5G industry campus network deployment guideline

Version 2.0

21 October 2021

This is a White Paper of the GSMA

Security Classification: Non-confidential

Copyright Notice

Disclaimer

The GSM Association (“Association”) makes no representation, warranty or undertaking (express or implied) with respect to and does not accept any responsibility for, and hereby disclaims liability for the accuracy or completeness or timeliness of the information contained in this document. The information contained in this document may be subject to change without prior notice.

Antitrust Notice

The information contain herein is in full compliance with the GSM Association’s antitrust compliance policy.

Table of Contents

1 Introduction

1.1 Background

From 2C to 2B

Mobile Broad Band (MBB) is currently the major focus for a Mobile Network Operator (MNO), and rightly so; a well-established market, needed infrastructure is in place, and the means to produce MBB services are well known by the MNOs. However, as a consequence of the digitalization of our society and the advent of 5G, the demands for capacity in the wireless networks will increase heavily. The rapid digital transformation across various industries has made it clear that wireless communication is an indispensable part of their future. 5G is a catalyst for the transformation of operators' business models from Business to Consumer (B2C or 2C) to Business to Business (B2B or 2B). 2C will continue playing major role in 5G era, and its deployment method and business model are relatively clear compared to 5G 2B business models. For instance, the communication services need to be quickly deployed and provisioned to meet the industry-grade security and performance requirements. In addition, 2B customers may have unique network Operation and Management (O&M) requirements, e.g. decoupled network service operation from maintenance.

Which role MNOs will play in 2B era?

In the conventional 2C network service era, MNOs mainly provide access networks. In order to develop new business models, it is essential for MNOs to think about how to enter the 2B market by using new technologies like 5G. However, there are still many challenging questions: How to innovate MNO’s business model to provide more than a pure connectivity pipe? Can MNOs in the end benefit from 2B opportunity and work together with industry customers to accelerate industry digital transformation? What are the business models and relevant business roles?

5G is now

In 2020, 5G era has officially arrived. Since the first release of 5G standards in June 2018, the telecommunication industry has been ready in terms of standards, products, terminals, and business, which makes 5G commercial deployment possible. Participation in the 2B type industry market is one of the main driving forces for MNOs to invest in 5G. However, the current 5G release is only the first step for MNOs to enter the vertical industry business, there is much work still to do. To tackle the 2B trend, the telecom industry needs to think about which kinds of network architecture could be leveraged to support many different types of industry cases with heterogeneous devices; how to effectively support inventory modernization; innovation that can greatly reduce the Total Cost of Ownership (TCO), etc.

1.2 Motivation

This white paper intends to provide an overview to deploy 5G industry campus network, which is also known as Non-Public Network (NPN) by 3GPP definition. This is one of the key 5G concepts to support 2B business. This work will tackle the standardization as well as non-standardization aspects of NPN especially from the MNO perspective, for example, standardization readiness, key factors that may influence the end to end solution, deployment options, case study, etc.

To better support the industry market with mobile network technologies which is future-prove, we need to understand the limitation and challenges of the current technology scope and bring such lessons learned to 5G and its future evolution. Hence, such future work recommendation will also be provided as well.

1.3 Abbreviations

Term	Description
5G-ACIA	5G Alliance for Connected Industries and Automation
API	Application Programming Interface
AR	Augmented Reality
B2C/2C	Business to Consumer
B2B/2B	Business to Business
CAPEX	Capital Expenditures
CAG	Closed Access Group
CN	Core Network
CPE	Customer-Premises Equipment
DDoS	Distributed Denial of Service
DNN	Data Network Name
EC	Edge Computing
eMBB	Enhanced Mobile Broadband
EUICC	Embedded Universal Integrated Circuit Card ID
GDPR	General Data Protection Regulation
GST	Generic Network Slice Template
IACS	Integrated Access and Control System
ICC	Integrated Circuit Card
IMSI	International Mobile Subscriber Identity
IoT	Internet of Things
MBB	Mobile Broad Band
MCC	Mobile Country Code
mMTC	Massive Machine Type Communications
MNC	Mobile Network Code (MNC)
MNO	Mobile Network Operator
MR	Mixed Reality
MSIN	Mobile Subscriber Identification Number
NaaS	Network as a Service
NBIoT	Narrow Band IoT
NID	Network ID
NPN	Non-Public Networks

Term	Description
NSI	Network Slice Instances
NSSI	Network Slice Subnet Instances
O&M	Operation and Management
OPEX	Operating Expenses
OSM	Open Source MANO
OT	Operational Technology
PKI	Public Key Infrastructure
PLMN	Public Land Mobile Network
PNI-NPN	Public network integrated NPN
QoS	Quality of Service
RAN	Radio Access Network
RIC	RAN Intelligent Controller
SLA	Service Level Agreements
SME	Small- and Medium-sized Enterprises
SNPN	Standalone NPN
S-NSSAI	Single Network Slice Selection Assistance Information
SUPI	Subscriber identifier
TCO	Total Cost of Ownership
TDD	Time Division Duplex
UE	User Equipment
UPF	User Plane Function

1.4 References

Ref	Doc Number	Title
[1]	3GPP TS 22.261 V17.2.0 (2020-3)	Technical Specification Group Services and System Aspects; Service requirements for the 5G system; Stage 1 (Release 17)
[2]	GSMA	GSMA Report on “Network Slicing – Use Case Requirements”, April 2018.
[3]	5G-ACIA White Paper	5G Non-Public Networks for Industrial Scenarios
[4]	3GPP TS 23.501 v16.5.0 (2020-07)	System Architecture for the 5GS system; Stage 2 (release 16)
[5]	3GPP TR 28.807 v1.2.0 (2020-06)	Study on management aspects of non-public networks; (Release 16)
[6]	3GPP TS 28.530 v16.2.0 (2020-07)	Management and Orchestration; Concepts; Stage 1; (Release 16)
[7]	3GPP TS 22.104 V17.3.0 (2020-07)	Technical Specification Group Services and System Aspects; Service requirements for cyber-physical control applications in vertical domains; Stage 1 (Release 17)

Ref	Doc Number	Title
[8]	3GPP TS 23.003 V16.3.0 (2020-07)	Technical Specification Group Core Network and Terminals; Numbering, addressing and identification
[9]		GDPR: https://gdpr-info.eu/
[10]	GSMA, NG.116	Generic Network Slice Template v2.0
[11]	GSMA, TS.25	Mobile Network Codes and Names Guidelines and Application Form
[12]	3GPP TR 23.700-07 V0.4.0 (2020-06)	Study on enhanced support of Non-Public Networks (NPN)

2 Lessons Learned

2.1 Vertical Industry Requirements

Vertical industries have a very wide range of use cases with very diverse requirements. From network coverage perspective, some industry use cases require wide area coverage, e.g. healthcare, public services, smart grid, and using public networks to support such use cases is the natural choice. These use cases tend to focus more on the isolation aspect of public network services. In comparison, some industry use cases only require local area coverage, e.g. industry campus network for manufacturing, which has been considered as the important user case for 5G B2B. This will be also the focus of this white paper. Relevant use cases have been well investigated by 3GPP [7], e.g. motion control, control to control in factory automation, which tend to have more challenging requirements in terms of network performance, for instance millisecond level latency, ultra-high reliability, deterministic communication, etc.

