5GACIA

5G Non-Public Networks for Industrial Scenarios

5G Alliance for Connected Industries and Automation

Table of Contents

1 Introduction

This paper describes four industrial (IIoT) deployment scenarios for 3GPP-defined 5G non-public networks. The paper also considers key aspects, in particular service attributes that can help to highlight the differences between these scenarios.

The primary target audience is any organisation considering 5G deployment for IIoT. At the very least, these include operational technology (OT) companies – in other words, those user organisations that will need to apply 5G technologies to their own real-world requirements – and ICT companies, who are considering IIoT as part of their 5G offering.

Some of the terminology and notation employed by 3GPP has been modified to make it more easily understood.

2 3GPP

The 3rd Generation Partnership Project (3GPP) is a collaborative project that brings together standardisation organisations from around the world to create globally acceptable specifications for mobile networks.

As its name implies, it was first created to establish such specifications for the third generation (3G) of mobile systems. It has continued its work for subsequent generations, including the one considered here, the fifth generation (5G).

This paper refers to technical specifications (TSs) published by 3GPP, i.e. the 5G standards.

3 5G-ACIA

The 5G Alliance for Connected Industries and Automation (5G-ACIA) was established to serve as the central and global forum for addressing, discussing, and evaluating relevant technical, regulatory, and business aspects with respect to 5G for the industrial domain. It reflects the entire ecosystem and all relevant stakeholder groups, ranging from operational industry (OT) players (industrial automation companies, engineering companies, production system manufacturers, end users, etc.), the ICT industry (chip manufacturers, network infrastructure vendors, mobile network operators, etc.), academia and other groups.

The paramount objective of 5G-ACIA is to ensure the best possible applicability of 5G technology and 5G networks for connected industries, particularly the manufacturing and the process industry. 5G-ACIA's mission is to ensure that the interests and needs of the industrial domain are adequately considered in 5G standardisation and regulation. 5G-ACIA will further ensure that ongoing 5G developments are understood by and effectively transferred to the industrial domain.

4   Non-public networks

In contrast to a network that offers mobile network services to the general public, a 5G non-public network (NPN, also sometimes called a private network) provides 5G network services to a clearly defined user organisation or group of organisations. The 5G non-public network is deployed on the organisation's defined premises, such as a campus or a factory.

Non-public networks can be desirable for several reasons:

- High quality-of-service requirements
- High security requirements, met by dedicated security credentials

- Isolation from other networks, as a form of protection against malfunctions in the public mobile network. Also, isolation may be desirable for reasons of performance, security, privacy, and safety
- Accountability. A non-public network makes it easier to identify responsibility for availability, maintenance, and operation

5   Network deployment scenarios

3GPP specifications foresee a variety of NPN deployment scenarios. 5G-ACIA's primary interest is in the use of NPNs in industrial/IIoT scenarios. However, this still comprises a wide range of use cases, with a corresponding variety of network configurations. This section focuses on the main configurations in terms of the structure of their logical architecture components.

At the highest level, NPNs can be divided into two categories:

- NPNs deployed as isolated, standalone networks, and
- NPNs deployed in conjunction with a public network.

The first category comprises a single configuration, while the second comprises three, each differing in terms of the degree of interaction and infrastructure sharing with the public network. For all scenarios, it is assumed that all networks provide all services and capabilities required by the NPN at the defined level, and that corresponding service level agreements are in place between the NPN operator and one or more public network operators.

There are many other factors to be considered when deploying NPNs. These include, for instance, what frequencies are to be used, who owns and operates each network, and what level of trust exists between the NPN operator and the public network operator. In addition, consideration needs to be given to the availability of solution components and economic feasibility, e.g. in terms of total cost of ownership. While these factors are very important, and some of them may be implicitly addressed in the scenarios given, they are beyond the scope of this paper. Spectrum aspects are discussed in 5G-ACIA "5G for Connected Industries and Automation" white paper [1]

5.1 Notation

Table 1 below lists and describes the logical elements used to depict network configurations. These are mapped to the 3GPP-defined architecture in Annex 1.

