN NFs, e.g., the PLMN CP NFs control the NPN User Plane (UP) NFs. 3GPP Release 16 supports the interaction between NFs in serving and visiting PLMNs, in particular via Security Edge Protection Proxy (SEPP) pairs [19]. However, the PLMN and the SNPN have very different network sizes and business relationships. Thus, there is a need for not only a secure communication but also scalable service communication between PLMN and NPNs.

A secure and scalable communication between PLMN and NPNs needs to support the following service communication and exposure functionalities:

- monitor the service traffic going out/in the network or network domain,
- aggregate or shape the traffic (e.g., service requests, monitoring data) going out/in the network or network domain when appropriate (i.e., this may be necessary due to a too high number of service traffic or overall traffic load to reduce congestion),
- perform the conversion of service parameters between different networks or network domains,
- change the source/destination service address and
- support the registration and discovery mechanism.

Figure 4-9 shows an example of a secure and scalable communication of CP NFs between PLMN and NPNs via a proxy which supports the above-mentioned functionalities. Generally, a proxy in one network or network domain should be able to connect to multiple proxies in one or more other networks or network domains. Service aggregation and traffic shaping is not supported between NPNs or between NPN-PNI.

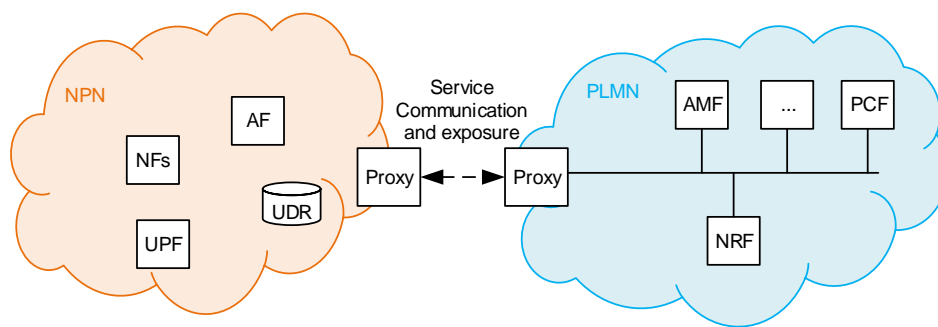


Figure 4-9: CP NFs service communication and exposure between PLMN and NPN via X-Proxy.

Given the wide variety of scenarios where NPN assets include non-public xNFs and applications, and which are distributed across two (or more) administrative domains (i.e., the PLMN or public cloud), adequate **connectivity and networking services** are required, typically provided by an MNO. The examples PNI-NPN scenarios described in section 2.1 indicate that often some assets are deployed on the private premises, and the rest hosted by at an edge of central cloud infrastructure. Networking services are necessary for conveying data, control and management traffic between the private premises and the corresponding PLMN. Table 4-1 provides guidance for deciding on a networking service, providing an overview of the main features and main fields of applicability.

Table 4-1 Solutions for data networking services

Solution	Topology	OSI	Technology	Underlay	QoS	Cost (per BW unit)
IPSec	PtP ⁴ , MP ⁵ , Mesh	Layer 3	IP	Shared	Low	Low
SD-WAN	PtP, MP, Mesh	Layer 3-7	SDN	Shared	Low-Mid	Low-Mid
Metro Ethernet	PtP	Layer 2	SONET	Dedicated	High	Low-Mid
EPL	PtP	Layer 2	SONET	Dedicated	High	High
MPLS VPN	PtP, MP, Mesh	Layer 2-3	MPLS	Shared	Low-Mid	Mid-High
EVPL	PtP, MP	Layer 2	MPLS	Shared	Low-High	Mid-High
VPLS	PtP, MP, Mesh	Layer 2	MPLS	Shared	Low-High	Mid-High
Wavelength	PtP	Layer 1	DWDM	Dedicated	High	Low

With respect to **security**, the increased adoption of 5G by new stakeholders in the ICT value chain extends the attack surfaces, as a result of:

- the amount of new use cases made possible – expressed by higher amounts of information, traversing the network at increasing speeds, with such information being associated to a myriad of different service types,
- new technologies intrinsically integrated – virtualization, orchestration, MEC...) and
- new industry verticals – featuring different types of information, and how it is generated, accessed/consumed and even different degrees of interaction with service providers

The intrinsic network control automation procedures, further contribute to the expansion of the attack surface. Therefore, the same aspects that contribute to potentially make security a more complex capability, need to be leveraged in order to promote it, particularly considering that the uncertainty of attacks grows, along with their exploitation capacity.

⁴ Point-to-Point

⁵ Multi-Point

NPN-deployed solutions provide new capabilities that leverage the deployment of new security solutions and mechanisms. Certain operational aspects are controllable within the non-public scope. Non-public deployments in scenarios such as smart factories allow the deployment of tighter latency control mechanisms. Such latency control mechanisms can be leveraged for the deployment of new security mechanisms, such as Moving Target Defense (MTD) [8], which imposes a time limit upon the validity of the gathered information, after which it becomes unactionable. Therefore, exploiting the private service(s) should become as hard as the first instants in which the attacker got a foothold to that network. MTD is a versatile defence mechanism that can be used to protect many types of services, without needing prior knowledge of the inner-workings of the service itself. However, the MTD mechanisms are not meant to assure the correctness of the function when on an adversarial setting.