Compared to the conventional requirements from 2C services, use cases hosted by industry campus networks have some unique features:

1. **Guaranteed Service Level Agreement (SLA)**: A SLA is a commitment between a service provider and an enterprise or organization in terms of provisioned network services. Network performance attributes like latency, reliability, deterministic communication, etc could be part of technical specification of the SLA. Other than performance requirements (e.g. ultra-low latency, ultra-high reliability), functional and operational requirements could be also specified in a SLA, e.g. high-precision positioning, real-time monitoring, etc. Guaranteed SLA is very essential for 2B use cases, which do not only require ultra-high network performance, but also the guaranteed provisioning of such high performance.
2. **New traffic model**: the uplink and downlink traffic ratio for such use cases is very different from the conventional 2C model, for instance a new uplink-to-downlink frame ratio design may be needed in the solution design.
3. **Strict data isolation**: Industries would like to keep their own data within their premises. Hence, strict data isolation is required, e.g. isolation between carriers' data (if they share the same infrastructure) and communication service data related user plane / control plane / O&M data (which may contain sensitive information of industry as well).

4. **Security & privacy:** Strong privacy and security framework are needed to protect Industry data (e.g. related to production line and corresponding management & operation). Industry data should be only available for industry customers themselves and capable to prevent various potential attacks.
5. **Decoupling between operation and management**: Many small- and medium-sized enterprises (SME) do not have sufficient technical expertise for network deployment and operation. Hence, cooperation with MNOs to obtain 5G services might be the most cost-effective way for such customers to offload the technical complexity. Industry customers may require decoupled network management and network operation. For instance, infrastructure management could rely on network service providers and industry customers may prefer to operate the network service themselves.
6. **Cost efficiency**: Cost effective mobile communication system (including both the infrastructure investment and terminal cost) is one of the essential prerequisites.
7. **Functional efficiency:** Efficient connectivity setup mechanism as well as O&M schemes to avoid inefficient consuming of limited network resource.

2.2 Key Reflections

2.2.1 Solution Prerequisites

In the coming years, the MNOs will undergo a transformation from operating best-effort networks to operating network services that have different service demands from different market segments. As well as streamlining the production of Enhanced Mobile Broadband/Mobile Boradband (eMBB/MBB) services, MNOs will further explore new services. High performance services with added value are envisioned in order to attract industry customers. That in turn calls for networks that are flexible and allow for the provision of new types of connectivity services to meet specific needs from vertical industries with agility and ease.

In 5G, network slicing is considered as the fundamental tool to roll out 2B business models. However, making a successful 2B business story is more than deploying a couple of eMBB or Massive Machine Type Communications (mMTC) slices. It is essential to consider how to provide network services (e.g. in terms of slices) **for local scope (or so-called industry campus scope) with strong performance, functional and operational capabilities**. In this way, MNOs could capitlaise on the opportunities to enter vertical industry markets. Such solution design begins from 5G and will also go beyond of 5G that handles vertical requirements summarized above:

1. **Cost-effective solution:**
   A competitive network service deployment solution needs to result into low TCO for industry customers, and meanwhile, it should be scalable for MNOs (e.g. from supporting handful tier-one enterprises to supporting huge amount of SMEs). It would be a plus if it could help industry customers to further innovate their own business models, meaning, generating new revenue streams. This could be tackled from two aspects:

   a) Optimization:

Being different from public network subscribers, users and applications from industry typically have unique demands on the network services. Generally speaking, specialized requirements may drive up the solution and O&M complexity. In order to support many of such 2B use cases, customized and optimized network solution could be helpful to reduce the cost overhead from communication system compared to the other feasibilities. Networks that inherently optimize the resource usage will allow more traffic with minimized need of investment. This may require new method to establish individual flows or services, as well as new mechanisms to continuously optimize the overall resource usage, avoiding any leakage and fragmentation.

b) Automation and Intelligence:
The bits/m^2 production cost must be optimised. A high degree of automation relaxes the burden from costly and error prone operational processes. Also, artificial intelligence will enable networks to interpret and transform high level strategic intents into explicit configuration of the network infrastructure.

2. **Flexible and sustainable solution:**
In 5G era (and beyond), the system architecture design should allow flexible extension of business scope from the current conventional services and this should be sustainable in term of O&M effort. Provisioning communication services on demand towards vertical industries without letting customers maintaining and/or owning the infrastructure. New services could be easily introduced without coupling with an infrastructure update cycle.
3. **Secured and privacy protected solution**
Data is one of the key assets of vertical industry customers. Secured and privacy protected data transmission over mobile communication system is a key consideration. Isolation methods (e.g. in terms of network resource, data access, etc.) should be used to keep industrial data within the campus as the first step. More factors should be considered in design, for example, how to protect data from various security attacks.
4. **Efficient solution**
During the past decades, the operation of mobile networks has not undergone any radical changes. It follows very much the same principles today as it did for earlier generations, from procurement to service delivery to decommisioning. To allow for the MNOs transformation as described above, networks that require much less attention than those of today are needed. This applies for the deployment phase as well as daily operation to maintain the network, ensure service fulfilment and the required dependability. Essential questions to ask are, how to flexibly operate and manage such huge amount of local industry networks? In particular, each industry network may have its own unique design and requirements. Can automatic deployment be implemented based on the MNOs' public network? Is it possible to manage them all together with the public network? What are the key constraints and how to address these challenges through a good architecture design? Can mobile communication system have a good coordination between the network service provisioning and 2B use cases in order to optimize resource usage and system performance?
5. **System Openness**
Mobile communication system has been always operated as a black box with limited/no capability exposure. This will have a change, when vertical industries will become the main stream customers for 5G, system capability exposure and system openness are

desired. For instance, a manufactory owner could add/remove a 5G capable machine himself/herself, or he/her is capable to monitor 5G system performance in real-time, etc.

2.2.2 AddOn Format

The paradigm shift from 2C to 2B, does not only change the business model, but also impact the overall system architecture design. This is mainly driven by two aspects:

1. Change of service types: Traditional services provisioned by mobile networks are classified by service type, such as voice, data, Narrow band Internet of Things (NB-IoT), etc. 2B service types are usually classified based on industry scenarios, such as Internet of vehicles, smart factory, smart healthcare, etc.
2. Change of service coverage: conventional wide-area coverage mobile communication service is mainly provisioned based on population distribution, for instance, the density of base stations in urban areas is much higher than in suburb areas. In the 5G era, service provisioning is based on economic factors like industry interests at local scope (i.e. industry campus).