Table 1: Legend for figures in this document

	Device that can communicate via Radio Network
	Radio Network only accessible to Non-Public Network Devices
	Radio Network in Public Network
	Radio Network accessible to both Public & Non-Public Network Devices
	User Plane Gateway only accessible in Non-Public Network
	User Plane Gateway in Public Network
	Control Plane functions in Non-Public Network
	Control Plane functions in Public Network
	Firewall
	Subscriber database for Non-Public Network subscribers
	Subscriber database for Private Network subscribers
	Subscriber database for both Non-Public and Public Network subscribers
	Services offered via Public Network, such as Voice and MBB
	Services inside the factory site, such as control and automation systems
	Physical perimeter of the factory site, which is the minimum coverage area of the Non-Public Network
	Overlay of the Public Network, covers the whole area
	Path for the payload data traffic, i.e. the User Plane (solid line). Blue = Non-Public NW, Green = Public NW
	Path for the wireless network control signalling i.e. the Control Plane (dashed line). Blue = Non-Public NW, Green = Public NW

Source: 5G-ACIA

5.2 Standalone non-public network (isolated deployment)

In this scenario, the NPN is deployed as an independent, standalone network. As shown in Figure 1, all network functions are located inside the logical perimeter of the defined premises (e.g. factory) and the NPN is separate from the public network.

The only communication path between the NPN and the public network is via a firewall. The firewall is a clearly defined and identifiable demarcation point. The OT company has sole and exclusive responsibility for operating the NPN and for all service attributes up to this point.

The NPN is based on 3GPP-defined technologies and is entirely independent with its own dedicated NPN ID. An optional connection to the public network services via the firewall, as shown in Figure 1, can be employed to enable access to public network services, such as voice, while within NPN coverage.

Alternatively, NPN devices can subscribe directly to the public network to access its services (dual subscription). If desired, the optional connection can be leveraged to access NPN services via the public network.

Furthermore, the NPN operator can conclude roaming agreements with one or more public network operators, and the optional connection also be used for this purpose. Roaming agreements with public networks may entail technical constraints. This will depend on the specific case.

Fig. 1: Deployment as isolated network
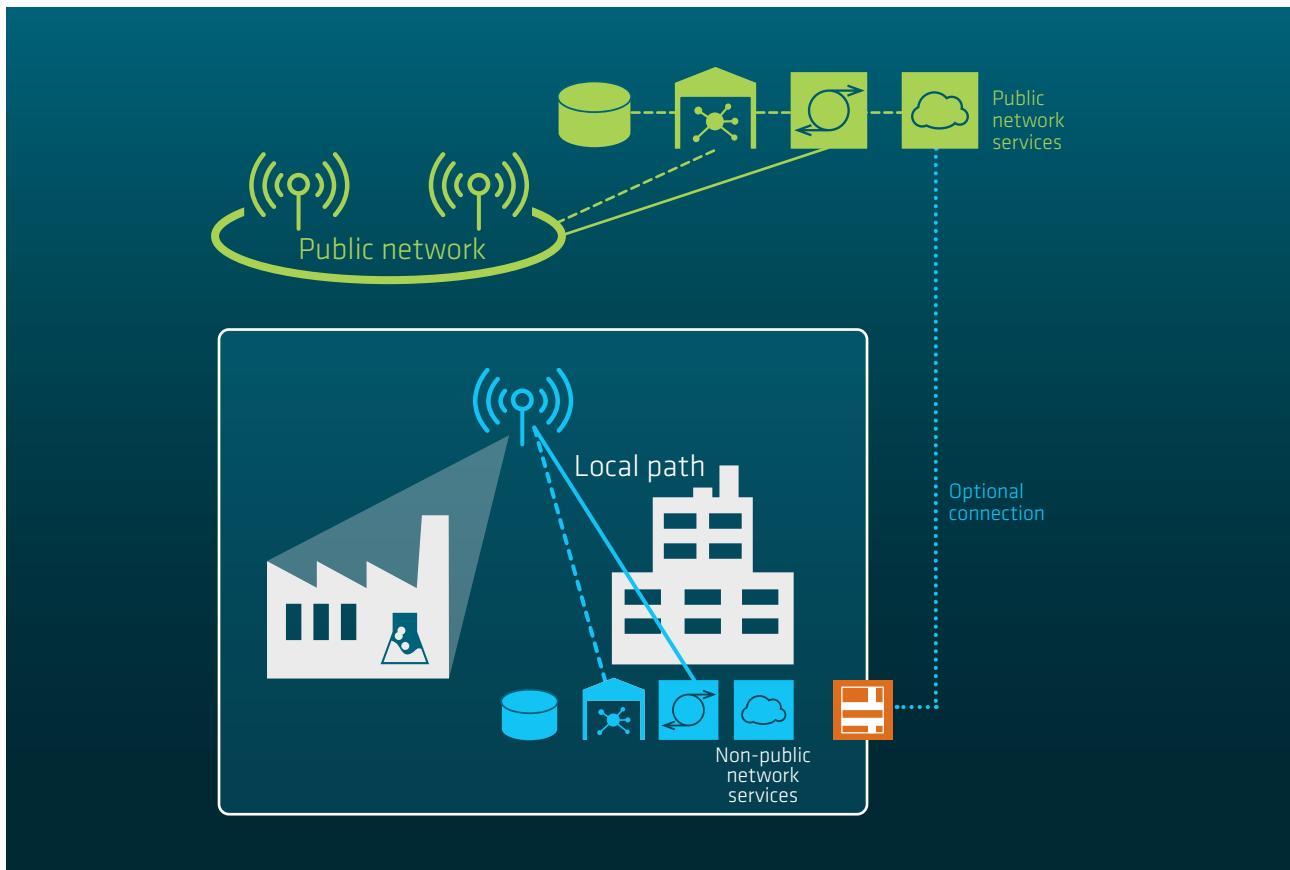
Source: 5G-ACIA