If such a stringent requirement must be fulfilled, as is the case in mission-critical functions that impact public utilities (energy grids) or public safety (transportation signals), the correctness of the functionality in an adversarial setting must be assured through a different approach. In this context, functionality refers not just to the Network Function, but also the 5G service provisioning platform services and underlying providers/resources which are entrusted with rules enforcement. Cyber Mimic Defence (CMD) [9] is a suitable approach for this type of scenario. However, unlike MTD, which is very versatile, the use of CMD requires multiple implementations of the same function by different parties, and the function being protected must obey the Input-Process-Output (IPO) model. That is, the output of the function must be calculated in a fully deterministic way when given the same input.

As for any network, **Operation, Administration and Management (OAM)** must be considered an intrinsic part of an NPN deployment. In certain cases, e.g., when the NPN customer has sufficient IT expertise in-house, an independent network operation is feasible though in-house management competencies encompassing the full NPN lifecycle management process. This will enable the vertical, among others, to manage authentication and authorisation of NPN devices, integrate the IT systems and control the exposure of network data. As illustrated in Figure 4-10, these tasks can be arranged into five main groups:

- (i) feasibility study,
- (ii) network planning,
- (iii) network installation and set-up,
- (iv) integration in the company IT infrastructure, and
- (v) operation and management.

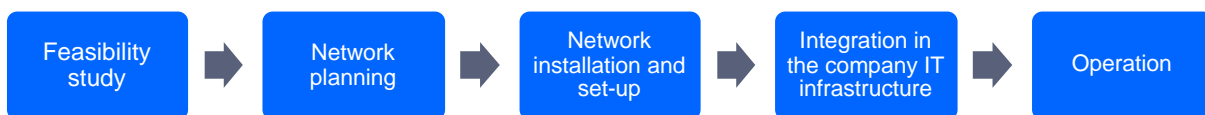


Figure 4-10 NPN lifecycle management

The first stage is the **feasibility study**. Before an enterprise customer starts using a communication technology like private 5G, it is essential for the customer to conduct a comprehensive economical and technical assessment, where a cost-benefit evaluation and a site analysis are important aspects. This is the heart of a feasibility study that should determine whether the legal, time-related and economic prerequisites for the desired deployment option of NPN can be satisfied, and the impact on organization related issues (e.g., how business processes will change and the issues of providing personnel and creating internal know-who must be reviewed) the selected NPN deployment option may bring.

Once this feasibility study gives green light to move forward, the next stage is the **network planning**. In addition to planning radio coverage, which is a sensitive factor in providing reliable services, this stage also includes numerous tasks of connection planning (physical and logical requirements for connecting 5G components, considering the electrical and cable network topology together and the physical hardening), infrastructure size (including compute, storage and networking resources), service architecture, and integration with existing/local systems.

With the completion of network planning stage, the **network installation and set-up** can get started. For this new stage, a number of aspects need to be considered. First, the *pre-testing and acceptance*. Due to the lack of market experience with private 5G networks, it is recommendable to start as soon as possible with prior testing on a small scale. Secondly, the *installation of systems and infrastructure*, including compute and networking fabric. The provider's SIM or eSIM must be installed and configured. Finally, the *adopting services*, whereby service applications and value-added features (e.g., localization support, MEC, etc) need to be integrated and jointly assessed.

As in occurs for any incumbent technology or service, one of the most critical issues to ensure a successful case story is the **integration in the company IT infrastructure**. As NPN becomes a part of the enterprise customer's IT infrastructure (and in industry 4.0 scenarios, with the previous industrial communication network), rights and service management of the 5G network based on 3GPP management system require close cooperation with the existing system landscape, with the definition of appropriate provisioning interfaces (management services) between them. This needs to be accompanied with a unified and consistent management of users, in terms of authorization, authentication and subscription data access/storage.

With the completion of the previous four stages, usually categorized into the so-called preparation stage of the NPN lifecycle, the NPN is ready for use. That means that 5G networks and hosted applications can be provisioned and activated, so that user incoming/outcoming traffic can be processed, thus entering into the **operation** stage. The ultimate goal of this stage is to keep NPN up and running, ensuring it behaves as expected (i.e., KPIs are met) and if not, identifying the cause of misbehaviour so corrective management actions (e.g., scaling) can be triggered accordingly. To that end, it is required: (i) data-driven and policy-based rules for FCAPS management and SLA monitoring, complemented with advanced mechanisms allowing for closed-loop automation; (ii) maintenance/network adaptation, with regular upgrades over NPN components and on-site/remote support.

Capability exposure can be defined as the ability of a network service provider to securely expose capabilities from their managed functions towards one or more authorized customer. These functions include:

- **xNFs**. The ability of exposing the capabilities from one or more VNFs/CNFs (including the NFV network services resulting from their composition), making them available for external consumption, is referred to as *network capability exposure*. First solutions that allow this exposure are already available, such as the Network Exposure Function (NEF), which provides a unified single-entry point to 5GC, and Software-Defined Transport Network (SDTN), which provides WAN connectivity capabilities agnostic to the underlay backhaul through the NBI. In the RAN segment, the O-RAN fostered principles of RAN disaggregation and openness facilitate the exposure of gNB-DU and gNB-CU offered capabilities through the E2 interface, so that RAN Intelligent Controller (RIC) and associated xApps - including RIC built-in xApps as well as over-the-top xApps- can consume and manipulate them. The work on RIC is still in its infancy.