Such paradigm shifts should be achieved by innovative system architecture design. Industry campus networks that utilize 5G technology for deployment, are also called private networks, or Non-Public Networks (NPNs) defined by 5G standardization group. From MNO’s perspective, it could be envisioned that deploying industry campus networks just like “AddOn” multiple network service units upon a common public network, meaning, 2B and 2C services share the same infrastructure. Such AddOn format could be a vivid way to describe the fundamental network service unit (especially from the wireless coverage aspect) that an MNO provides to industry customers by utilizing Network as a Service (NaaS) business model. On the other hand, industry campus networks could be constructed and operated by industry players themselves by using standardized technology, but this is out of scope of this document.

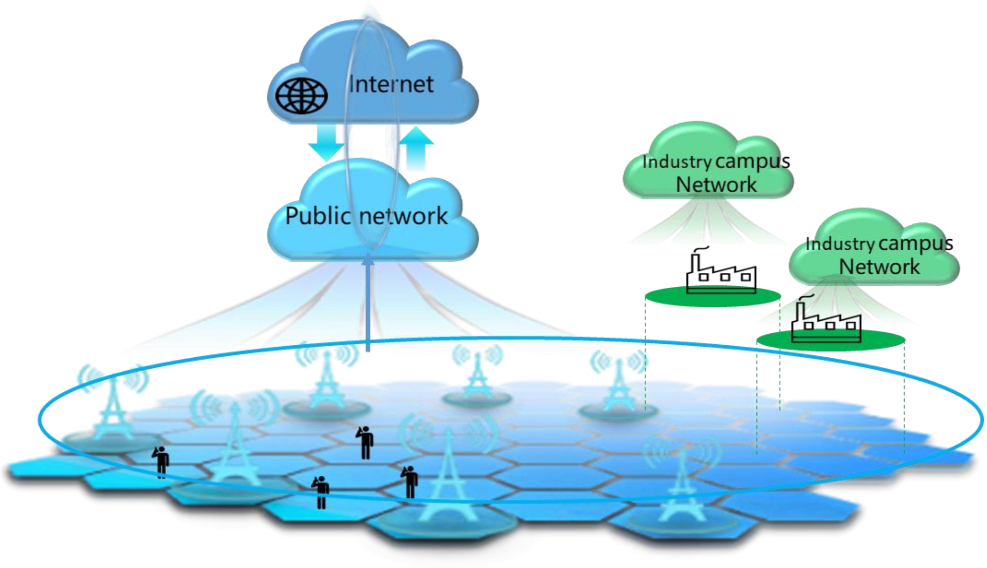

Figure 1 AddOn format to implement B2B type industry campus networks

3GPP has defined the relevant concept and logical architecture to enable NPN, but it is still a distance from the concept of deployment in real life. Such AddOn vision goes beyond standardization in the way that, it is the combination of NaaS business model, network deployment choice and corresponding technologies which is used for MNOs to deploy NPN upon public network for vertical industries. AddOn vision is motivated to take the balance between vertical industry requirements and mobile communication infrastructure cost via a more innovative and inclusive way. The public network deployed for wide-area coverage purpose and potential capability of network automation lay out a good foundation to enable such vision. On this basis, MNOs could add a variety of logical network technologies to support 2B services, while industry customers will have lower Capital expenditures (CAPEX) and operating expenses (OPEX) than building and maintaining private 5G infrastructures by themselves. What's more, a series of system technologies should be considered in order to achieve the industry SLA goals.

The above mentioned solution prerequisites and AddOn vision are derived based on the deep dive of industry use cases and requirements. An end to end solution that could realize such vision may not be achieved in one move. Many open questions still do not have clear answers which need constant technical debates and active contribution to the relevant standardization activities. Section 3 will provide an overview of current standardization status, which could help us to understand what our standing point are.

3 Standardization and Industry Organization Progress

3.1 3GPP Activities

3.1.1 Concepts

NPN is a term defined by 3GPP [1] for a network that is intended for non-public use purpose. It could be exclusively used by a private entity such as an industry enterprise, and could utilize both virtual and physical elements and be deployed in different type of configurations. NPN could exist in two different formats [4] and their corresponding management aspects has been studied in [5]:

- Standalone NPN (SNPN)
  SNPN is operated by an NPN operator and not relying on the network functions provided by a Public Land Mobile Network (PLMN) owned by MNO. An NPN operator could be the enterprise itself or a 3rd party. An NPN operator has full control and management capability on the network functions provided by SNPN.
- Public network integrated NPN (PNI-NPN)
  PNI-NPN is an NPN deployed with the support from a public network. Based on the contract between the MNO and enterprise, the MNO could provide network resources extracted from the public network for the enterprise to use. PNI-NPN could be provided by means of dedicated Data Network Names (DNNs) (assigned for industry customers) or network slicing from a public network (which is further explained in Section 3.1.2).

3GPP defines that Radio Access Network (RAN) could be shared in different access scenarios, for instance, shared by one or multiple SNPNs, and one or multiple PLMNs, etc.

NPN architecture aspects begins from 3GPP Release 16, and a number of enhanced features are further discussed in Release 17 [12], for instance:

- enhancement to enable support for SNPN along with subscription / credentials owned by an entity separate from the SNPN
- support device on boarding and provisioning for NPNs
- enhancement to the 5GS for NPN to support service requirements for production of audio-visual content and services e.g. for service continuity
- support voice/IMS emergency services for SNPN.

3.1.2 Network Slicing

To support the industry use cases with diverse requirements, 3GPP introduces the concept of network slicing, which is defined as a logical network that provides specific network capabilities and network characteristics [4]. To be more specific, from a mobile operator's point of view, a network slice is an independent end-to-end logical network that runs on a shared physical infrastructure, capable of providing an agreed service quality [2]. Network slicing is not only a technical feature of 5G system, but also the key feature that makes Service Level Agreements (SLA) monetizable for vertical industry customers, hence new 2B business model could be introduced.

Network slicing could be used to provide public network services, or NPN services, especially PNI-NPN. Such network slice could contain specific network functions or features for industry customers like device on boarding, secondary authentication, TSN integration, etc. Moreover, certain network capability or Application Programming Interfaces (APIs) offered by the network slice could be exposed to the industry customers as well.

The existing 3GPP network slicing functionalities for management could apply for managing such PNI-NPN following the Network Slice as a Service principle [6].

What should be noticed is that, network slicing is a compulsory feature for 5G, so in theory, a SNPN could also contain one or multiple slices which are not related to PLMN.