5.3 Non-public network in conjunction with public networks

These deployments are a combination of public and non-public networks. These scenarios assume that certain use cases on the defined premises can be supported entirely by the public network, whereas others require a dedicated NPN.

There are therefore two network parts, one public and one non-public, with traffic assigned to the appropriate part.

5.3.1 Shared radio access network

In these scenarios, the NPN and the public network share part of the radio access network, while other network functions remain segregated. All data flows related to the NPN traffic portion are withi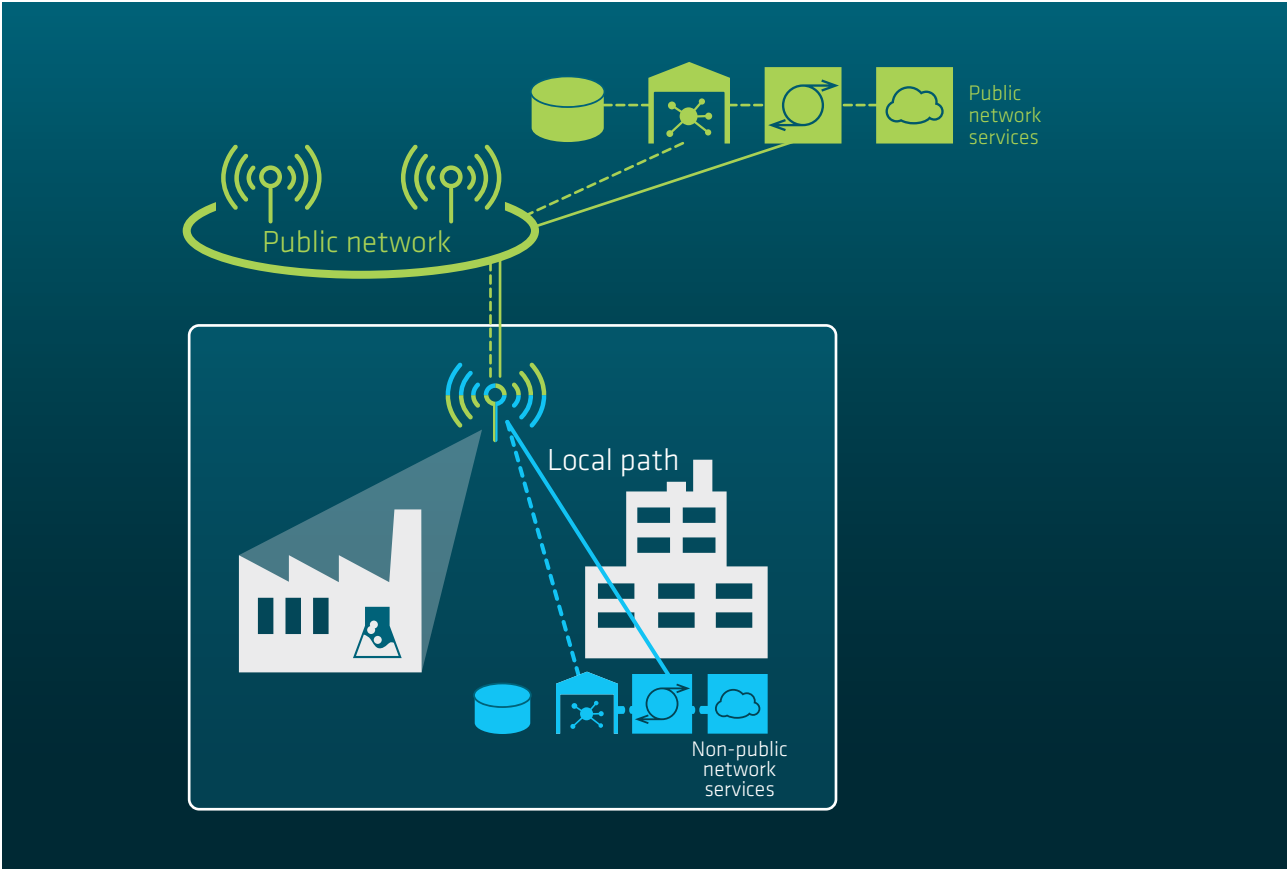n the logical perimeter of the defined premises, e.g. factory, and the public network traffic portion is transferred to the public network. 3GPP specifications include functionality that enables RAN sharing [2].