- **MFs.** The ability of exposing the services from one or more Management Functions (MFs), making these services available for external consumption, is referred to as *management capability exposure*. This category, unprecedented so far and much less mature than network capability exposure, has raised attention in industry community with the use of novel XaaS model, specially NaaS. In this regard, different surveys that can be found in acclaimed technology analyst reports (e.g., Gartner, Heavy Reading, Analysis Manson, etc.) state that NaaS, and in particular NSaaS when applied for NPN provisioning, open up opportunities for service innovation, with a win-win solution for both slice providers and tenants. NSaaS allows the provider to make the network instances available to different tenants, allowing the latter to consume them at their own administrative domain. To that end, the different analyst reports recognize the need for the provider to open its management systems to individual tenants, allowing them to get involved in the operation of received network instance by regulating this openness and exposure, the provider can define the degree of control the tenant can take over the network instance.

In general, the Network Exposure Function (NEF) capabilities can be categorised as illustrated in Figure 4-11.

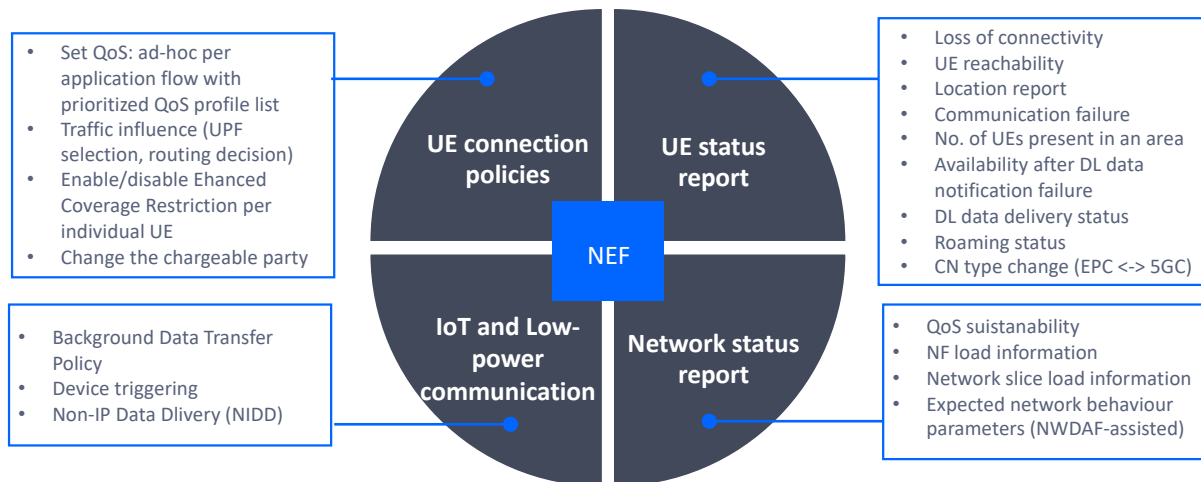


Figure 4-11: Network Exposure Function information categories

The **management capability exposure** in NPNs is highly dependent on the OAM model in place. An OAM model allows specifying “who” is responsible for managing “what” part of the network. In NPN scenarios, the “who” represents stakeholders participating in the NPN operation, i.e., MNO and/or an enterprise customer. The various NPN scenarios, with a number of in-scope use cases and a plethora of deployment variants (section 2.1), may lead to the definition of different OAM models. Table 4-2 provides a tentative categorization of these models, with 1.x models applicable to SNPN scenarios and 2.x models corresponding to PNI-NPN deployments:

- **Model 1A:** The NPN is entirely managed by the enterprise customer, meaning that the customer has full control on all NPN components, no matter if deployed on-site or at the hyperscaler cloud⁶.

⁶ For those NPN components hosted by the hyperscaler cloud (see SNPN #2 and SNPN #3 scenario), the hyperscaler is only responsible for (cloud) resource management activities. All that is related to the NPN component application layer/logic is up to the enterprise customer.

Cooperation with MNO is only required if SNPN has connectivity to external PLMN resources (e.g. to allow UEs camping/registered into the SNPN to access public data network services such as voice and emergency services).

- **Model 1B:** The NPN operator role is shared between the MNO and enterprise customer. In this model, MNO is mostly focused on 3GPP 5G management aspects (provisioning, fault management, performance assurance using 3GPP management system), while the customer focuses on device and LAN service-related management aspects instead, e.g., device (group) authentication/authorization, E2E service analytics, etc. To perform these management activities, it is important for the customer to consume some 3GPP 5G management capabilities. The customer gets needed management capabilities from the MNO according to the business agreement between the two parties.
- **Model 1C:** The NPN is entirely managed by the MNO, which also plays the role of PLMN operator. The customer focus on business logic, handing all the operational activities over the MNO, leveraging its historical OAM expertise. This model brings OPEX reduction for the customer.
- **Model 2A:** Similar to the model 1B, but with less control retained by the customer.
- **Model 2B:** The NPN is entirely managed by the MNO, which also plays the role of PLMN operator. Apart from bringing the same advantages for the customer as in Model 1C, Model 2B also guarantees service continuity and roaming capabilities with the PLMN.