In order to have an end to end network slicing, it requires a cross standardization organization effort. For more information about the relevant network slicing industry, please refer to Annex B.

When network slicing is used to deploy NPN, it is important for industry customers to specify which kinds of network services they would like to have. The Generic Network Slice Template (GST) defined by GSMA [10] could be used for this purpose. GST contains a set of attributes that can characterize a type of network slice. Even though the current version of GST may not contain all attributes to support NPN, it is evolving over the time and it could be further extended to address the NPN aspects.

3.1.3 Terminal and Access

In 3GPP context, a User Equipment (UE, also referred as terminal/device) is configured with a Subscriber identifier (SUPI) and credentials for each network it is supposed to connect to. The UE used in the industrial environment could connect to SNPN, PNI-NPN, both, or none.

Depending on the type of access, the required parameter set for a UE could be different as shown in Table 1.

	1-SNPN Standalone	2-SNPN shared RAN	3-PNI-NPN	4-PLMN
SUPI	X	X	X	X
PLMN ID	X	X	X	X
NID	X	X		
CAG			X (Optional)	

Table 1: Parameters to set in UE depending on the network to access

SNPN standalone: The combination of a PLMN ID and Network identifier (NID) identifies an SNPN. Hence, UE is configured with a PLMN ID and NID to access a SNPN. The NID could be self-assigned by individual SNPN or coordinated assigned [8]. The PLMN ID may be a private network ID (e.g. based on mobile country code (MCC) 999 as assigned by ITU[1] for 3GPP), or the ID of a public PLMN that is operating that SNPN.

SNPN with Shared RAN (see further down below for details**)**: The UE is configured with both PLMN ID and NID. The UE can move from SNPN to PLMN connection and vice versa. In that case the UE needs to register with the new network. To connect to SNPN, the UE will listen to the IDs (PLMN ID + NIDs) broadcasted by the NG-RAN.

Note that emergency services are not supported in SNPN. The UE must be connected to the PLMN to use a emergency service.

PNI-NPN: UE must have a subscription for a PLMN in order to access PNI-NPN. Hence, PLMN ID is used to access a specific PNI-NPN. Closed Access Group (CAG) could be optionally used to prevent the UE from trying to access some parts of the network. When PNI-NPN is delivered by the network slicing, a UE may be preconfigured with Single Network Slice Selection Assistance Information (S-NSSAI) to access certain slices.

PLMN: If a UE only uses the public network service, it is not allowed to access to any NPN, because it is only configured with PLMN ID.

3.2 5G-ACIA Activities

5G Alliance for Connected Industries and Automation (5G-ACIA) is an industry forum focused on how to apply 5G technology for Industrial IoT (IIoT), especially in the domain of factory automation and process automation. 5G-ACIA aims to bridge the gap in between ICT and Operational Technology (OT) industries, and apply 5G technology in the best possible way for OT players. Other than identifying relevant use cases and requirements, 5G-ACIA also elaborates integration concepts and possible NPN deployment format in one of their

[1] International Telecommunication Union (ITU), Standardization Bureau (TSB): "Operational Bulletin No. 1156"; http://handle.itu.int/11.1002/pub/810cad63-en (retrieved October 5, 2018).

white papers [3]. It is aligned with the 3GPP definitions, with standalone and in conjunction with PLMN, but they have explored more in terms of deployment details, which contain four deployment options:

(1) Standalone NPN (isolated deployment): the enterprise deploys its own mobile infrastructure and standalone network. It may optionally connect to the public network via a firewall. This equivalent to SNPN defined by 3GPP.

When NPN is deployed in conjunction with public networks, there are three further options.

(2) Shared RAN: In this scenario the public network and the NPN network share one or multiple RAN. NPN may optionally connect to the public network via a firewall. This equivalent to SNPN with RAN sharing defined by 3GPP.

(3) Shared RAN and control plane: In this scenario the NPN network share the RAN and the control plane with the public network. All control plane decisions are being done on the public network. Isolation and routing of the traffic to the NPN is achieved with network slicing or dedicated DNN. NPN may optionally connect to the public network via a firewall.

(4) NPN hosted by the public network: In this scenario the NPN is deployed upon the public network outside of the enterprise premises with isolation being performed by slicing or dedicated DNN mechanism. Optional connection to the public network is not needed in that scenario. Both Option (3) and (4) are equivalent to PNI-NPN defined by 3GPP.

4 NPN Deployment Guideline

3GPP defines the fundamental technologies to enable 5G NPN. However, deploying NPN is an activity that also contains many other non-standardization aspects, for instance, regulatory, and business aspects which need to be considered all together with the technical aspects. This paper intends to lay out the key factors that may influence the NPN deployment choices, and we will discuss this from non-technical and technical perspectives.

4.1 NPN deployment consideration – Non-Technical Aspects

4.1.1 Regulatory Aspect

Each country, where the NPN will be deployed, has its own set of regulations that should be followed. The following areas need to consider:

- **License for operation**
  Operators of private networks may need to obtain a license subject to a general authorization obligation. It will be also essential to consider which license conditions will apply.
- **Spectrum**
  The major regulatory concern for network campuses will be around spectrum availability and the conditions how this scarce resource can be used. While, for unlicensed spectrum, the conditions will be mainly around interference issues; for

licensed spectrum, the obligations are more complex and various criteria can be set by national regulator which could be different across the Member States. All those further depend on to whom the band is assigned, i.e. directly to the MNO or to the vertical. There are some obligations set up by National Regulatory Authorities concerning notification of the start and end of use; frequency transfer and relinquishment; potential rules around revocation if the band has not been used; ElectroMagnetic Field limits, Time Division Duplex (TDD), bands plans etc. For Europe, for example C-band is widely available and the rules around its deployment must be followed[2].

- **Net neutrality**
  In Europe, when deploying network campuses also net neutrality rules have to be considered. Here, the legislation clearly excludes internet access services that are not provided to public, which means those are not subject to the Net neutrality principles (para. 18, NN Guidelines). This means that MNOs will be free to use traffic management necessary for network slicing. It is expected that a new Guidelines on Net neutrality may introduce clearer guidance on its scrutiny for 5G as in some instances network slicing can fall under the provisions of this legislation (when they classify as a specialized service). There is a need to do a case-by-case assessment as there could be instances where internet access is offered to public and this might be subject to those rules.
- **Risk Mitigation**
  The security related measures taken by individual countries will be also be considered in a great extent when deploying such a campus network, e.g. in the EU the 5G toolbox. NPN network services shall comply with Lawful Interception regulations from the countries that apply as well as to comply with the *General Data Protection Regulation* (GDPR) [9] laws.