For the sake of simplicity, Figure 2 only shows a single shared base station for the RAN on the defined premises. It is possible to configure additional base stations that are only accessible to NPN users.

The NPN is based on 3GPP-defined technologies and has its own dedicated NPN ID. However, there is a RAN sharing agreement with a public network operator.

As discussed in section 5.2, it is possible to have an optional connection between the NPN and the public network via a firewall (not shown in Figure 2), and the same considerations as described in section 5.2 apply.

Fig. 2: Deployment with shared RAN

Source: 5G-ACIA

5.3.2 Shared radio access network and control plane

In this scenario, the NPN and the public network share the radio access network for the defined premises, and network control tasks are always performed in the public network. Nevertheless, all NPN traffic flows remain within the logical perimeter of the defined premises, while the public network traffic portion is transferred to the public network.

This can be implemented by means of network slicing, i.e. the creation of logically independent networks within a single, shared physical infrastructure. Segregation of the public and the private networks is achieved by employing different network slice identifiers.

This scenario can also be implemented by means of a 3GPP-defined feature called access point name (APN). The APN denotes the final target network (where to route traffic), allowing differentiation between traffic portions.

Figure 3 shows a single shared base station for the factory RAN but it is also possible to configure additional base stations accessible only to NPN users.

In this scenario, the NPN is hosted by the public network, and NPN devices are public network subscribers. This makes the contractual relationship between the NPN and the public network operator more straightforward. It allows NPN devices to connect directly to the public network and its services, including roaming.

There may also be an optional connection from the private network services to public network services, as shown in Figure 1 in section 5.2. It is possible to harness this optional connection to connect NPN devices to private network services via the public network when the device is outside NPN coverage, but within public network coverage. If public network services are accessed directly via the public network, the optional connection is not needed for this purpose.