Table 4-2 Tentative categorisation of OAM models for NPN

Model	3GPP NPN category	NPN operator
1A	SNPN	Enterprise
1B	SNPN	MNO and enterprise customer
1C	SNPN	MNO
2A	PNI-NPN	MNO and enterprise customer
2B	PNI-NPN	MNO

As seen, there are situations where the NPN operator role can be played by a single stakeholder (see 1A, 1C, 2A), or shared between both stakeholders. The selection of one or another model strongly depends on the individual customers and their economical/technical abilities for network operation. For example, many small and medium-sized enterprises (SME's) do not have sufficient technical expert; therefore, cooperation with MNOs is the most cost-effective way for such customers (see models 1B, 1C, 2A, 2B). On the other hand, large-sized enterprises like manufacturing or electric utility companies might want to have full control and governance of their NPNs; in such a case, they may go for SNPN scenarios with model 1A.

Finally, note the relevance of management capability exposure in models 1B and 2A, where the MNO makes some capabilities available for consumption to the enterprise customer. These capabilities can be of two types: (i) configuration management related capabilities and (ii) assurance related capabilities. The first capability group defines the ability of a customer to modify the parameters on certain nodes. To that end, the MNO should characterize the permissions associated to these parameters (i.e., isReadable, isWritable, isInvariant, isNotifiable) accordingly. The second capability group defines the ability of a customer to subscribe to certain performance measurements and fault alarms, so he can consume them in the format he seems more appropriate (e.g., batches vs streaming).

There are several **spectrum options** for NPNs dependent on the requirements of the vertical company in question and the spectrum regulations in the given country. Using unlicensed or license-exempt spectrum

is the simplest solution if it can offer the QoS the company requires. This might be the case if the QoS requirements are modest or if the company has sufficient control of the radio environment (e.g. inside a factory building).

However, it is often not possible to satisfy companies' strict QoS requirements without using licensed spectrum. Regulators are considering different options for making licensed spectrum available for NPNs. These include making spectrum available for verticals either outside or in core mobile bands, use local licensing and creating license terms that allows and encourages sub-leasing of mobile spectrum to verticals. MNOs can also offer NPN solutions where the NPNs use the MNO's spectrum and end-to-end slicing is used to fulfil the MNO's SLAs with the vertical customers.

Currently, different solutions are used in different countries. The German regulator BNetzA has for example reserved 100 MHz of spectrum on the 3700 – 3800 MHz band. In the UK, Ofcom has made spectrum in the 3.8–4.2 GHz band available through local licenses. In addition, the frequency band 24.25-26.5 GHz is available for indoor use through local licenses. In Finland, the 3.5 GHz licensees are obliged to either offer services to verticals in local areas or sub-license their spectrum to verticals.

Setting aside spectrum exclusively for verticals is somewhat disputed. Some claim that this will result in underutilization of scarce and precious spectrum. On the other hand, exclusive spectrum is the best way to minimize interference to public networks and give the vertical user largest degree of flexibility. If NPNs operate in the same or neighbouring frequency bands as public networks, the NPN will often have to use TDD schemes that are synchronized to and use the same uplink/downlink ratio as the public networks, which can make the NPN less efficient for serving the vertical company's needs. In some cases, using high band spectrum (> 10 GHz) can be a good solution since such spectrum provides better isolation and has relatively relaxed TDD coexistence constraints.

Another important aspect related to spectrum regulation is spectrum harmonization. In order to enable a device ecosystem for industrial applications, the spectrum allocations in different countries and markets should be harmonized. It is also important that the regulators ensure that the spectrum will be available for the vertical company for a long time in order to defend the large investments an NPN represents in the company's facility.

Finally, licensing of spectrum for NPNs must be very simple. Current regulations and licensing schemes are mostly made with large MNOs in mind. Since spectrum is a key resource for MNOs they have deep competence and are willing to spend large resources on spectrum acquisition. Vertical companies on the other hand does not have this competence and resources. Therefore, the spectrum acquisition process should be simplified, constraints and conditions associated with the licenses should be simple, and compliance verification should be easy.

One of the most important factors that will influence small and medium NPN operators and enterprises (SMEs) is the answer to the question how simple is to buy, configure and operate wireless connectivity that can meet its needs and applications in terms of cost, device density, throughput and security? This requirement calls for a simple solution that could be interpreted as a **5G NPN “in a box”**.

An architecture and implementation for a small and simple private 5G network must still comply with the SNPN type described in section 2.1 and can target the market of SMEs that need a simple and low cost 5G network meeting the 5G performance characteristics such as for low latency, high throughput, accurate UE localisation, etc. This type of users do not have the experience and knowledge to purchase, install, configure and maintain a wireless network and are looking for a 5G solution that is “self-install”, “zero touch” and

“maintenance free” like a SOHO-based Wi-Fi router. An NPN system solution meeting these requirements consists mainly of two components as illustrated in Figure 4-12.

The NIB – Network in the BOX – includes all the network functions needed to execute applications on site from the MEC and NgCore in the upper layers side and High PHY on the O-DU in the lower layer. The NIB HW consist of two main cards: a) an FPGA based accelerator card for the HIGH PHY and a Computer on Board server card that include all the upper layers Protocol Stack NgCore and MEC. The NIB can run many O-RUs at different bands to cover the entire area needed by the NPN customer, the NIB and the O-RUs are interconnected via the O-RAN interface PHY Split protocol 7.2 option.