4.1.2 Business Model

There are variant factors deciding the business model of NPN deployment, among which, the important ones are: infrastructure ownership, O&M parties, and spectrum ownership. Infrastructure ownership refers to the business entity that provides the investment on the CAPEX. O&M parties refers to which business entity will operate and manage the NPN, for instance, if an industry player (e.g. plant owner) builds the NPN by his own, he could still outsource the NPN O&M to the 3rd party like MNO. These factors could be considered as input to design the deployment model. Example business model options are shown in Table 2 by assigning different business roles to operator and industry player.

[2] This band is subject to technical standards set up in *The Commissions implementing decision 2019/235 of 24 January 2019*, which amongst all requires the use of TDD and blocks shall be assigned in multiples of 5MHz.

	Option1	Option2	Option3	Option4	Option5	Option6	Option7
Infra.	Operator	Operator	Industry	Industry	Operator	Industry	Industry
O&M	Operator	Industry	Operator	Industry	Operator	Operator	Industry
Spectrum	Operator	Operator	Operator	Operator	Industry	Industry	Industry

Table 2: Example options of business models

4.1.3 Service Level Agreement (SLA)

SLA defines the agreement in the format of contract in-between the NPN service provider and NPN customer. It defines the technical requirements, business relationship and legally bindings between involved business entities.

4.2 NPN deployment consideration – Technical Aspects

4.2.1 NPN Coverage

NPN coverage is an essential factor that decides which kind of wireless products format should be used in the deployment. It could refer to indoor, outdoor or hybrid coverage type. For instance, many use cases in the factory automation domain requires local indoor and process automation domain requires local outdoor coverage. Such indication may have a strong influence in terms of deployment options.

4.2.2 Inter-connectivity with Public Network

This factor defines the requirements on NPN device connectivity, for instance if an NPN device could utilize public network services whenever it is not in the service area of the NPN. This could be resolved for instance via service continuity provided by a public network [3]. These requirements together with the ownership investment plan will play a major role for deployment model preferences, meaning, having the NPN standalone or conjunction with the public network.

4.2.3 Isolation

Multiple infrastructure formats could be considered in the deployment in order to deliver the isolation premise, for instance dedicated physical infrastructure, dedicated logical network elements with common infrastructure or sharing logical network elements/functions, etc.

4.2.4 Use Cases and Requirements

Based on the use cases that will be hosted by the NPN, a set of technical requirements, which is also called key performance indicators (KPIs), needs to be satisfied by the mobile communication system. This set influences the fundamental deployment factors like capacity planning, etc. An NPN customer should provide such requirements to the network service provider. Investigation on vertical industry use cases has been performed since the beginning of 5G [2]. Some typical IIoT use cases used in NPN scenarios are introduced here:

- **Machine-to-machine Communications**
  A key element of the Industry 4.0 and IoT paradigm is the ability for machines to directly communicate with each other to optimize complex processes. Instead of the traditional client-server model, this creates an interconnected network of robots machines and sensors that collaboratively work to perform their tasks. NPN improved reliability and ultra-low latency becomes essential to making the machine-to-machine communications work.
- **Motion control of both mobile and stationary equipment**
  Motion control is one of the most challenging industrial use cases where the controller sends commands in order to control machines motion in a well-defined way. Very-low latency is important in a use case that usually requires cycle times of less than 1ms (e.g., printing machines, packaging machines). Mobile machines used for goods/materials transport in sites such as shipyards, mines and manufacturing facilities are usually spread across wide geographical areas. At these sites, consistent coverage is essential across all premises. Motion control applications can clearly benefit from the ultra-low latency and reliable ubiquitous wide-area coverage provided by NPN.
- **Augmented and Mixed Reality**
  Augmented and Mixed Reality (AR/MR) is another innovative technology that is gaining more and more importance in industrial sites. AR/MR can be used in tasks such as step-by-step guidance for precise activities (e.g. manual assembly process), end-of-line inspection for highly customized products and remote support from experts (e.g. machine set-up). Industrial sites that plan to use AR for their design, manufacturing and maintenance processes will undeniably profit from NPN's low latency and high data throughput capabilities needed for transmitting video streams.
- **Tracking** of devices and products
  5G broad coverage enables manufactures track real-time locations of devices and items throughout the supply chain. This location information helps increase efficiency and detect and prevent operational risks. Assets tracking such as wagons, pallets and shipping containers may require both an indoor and outdoor coverage availability.
- **Process automation**
  Process automation is the monitoring and control of processes in a plant. Process monitoring usually includes several sensors (e.g., humidity, pressure, temperature sensors) that perform continuous measurements. Actuators (e.g., valves, pumps, heaters) are used to influence the process. Process automation industries (e.g., chemicals, oil and gas, food and beverage) require a deterministic behaviour with a typical latency of around 50-100ms and can be spread over relatively large areas meaning a wide-area coverage is required.

4.2.5 Network Function Deployment Options

Edge computing (EC) is an essential aspect of NPN, which is normally related to the placement of e.g. 5G Core Network (CN), O&M, and industrial APPs. **Error! Reference source not found.** indicates high level deployment options of the core network under the scope of NPN. In deployment option (A), NPN shares the CN with the public network. To increase the service experience, certain CN functions like User Plane Function (UPF) could be deployed at the edge of MNO's premises. In this case, the service isolation could be only achieved at QoS level, but it is possible to have independent operation for the NPN, e.g. NPN customer subscription, resource measurement, monitoring, etc. In deployment option (B), dedicated user plane could be deployed within the scope of industry campus, and NPN shares the control plane with the public network. Independent operation (e.g. lifecycle management of user plane) could be achieved. In deployment option (C), dedicated CN is deployed in the industry campus.

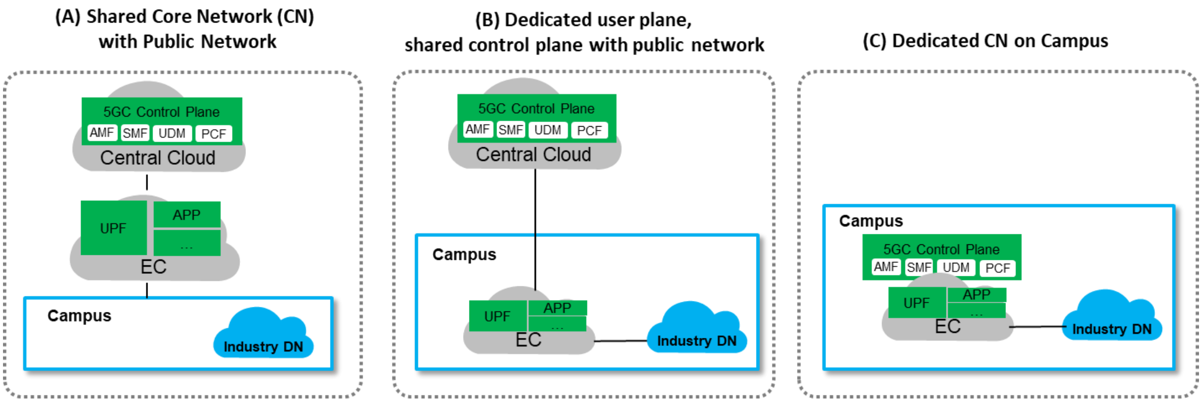

Figure 2: NPN deployment - Core Network Options

4.2.6 Terminals

Terminals need to be properly configured to connect to NPN environments. This could reference 3GPP standards discussed in Section 3, including identification, access control and registration/session management.