**Fig. 3:** Deployment with shared RAN and control plane
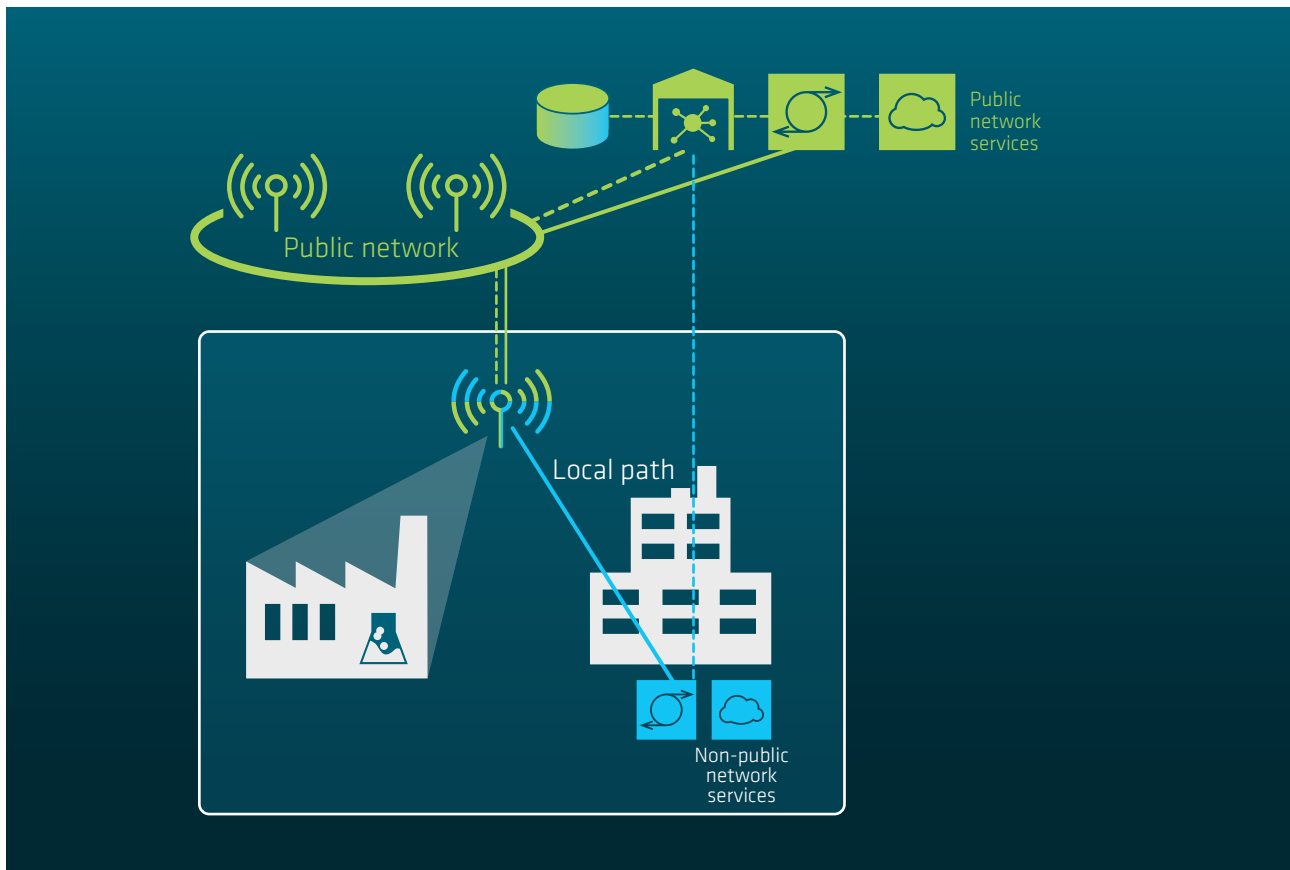
Source: 5G-ACIA

5.3.3 NPN hosted by the public network

In this scenario, both the public network traffic portion and the NPN traffic portion are external to the defined premises, but treated as if they were parts of completely different networks. This is achieved through virtualisation of network functions in a (generic) cloud environment. These functions can then be used for both public and for private network purposes.

This scenario can be implemented by means of network slicing or APN (access point name) functionality. In this scenario NPN subscribers are, by definition, also public network subscribers. Since all data is routed via the public network, access to public network services and the ability to roam can be implemented easily in accordance with the agreement between the NPN and the public network operator. The optional connection depicted in Figure 1 in section 5.2 is not needed in this scenario.