The O-RU – Open RAN Radio Unit – consist of the Low PHY and the RF boards and embedded antenna units. It is implemented in different frequency bands such as Sub 6GHz and mmWave (28GHz). The O-RU HW includes an FPGA based accelerator card for the Low PHY, an RF board with the analogue to digital and digital to analogue converters and the necessary RF components in the required frequency band and the dedicated active beam forming antenna.

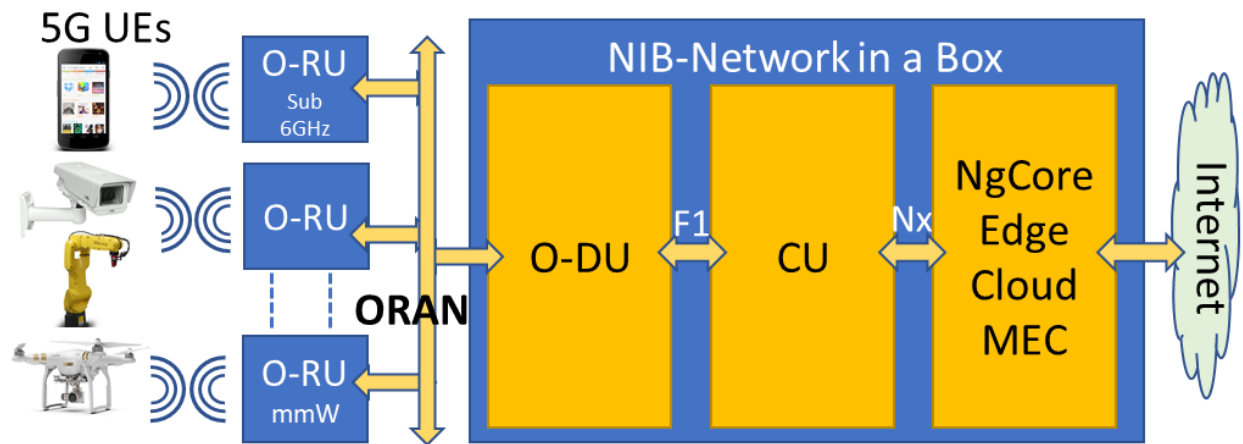


Figure 4-12: 5G NPN in a Box

A possible implementation of the NIB and O-RU is illustrated in Figure 4-13 and can be implemented as an outdoor or indoor solution. The 5G NPN implementation includes an AI-based scheduler and orchestrator that convert it to a “Zero Touch” and “Self-Install” solution and as such it dramatically reduces the customer capital and operation expenses.

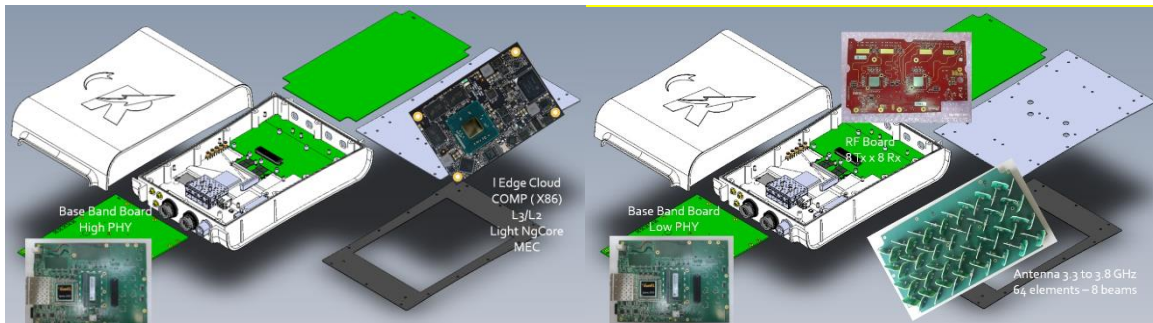


Figure 4-13 : Hardware implementation of 5G NPN in a Box

5 Impact of NPN on 5G Ecosystem

The current 5G PPP actor role model is focused on the **sole use of 3GPP 5G access** solutions for the provision of **public services**. This allows covering most of operational aspects which are relevant in PLMN scenarios. However, NPN ecosystem represents a significant leap forward, considering the involvement of resources from **multiple access technologies** as an integral part of the E2E service delivery, as well as the interoperation of private and public network infrastructures for the deployment and operation of **non-public services**. To reflect these novelties, the original 5G PPP actor role model is modified to consider the impact of NPNs, resulting in the diagram illustrated in Figure 5-1. It should be noted that the resulting actor role model shall be considered complementary to the primary model that is given in the architecture white paper V4.0 (see Figure 2-2 in [11]). Herein we present a manifestation of the Data Centre Service Provider (DCSP) role for the NPN case. This does not pre-empt the choice of a certain firm to assume the role of DCSP for the public case, the private case, or both.