4.2.7 Identifiers

A mobile network has many unique identifiers which enable it to interoperate in standard ways with other networks. The NPN itself or the NPN's Service Provider will need to acquire these identifiers or will need to depend on an integrated Public Network to provide these identifiers.

Such identifiers include:

- Issuer Identification Number (IIN) – Governed by ITU-T E.118, and ISO/IEC 7812 are used to identify operating agencies as part of the Integrated Circuit Card ID (ICCID) and Embedded Universal Integrated Circuit Card ID (EUICCID) for SIMs and eSIMs respectively.
- ITU Carrier Code (ICC) – Administered by each country's regulatory authority per ITU-T, M.1400 is used to identify parties in an interconnect.
- Mobile Country Code (MCC) and Mobile Network Code (MNC) – Both are defined by ITU-T E.212 with the MNC being administered by the country's regulatory authority. The MCC-MNC tuple is used to define the PLMN-ID of the network as well as used as part of the International Mobile Subscriber Identity (IMSI) portion of the SUPI, and as part of the GUAMI portion of the GUTI. The MCC-MNC tuple 999 999 is designated for "internal use" and could be used for a NPN that was completely isolated. The ITU administers MNCs within a shared MCC for global usage (presently

901). To mitigate MNC exhaustion, governing bodies responsible for shared spectrum have resorted to subdividing the Mobile Subscriber Identification Number (MSIN) portion of the IMSI to enable more networks to be identified under their purview.

Additional information can be found in [11].

4.2.8 Security & Privacy

Strong privacy and security are important for industrial deployment scenarios to ensure data confidentiality and data integrity, including authentication and access authorization, as well as dependability and trustworthiness. For different branches and industries, since they have different regulatory, business models, and deployment scenarios, security and privacy policies differ. For example, data privacy can be driven with different deployment scenarios. The degree of privacy is mainly influenced by the degree of isolation (physical as well as logical) of data, control and management. With different security and privacy policy, the following aspects can be considered:

- Data privacy: Data in the NPN and the public network need to be separated (physically or logically) and processed separately, in order to fulfil the security and privacy requirements of both networks. Note that the industry application layer data includes not only the user payload data, but also operational data such as subscriber identities, number of active devices, devices identities etc. Network resource isolation (physical and/or logical) as described in the above sub-section, can be a mean to provide the isolation of user payload data but not necessarily the operational data. Consideration also has to be given to the infrastructure used to transmit and possibly store data in the NPN, and to secure- guarding the privacy of industry customers and other users of the public network, especially with regards to possible visibility into the volume of data traffic in the NPN, and when this traffic is taking place. Last but not least, the data belonging to the industry customers should only be visible by themselves. Even the MNOs the fully or partially provide the network Infrastructure can’t access the data.
- Control and management privacy through isolation: This service aspect relates to the degree of segregation/isolation of the control and management plane functions of both networks for privacy and security reasons. This isolation can be provided through network resource isolation (physical and/or logical) as described in the above sub-section and/or through 3rd party APIs.
- Flexibility in choice of security mechanisms: There is a need for flexibility in terms of selecting and administering security mechanisms. The degree of flexibility depends upon the network type, i.e. public or non-public. Or another criteria for selection of security mechanism relies on various industry use cases, e.g. remote medical network, vehicle network. Since different services require different security mechanisms, it’s very necessary to consider case by case to fulfil those security requirements. With NPNs, attention needs to be given to the use of USIM and/or certificates for device authentication and identification, and for access authorization. As required in IEC 62443, Public Key Infrastructure (PKI) may be used for Integrated Access and Control System (IACS). Thus, dedicated NPN certificates can be administered locally, and may allow greater security customization whereas USIM-based authentication allows devices to also access public networks. The same considerations apply to the selection of algorithms for data confidentiality and

integrity. Additionally, it may be necessary to enable lawful interception, depending on the deployment scenario and country of operation.

- Availability assurance: Industrial operations have little tolerance to the disruption of their production lines or operations due to the unavailability. Wireless is an open communication channel; physical isolation is no longer maintained. Thus, anti Denial of Service DoS attack mechanism needs to be considered, e.g. anti-radio jamming, anti Distribited Denial of Service (DDoS) attack, physical security, etc.
- Global availability of security mechanisms: There may be a need for a globally available single security mechanism to minimize administration, and to aid interoperability. The selected deployment scenario affects how universally security mechanisms can be assumed to be available.

In addition, security assessment of NPN infrastructure deployment, which is to ensure the infrastructure that operates properly. By applying security assessment adequately in the infrastructure, the MNO and NPN enterprise customer could prevent the misuse of the valuable assets in the organization. The security assessment could be included such as authentication, authorization, identification, delegation, encryption and tokenization etc. These measures ensure confidentiality as to guarantee user's privacy, ensure integrity as to guarantee the accuracy of the data and ensure availability of the service.

5 Case Study

The enterprise's industrial networks may be complicated due to the legacy method of traditional production design. Most of the equipment may be under independent control and decentralized management, which are desired to be coordinated and managed in a more efficient way. Moreover, due to the long life cycle, communication capacity tends to be limited due to the insufficient planning at the first stage. With more and more new applications, the requirements on communication capacity are increasing dramatically, however, it is very difficult to upgrade the existing wired industrial communication systems.

5G mobile communication system is introduced to replace the traditional cable-based network (e.g. video monitoring system) which could effectively solve the problem of not sufficient optical fibre and limited bandwidth resources constrains. With 5G NPN technology, industry enterprises could build smart manufacturing demonstration plants, especially for industrial control purposes.

5.1 Network Deployment Strategy

Industry enterprise has the vision to bring 5G networks in the manufacturing process to enable intelligent manufacturing business scenarios. China Unicom and Huawei have formulated the 5G NPN solution based on the usage of edge computing and SA network slicing. By using this method, it is possible to provide industry enterprise with an enterprise private network upon end-to-end slicing. In the 5G NPN network, enterprise users and public users can be physically separated, so as to ensure that the enterprise data cannot leave the campus. Moreover, it also ensures the security to protect the production data via exclusive reserved resources for industrial enterprise (e.g. bandwidth). Network performance-wise, enterprise users could have higher data rate, bigger bandwidth, lower latency and more security and reliable network. For instance, the latency between 5G industrial terminals on campus and enterprise Intranet could be reduced from 20ms to 9ms, meaning, improvement by 55%. At the same time, it also reduces the cost of network construction and the cost of maintenance.