Fig. 4: NPN deployed in public network
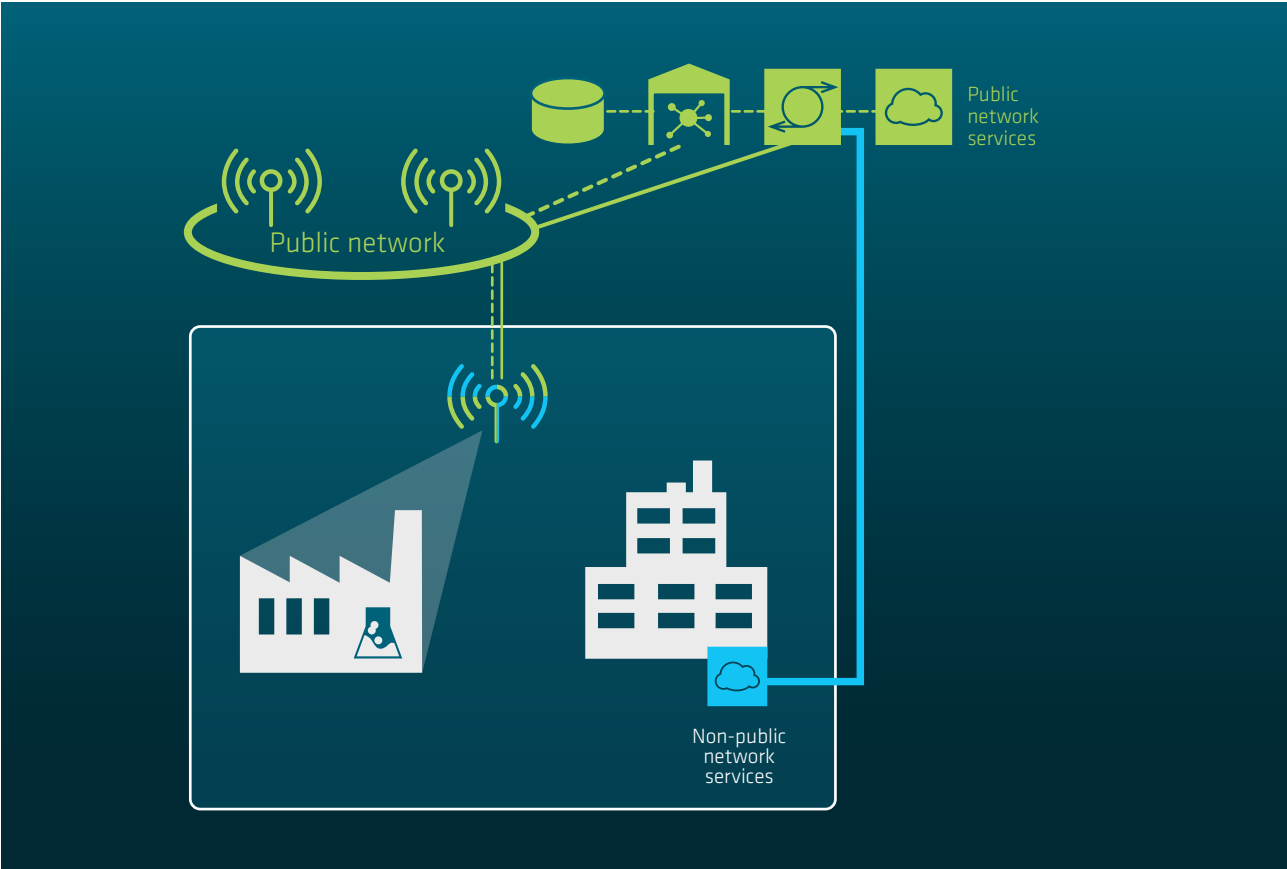
Source: 5G-ACIA

6 Selected 3GPP-defined service attributes

This paper focuses on selected service attributes of 3GPP-defined 5G non-public networks, i.e. those attributes of greatest significance to industrial (IIoT) use cases. The degree of compliance with these attributes should be considered when evaluating the suitability of an NPN deployment scenario for a planned IIoT use case.

6.1 Device connectivity

Device connectivity describes the ability of NPN devices to connect to other networks, such as public networks, to access desired services. This ability is needed in order to make use of services external to the NPN, or to continue the NPN service when devices move out of the NPN, or to remain within the same NPN but to move to another geographic location.