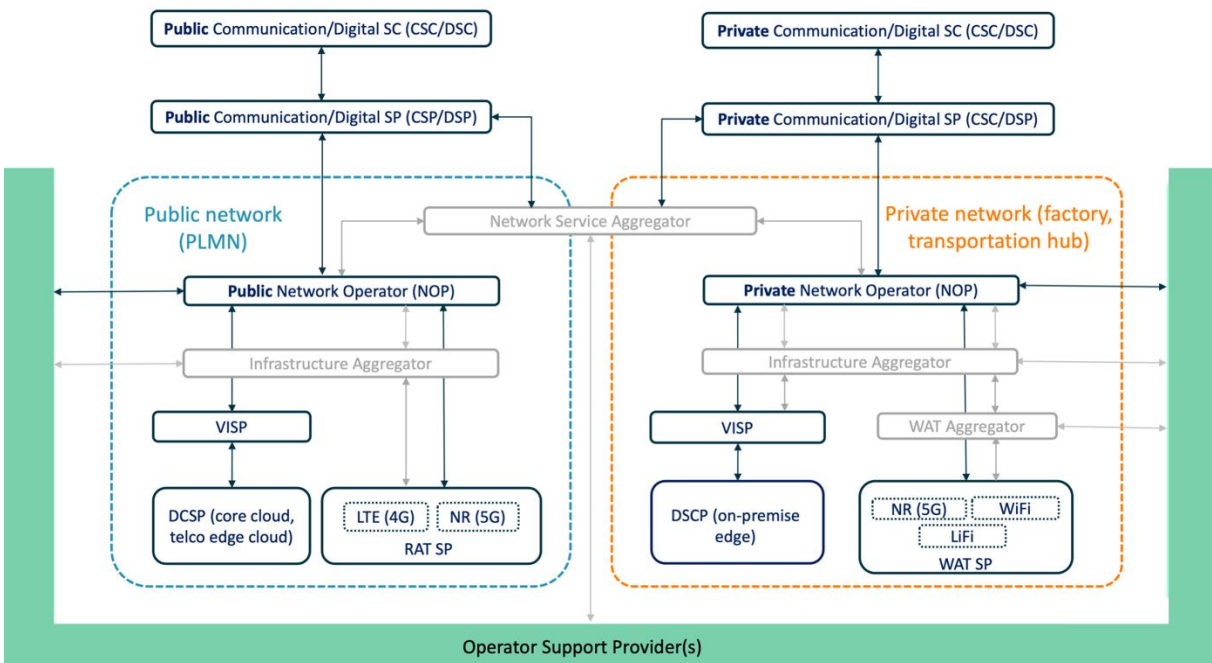


Figure 5-1: Extension of 5G PPP actor role model for NPN support

The key novelties of this new actor role model are essentially two.

On the one hand, the private and public roles are decoupled, to keep in-house management and orchestration separated from the provisioning activities executed on the PLMN. This decoupling ensures the private network can be operated independently of the PLMN, facilitating the realization of Standalone NPN as well. For PNI-NPN scenarios, the network service aggregator oversees providing the necessary means for the public-private network integration.

On the other hand, additional roles are defined. These new roles, belonging to the private administrative domain, allow for dealing with the on-premise operational aspects intentionally omitted with the original 5G PPP model. These new roles are three:

- Wireless Access Technologies (WAT) service provider: it allows for indoor coverage using one or more WATs, including 3GPP 5G NR and non-3GPP wireless technologies (e.g., Wi-Fi and Li-Fi).

- WAT aggregator: it allows federating different WATs, for a unified and consistent management of wireless resources when used in conjunction (e.g., for bandwidth aggregation, enhanced reliability, etc.).
- Data Centre Service Provider (DCSP): provides infrastructural services in local environments, leveraging the use of edge clusters. These clusters are built out of small-scale servers, sized for local execution, and typically provisioned with hardware acceleration solutions. This constitutes a key difference with respect to the commodity servers in the data centres, thus establishing a clear demarcation point with respect to traditional DCSPs (core cloud, telco edge cloud).

The biggest opportunities emerge from the ongoing digitisation of many vertical industries. In domains where a mix of very different wired and wireless communication technologies have been deployed over the last couple of decades and in which the legacy solutions do not meet anymore customer expectations, there is a high potential of business opportunities. Among the most prominent drivers for migration are:

- End-of-life of existing narrowband mission-critical networks. Such networks can be found in many vertical sectors, and are more prominent in manufacturing, public safety, transportation and logistics.
- Productivity in Industry 4.0 environments is increasingly coupled to the ability of rapidly and flexibly change the manufacturing process and shop floor configuration according to customer needs in a just-in-time manufacturing manner. This flexibility must be supported by the ICT install base.
- Emergence of high data volumes from use cases employing high resolution imaging, augmented and extended reality, surveillance as well as high number of sensors, requiring flexible aggregation and delivery of data to the processing tiers.
- High cybersecurity and data security requirements across all end-to-end network configurations. These requirements are amplified by frequent network configuration changes.
- Interconnection requirements of multiple NPNs that are forming a logical entity in cases of distributed enterprises.
- Provisioning of external interfaces for interconnection with partnering domains in B2B2C scenarios

System integrators will play a critical role in the deployment of 5G NPNs and their integration with public networks. Specialised integrations with vertical sector domain knowledge will be able to deliver turnkey solutions to their vertical sector customers. The common case could be that system integrators plan and architect the solution, deploy the equipment and develop the necessary functions to manage orchestrate and secure the solution. However, complementing construction and delivery of the solution with the capacity to fully operate the 5G NPN promises a long-term steady revenue stream for the system integrator in exchange of a worry free 5G NPN solution for the customer.