Technical Domain	Deployment consideration
Access Network	The base stations adopt the sharing mode between the NPN and the public networks. The 2B services hosted by NPN and the 2C services in the public networks are connected to the same cell under the same base station, but the 2B services are configured with higher priority QoS.
Backhaul Network	IP RAN equipment was newly built in the office of Zhuhai (city) Unicom for deployment of load-bearing network slices.
Core Network	Edge computing platform hosted UPF is deployed in industrial enterprise campus and the control plane is shared with 5G core deployed at Guangzhou province.

Table 3: Deployment example consideration for different technical domains

In industrial campus, 5G systems are expected to support different types of use cases with very diverse requirements. Traffic flows are routed from industrial terminal, to Customer-Premises Equipment (CPE), industrial campus base station, Zhuhai IP RAN, industrial campus UPF and finally reach industrial applications.

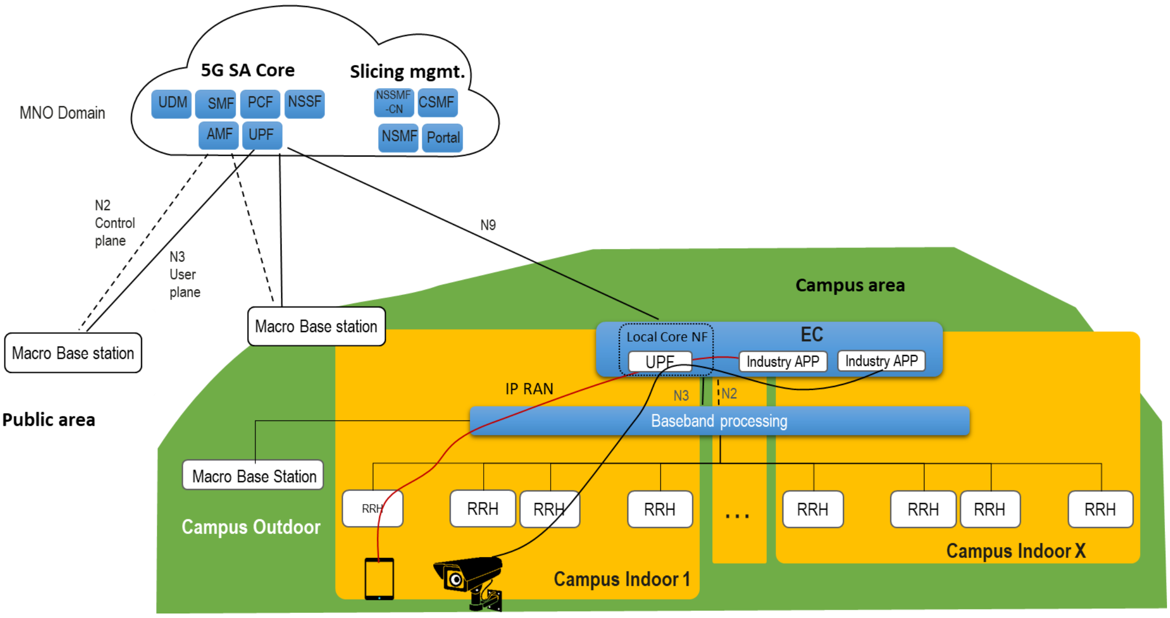

Figure 3: NPN deployment example case

5.2 Use Cases

5.2.1 Paperless initial inspection

The paperless initial inspection system is a system with touchable mobile terminals, which adopts the advantages of 5G networks with low delay and high bandwidth to realize the paperless initial inspection and to obtain the graphic information from the cloud in real time, so as to ensure that the production line personnel can smoothly browse the electronic files in real time. Through the paperless initial inspection project, the efficiency of initial inspection can be improved and the information management of quality traceability can be realized. Such electronic method can replace paper initial inspection and save operational costs.

5.2.2 Video monitoring

Video monitoring is a common practice for commercial production line. By using 5G, for the first time real-time, video streaming of production line is connected to the enterprise Intranet. Sufficient uplink bandwidth resources of 5G network could enable multiple industrial cameras to be used at the same time on shop floor. Real-time monitoring of production line could observe electrical leakage and perform electronic safety inspection, testing, process inspection, operation and other key working procedures. Furthermore, based on the process behaviour recognition by using AI, the quality of production process control could be predicted and further improved. In addition, replacing the traditional wired networks with 5G networks can effectively improve the deployment flexibility of the production line and resolve the problems of insufficient optical fibre deployment, lack of bandwidth resources and construction difficulties in a factory.

6 Conclusion

6.1 Open Issues for NPN

5G is on its commercialization path and aims to extend the MNO's business focus from 2C to 2B. However, 5G standardization work is not finished yet, it is still a way to go, not only from the technical perspective but also from the industry and business development perspective.

This GSMA white paper on one side provides information for relevant telecommunication and industry readers who are interested to deploy NPN based on the state of the art 5G, on another side, it also identifies a number of open issues.

- **Network deployment format**: Industry network deployment format is very different from the nation-wide public networks. It has unique requirements on performance and provisioned network functions. Therefore, a well-designed industrial campus network solution with high flexibility and scalability is envisioned to realize AddOn format of NPN.
- **Network function design**: Core network functions are mainly designed for 2C market. It may worth the effort to think about, which kinds of 2B features need to be reflected on the network function level. For instance, core network manages the connection based on per UE granularity, whereas most industry terminals can be managed based on group granularity as they have same attributes, e.g. Quality of Service (QoS) requirement, session context.
- **Terminal format**: The industry terminal format is not fully clear. It is essential to understand, if the industry needs a 5G module embedded in the industry terminal, or the Customer-Premises Equipment (CPE) format would be sufficient. From the cost effective perspective, it seems beneficial to share the mature terminal ecosystem with the other industries (especially for the low-cost terminals, such as sensors).
- **Solution scalability**: Industry use cases are very diverse. The key of a successful architecture design is how to remain unchanged to cope with ever-changing

situations. The AddOn format of NPN upon public networks enables industry customization to become large-scale in order to support digital transformation of thousands of industries. Large-scale application of 5G is the major determinant of whether 5G can be commercially deployed for 2B as early as possible. Such aspect has not been considered by any relevant bodies. It remains as an open issue how to balance the network resource optimization and deployment flexibility of industry networks.

- **ICT and industry system integration**: 5G does not work as a standalone technology in the vertical premises. It should interact with the existing communication method used in the vertical domain especially when the brownfield system and equipment are considered. Even though 3GPP has been working on the integration of 5G system with some of the existing industrial communication mechanism, however, this is only the first step of the entire integration scope.