In relation to the roles introduced in Figure 5-1 above, a system integrator can be related with the role of Network Service Aggregator and Operator support Provider in addition to any roles related to planning and deploying the solution.

6 List of Editors and Contributors

Name	Company / Institute / University	Country
Editors		
Kashif Mahmood	Telenor	Norway
Anastasius Gavras	Eurescom GmbH	Germany
Artur Hecker	Huawei Munich Research Centre	Germany
Contributors		
Anastasius Gavras	Eurescom GmbH	Germany
André Gomes	Onesource	Portugal
Andres Gonzalez	Telenor	Norway
Andrés Meseguer Valenzuela	Fivecomm	Spain
Artur Hecker	Huawei Munich Research Centre	Germany
Bruno Parreira	Capgemini Portugal	Portugal
Daniel Campus Mur	I2CAT	Spain
Daniel Corujo	Instituto de Telecomunicações	Portugal
David Gomez-Barquero	Universitat Politecnica de Valencia	Spain
Dirk Trossen	Huawei Munich Research Centre	Germany
Emil J. Khatib	University of Malaga	Spain
Hanwen Cao	Huawei Munich Research Centre	Germany
Israel Koffman	RunEL	Israel
Jose Alcaraz-Calero	University of the West of Scotland	U.K.
José Antonio Ordóñez Lucena	Telefónica	Spain
Jose Costa-Requena	Cumucore	Finland
Kashif Mahmood	Telenor	Norway

Marco Centenaro	Athonet	Italy
Marius-Iulian Corici	Fraunhofer FOKUS	Germany
Mika Skarp	Cumucore	Finland
Mir Ghoraishi	Gigasys Solutions	U.K.
Ole Grøndalen	Telenor	Norway
Pål Grønsund	Telenor	Norway
Paola Sunna	EBU (European Broadcast Union)	Switzerland
Qi Wang	University of the West of Scotland	U.K.
Qing Wei	Huawei Munich Research Centre	Germany
Raquel Barco Moreno	University of Malaga	Spain
Sebastian Robitzsch	InterDigital	U.K.
Vitor Cunha	Instituto de Telecomunicações	Portugal
Wint Yi Poe	Huawei Munich Research Centre	Germany
Xi Li	NEC Laboratories Europe	Germany

Contributing 5G PPP Projects

FUDGE 5G		https://fudge-5g.eu/
5G-CLARITY		https://www.5gclarity.com/
5GROWTH		https://5growth.eu/

5G RECORDS		https://www.5g-records.eu/
LOCUS		https://www.locus-project.eu/
6G BRAINS		https://6g-brains.eu/
5G-VINNI		https://www.5g-vinni.eu/
SLICENET		https://slicenet.eu/

References

- [1] Kaloxylos, Alexandros, Gavras, Anastasius, & De Peppe, Raffaele. (2020). Empowering Vertical Industries through 5G Networks - Current Status and Future Trends. Zenodo. <https://doi.org/10.5281/zenodo.3698113>
- [2] 3GPP TS 23.501, “System Architecture for the 5G System (5GS); Stage 2”
- [3] Xinyan Coal Mine, Shanxi Mobile, and Huawei Launch 5GtoB PNI-NPN Kite-like Solution, <https://www.huawei.com/en/news/2021/2/kite-like-solution>
- [4] Internet Engineering Task Force - Autonomic Networking Integrated Model and Approach (ANIMA), <https://datatracker.ietf.org/wg/anima>
- [5] ETSI Zero Touch service and network Management, <https://www.etsi.org/technologies/zero-touch-network-service-management>
- [6] 5G Alliance for Connected Industries and Automation (5G-ACIA), “5G Non-Public Networks for Industrial Scenarios,” July 2019. [Online]. Available: https://5g-acia.org/wp-content/uploads/2021/04/WP_5G_NPN_2019_01.pdf
- [7] GSMA NG.123, “5G industry campus network deployment guidelines,” Nov 2020.
- [8] Vitor A. Cunha, Daniel Corujo, Joao P. Barraca, Rui L. Aguiar, TOTP Moving Target Defense for sensitive network services, Pervasive and Mobile Computing, Volume 74, 2021, 101412, ISSN 1574-1192, <https://doi.org/10.1016/j.pmcj.2021.101412>.
- [9] W. Liu, F. Chen, H. Hu, G. Cheng, S. Huo and H. Liang, "A Novel Framework for Zero-Day Attacks Detection and Response with Cyberspace Mimic Defense Architecture," 2017 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), 2017, pp. 50-53, doi: 10.1109/CyberC.2017.39.
- [10] Redana, Simone, Bulakci, Ömer, Mannweiler, Christian, Gallo, Laurent, Kousaridas, Apostolos, Navrátil, David, Tzanakaki, Anna, Gutiérrez, Jesús, Karl, Holger, Hasselmeyer, Peer, Gavras, Anastasius, Parker, Stephanie, & Mufungwa, Edward. (2019). 5G PPP Architecture Working Group - View on 5G Architecture, Version 3.0 (3.0). Zenodo. <https://doi.org/10.5281/zenodo.3265031>
- [11] Gavras, Anastasius, Bulakci, Ömer, Gramaglia, Marco, Iordache, Marius, Ghorashi, Mir, Garcia, Antonio, Cogalan, Tezcan, Gutiérrez, Jesús, Tzanakaki, Anna, Warren, Dan, Li, Xi, Landi, Giada, Mangues, Josep, Tsagkaris, Kostas, Frasca, Valerio, & Lee, Haeyoung. (2021). 5G PPP Architecture Working Group - View on 5G Architecture, Version 4.0. Zenodo. <https://doi.org/10.5281/zenodo.5155657>
- [12] Bringing Reinforcement learning Into Radio Light Network for Massive Connections, Project 6G BRAINS, online <https://6g-brains.eu/>
- [13] End-to-End Cognitive Network Slicing and Slice Management Framework in Virtualised Multi-Domain, Multi-Tenant 5G Networks, Project SliceNet, online <https://slicenet.eu/>
- [14] NETMANIAS, "7 Deployment Scenarios of Private 5G Networks". [Online]. Available: <https://www.netmanias.com/en/post/blog/14500/5g-edge-kt-sk-telecom/7-deployment-scenarios-of-private-5g-networks>

- [15] W. Y. Poe, J. Ordonez-Lucena and K. Mahmood, "Provisioning Private 5G Networks by Means of Network Slicing: Architectures and Challenges," 2020 IEEE International Conference on Communications Workshops (ICC Workshops), 2020, pp. 1-6, doi: 10.1109/ICCWorkshops49005.2020.9145055.
- [16] GSMA NG.116 - Generic Network Slice Template, Version 4.0; 23 November 2020
- [17] 3GPP TS 28.541: '5G Network Resource Model (NRM); Stage 2 and stage 3 (Release 17)'
- [18] 3GPP TR 23.700-40: 'Study on enhancement of network slicing; Phase 2 (Release 17)'
- [19] 3GPP TS 23.501: "System Architecture for the 5G System; Stage 2 (Release 17)"
- [20] 3GPP TS 23.502: "Procedures for the 5G System (5GS); Stage 2 (Release 17)"
- [21] FUDGE-5G, "Fully Disintegrated private nEtworks for 5G verticals", <https://fudge-5g.eu>
- [22] 5G Alliance for Connected Industries and Automation (5G-ACIA) white paper "Integration of 5G with Time-Sensitive Networking for Industrial Communications". [Online]. Available: https://5g-acia.org/wp-content/uploads/2021/05/5G-ACIA_Integration_of_5G_with_Time-Sensitive_Networking_for_Industrial_Communications_single-pages.pdf
- [23] 5G-MAG explainer 5G Non-Public Network for Content Production, Nov. 2020
- [24] 5G Alliance for Connected Industries and Automation (5G-ACIA) white paper: Integration of Industrial Ethernet Networks with 5G Networks. [Online]. Available: https://5g-acia.org/wp-content/uploads/2021/04/5G-ACIA_Integration-of-Industrial-Ethernet-Networks-with-5G-Networks-.pdf
- [25] A. Conti, S. Mazuelas, S. Bartoletti, W. C. Lindsey, and M. Z. Win, "Soft Information for Localization-of-Things," Proc. IEEE, vol. 107, iss. 11, pp. 2240-2264, 2019.
- [26] 3GPP TR 23.700-07: "Study on enhanced support of Non-Public Networks (NPN) (Release 17) "
- [27] J Ordonez-Lucena, J.F. Chavarria, L.M. Contreras, A. Pastor, "The Use of 5G Non-Public Networks to support industry 4.0 scenarios", in 2019 IEEE Conference on Standards for Communications and Networking (CSCN), Granada, Spain, Oct 2019, pp. 1-6.
- [28] Y. Poe, J. Ordonez-Lucena and K. Mahmood, "Provisioning Private 5G Networks by Means of Network Slicing: Architectures and Challenges," 2020 IEEE International Conference on Communications Workshops (ICC Workshops), 2020, pp. 1-6
- [29] GSMA White Paper, "5G IoT Private & Dedicated Networks for Industry 4.0: A guide to provide and dedicated 5G networks for manufacturing, production and supply chains", October 2020.
- [30] 5G Americas White Paper, "5G Technologies in Private Networks", October 2020.
- [31] German Federal Ministry for Economic Affairs and Energy, "Guidelines for 5G Campus Networks – Orientation for Small and Medium-Sized Business".
- [32] 3GPP TR 23.734; Study on enhancement of 5G System (5GS) for vertical and Local Area Network (LAN) services (Release 16)
- [33] 3GPP TS 24.535 V17.0.0 (2021-06); Device-Side Time Sensitive Networking (TSN) Translator (DS-TT) to Network-Side TSN Translator (NW-TT) protocol aspects; Stage 3 (Release 17)

- [34] 5G-CLARITY Deliverable D3.1, State-of-the-Art Review and Initial Design of the Integrated 5G NR/Wi-Fi/LiFi Network Frameworks on Coexistence, Multi-Connectivity, Resource Management and Positioning, August 2020, online: https://www.5gclarity.com/wp-content/uploads/2020/09/5G-CLARITY_D3.1.pdf
- [35] 3GPP TR 38.855 V16.0.0 (2019-03), Study on NR positioning support (Release 16)