6.2 Recommendation for Future Work

The 5G wireless network is oriented to the requirements of industry application scenarios and aims to provide wireless network services for thousands of industries. The foundation lies in the construction of industry-oriented wireless networks, resource allocation, industry-related feature application, and network O&M management. Based on the industry insight results, the traditional 2C wireless public network centred on user/session services cannot effectively cope with the future challenges at the site management. Key considerations from architecture perspectives are as follows:

- Architecture feature:
  Cost-effective and business-wise scalable are the key factors to ensure the commercial success of an architecture design. Hence, such design should have the capability of adding on NPNs upon the public network with high deployment flexibility, and meanwhile, with the possibility of end-to-end resources isolation. Such AddOn format could be the fundamental logical unit to construct NPN. In this way mobile communication systems could be applied to support industry connectivity requirements in an efficient and agile way.
- Guaranteed SLA:
  Industry digitalization will bring new requirements for wireless connectivity, and it is expected that 5G will fulfil this need. Enterprise production sites will need high performance wireless connectivity supporting industrial control applications with end-to-end guaranteed SLA. For instance, if NPN is provided via network slicing method, it is essential to have guaranteed SLA in each technical domain of a network slice, from radio access, transport, to core network. In addition, guaranteed SLA is not simply equal to resource over-provisioning. Resource management and usage efficiency should be considered in the architecture.
- Industry O&M:
  The future architecture should support network autonomous O&M, in which, the O&M scope should be unified for the public network services and the AddOn format of NPNs for the vertical industries, and meanwhile promise customization flavour of O&M based on industry needs. Achieving these may require further consideration on:

  - *Reduced manual network operation:* This will be secured by a network that has advanced and intelligent self-healing capabilities to maximize service resiliency (i.e. maintain delivered connectivity even though the network experiences temporary problem), relaxing pressure on network supervision, and reducing the need for manual and error prone emergency measures.

  - *Easy extension and upgrade:* Increase in both capacity and coverage, as well as feature upgrades must be seamless from on operational perspective and should require minimal manual intervention.
  - *Abstracted management:* The actual strategic goals with the network, like capacity, coverage and features, and produced services must be expressed as intents and policies to the network and processed automatically by the network to become explicit configuration of network resources. This will minimize the error prone manual management processes of today's networks.

  This simplification of operation requires a high degree of autonomy and the employment of artificial intelligence, and in the end it will bring about a network that is much cheaper to maintain, allowing the increased focus on development and delivery of new connectivity services for new market segments.

- System Openness:
  Based on the granularity of NPN, it is desired to provide O&M capabilities to industry customers through open interfaces, in order to perform tasks as fault management, resource management, etc. With such powerful customization and integration capabilities, industry customers can easily integrate mobile communication systems with their own to have an end-to-end solution.
- Security and Privacy:
  For many industries, sufficient industry-grade security and privacy are the most important requirements to apply wireless communication technologies. For example, industry data should not be sent out of the industry campus. Solutions need to ensure the isolation between the industry control, management, user data and MNOs' public networks, hence, the industry data is not visible to any other parties, even the MNOs who fully or partially provide the network infrastructure, apart from industry customers themselves. This can be achieved via security key management mechanisms for instance.
- Seamless Integration:
  5G and its future evolution will be part of the entire industry system. Hence, it needs to meet the industry network service and O&M requirements via NaaS model to achieve seamless integration. Reduced efforts on the system integration could help customers in various industries to leverage the advantage of a wireless communication technology in order to utilize it or even further innovate their own portfolio.

Annex A Relevant Industry fora for Network Slicing

Regarding network deployment, network slicing is one of the ways to realize NPN. There are several industry fora discussing the network slicing from RAN, core network, transport network or O&M perspective. [2] A high level summary of some activities is as follows;

- 3GPP has defined the network slicing to meet the diversified network requirements of the vertical industries and to enable B2B opportunities for telecom operators by switching from dedicated networks deployed by the vertical companies (e.g. electric power company) to network slice provided by telecom operators. The fundamental features of the network slicing have been specified in 3GPP Release 15, mainly in terms of the core network system architecture.
- O-RAN Alliance designs reference architecture of the next generation of RAN infrastructure with intelligence and openness principles. It defines RAN Intelligent Controller (RIC) to control the RAN, which consists of central unit, distributed unit and radio unit. It covers network-slicing-related RIC features and interfaces in order to control the RAN based on policy and monitoring data.
- IETF is a standardization body for internet and IP network and recently discussing overall system for transport network between 3GPP defined user plane functions such as gNB, UPF and DN. The aims of the discussion are how to use existing traffic steering technology along with the 3GPP network slice as well as the management system with northbound interface.
- ONAP provides a comprehensive platform for orchestration and automation of physical and virtual network function. The platform includes 3GPP defined Network Slice Management Function (NSMF) and Communication Service Management Function (CSMF). The 6th release of ONAP, which has been published in June 2020, provides a platform for 5G automation including support of end-to-end 5G service orchestration and network slicing.
- Open Source MANO (OSM) provides a global open source platform for end-to-end orchestration across heterogeneous networks, cloud technologies, and physical and virtual components. Since 2018, this platform is capable of providing Network Slices as a Service, assuming also the role of Slice Manager as per 3GPP TR 28.801 and ETSI NFV EVE012. From a resource viewpoint, OSM provides Network Slice Instances (NSIs) as a concatenation of different Network Slice Subnet Instances (NSSIs), implemented as Network Service Instances that may be exclusive or shared. OSM supports an integrated operation of NSIs along with constituent Network Service Instances, integrating also Day-2 operations from a unified northbound interface. This approach brings the possibility to add custom primitives to a given network slice like the general network service construct enables, and to include non-3GPP related network functions with no need of special integration.
- ETSI ISG ZSM is a standardization group to accelerate the definition of the end-to-end architecture and solutions from orchestration and automation perspectives. It is working to specify solutions and management interfaces for the orchestration and automation of end-to-end network slicing technology as well as to specify the cross-domain service orchestration and automation.

As described above, network slicing is discussed and defined in different industry fora. In order to have end to end network slicing, crossing standards developing organizations SDO effort is are required in order to develop relevant specifications.

Annex B Document Management

B.1 Document History

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
0.1		Formal inputs	NGVT	Marie-Paule Odini (HPE) Stan Wong (PCCW) Xueli An (Huawei)
1.0	10/11/2020	White Paper (NGLT – NG.123) first version	TG	Xueli An <Xueli.An@huawei.com>

B.2 Other Information

Type	Description
Document Owner	NG-NGLT Task Force
Editor / Company	Xueli An <Xueli.An@huawei.com>

It is our intention to provide a quality product for your use. If you find any errors or omissions, please contact us with your comments. You may notify us at prd@gsma.com

Your comments or suggestions & questions are always welcome.