A public network can provide connectivity when a device leaves NPN coverage, i.e. it extends the NPN to other geographical locations. The public network can also be used to access public network services while remaining connected to the NPN.

Whether or not an NPN is implemented as part of or as an extension to a public network, or if an NPN has the capability to interact with public networks can have an impact on:

• Global connectivity, i.e. an NPN device can utilize public network services whenever it is not in the service area of the NPN. It is inherently available in scenarios based on public network subscription, whereas it otherwise requires a secondary public network subscription. NPN devices need to be configured to automatically select the correct network considering whether only NPN selection, or in addition public network selection applies. In all cases, 3GPP-defined network selection processes apply.
• Service continuity, i.e. the ability of the NPN and the public network to act together to provide seamless service continuity, such as non-interrupted streaming video, when a device moves between the NPN and public network.

6.2 Quality of Service (QoS)

QoS requirements vary according to the deployment scenario (see ref [3] and [1] for more detailed definitions):

• Latency (maximum permissible end-to-end latency, i.e. from the device to the data network interface), ranging from highly stringent values (e.g. 1 ms or below) to modest values (e.g. 100 ms). This is the maximum end-to-end latency permissible for the 5G system to deliver the service where latency is completely attributable to the 5G system.
• Availability (the availability of a service that satisfies the defined QoS as a percentage of time), ranging from stringent values (e.g. 99.999999%) to modest values (e.g. 99.9%). The communication service is considered unavailable if it does not meet the applicable QoS requirements (for instance, the system is considered unavailable if an anticipated message is not received within a specified time).

In many deployment scenarios, the NPN and the public network will use the same infrastructure and resources. Due to this sharing, traffic in one network may impact the traffic in the other network unless proper traffic isolation is provided through isolation of network resources. It is therefore necessary to consider the following two possible forms of isolation to achieve the above mentioned QoS requirements:

1. Logical network resource isolation means that the NPN and the public network functions, although sharing a common physical network infrastructure, cannot communicate with each other. This can be achieved thanks to efficient resource allocation mechanisms (e.g. through network slicing).
2. Physical network resource isolation indicates that the network resources for the NPN and for the public network are physically segregated from each other.

Since the QoS in both networks are influenced by the degree of traffic isolation as described above, the different deployment scenarios are evaluated from an isolation point of view.

6.3 Operation and Management (O&M)

The specific NPN deployment scenario can impact how OTs can operate and manage the NPN, i.e. whether and how they can statically or dynamically create, configure, scale and operate network functions, and the ability to capture important network and service information. This might be needed e.g. to meet the specific needs of an automated factory process. Operation and management (O&M) functions to be addressed include:

• Access to monitoring data: This refers to the ability of OTs to monitor the NPN in real time. It may include e.g. monitoring the QoS of traffic for critical applications, the communication and connectivity status and general service availability of devices and network equipment, etc. The information captured may be used for observance of agreed QoS, data analytics, safety management, and troubleshooting. Isolated NPN operated by the OT provides direct access to this data. When the NPN and the public network share the same infrastructure, it may be necessary to expose 3rd party Application Programming Interfaces (APIs) in the network to provide access to this information.

• Access to O&M functions: This refers to how much control and freedom the OT has to operate and manage the NPN and its functions, such as the ability to create, delete, configure, monitor and troubleshoot dedicated NPN functions in order to meet the OTs' service needs. OT operating an Isolated NPN is responsible for the O&M and has full control of all functions. Consideration also needs to be given to the simplicity and feasibility of the operation and management functions in real time. Again, when the NPN and the public network share the same infrastructure, it may be necessary to expose APIs in the network to provide access to these functionalities.

6.4 Privacy & Security

Strong privacy and security are important for industrial deployment scenarios to ensure data confidentiality and data integrity, including authentication and access authorisation, as well as dependability and trustworthiness. In this context

privacy means, to decide what information goes where. Security offers the ability to be confident that those decisions are respected. In different branches and industries, security and privacy policies differ. Several policies 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. Therefore, isolation of data, control and management are considered as service aspects to assess the privacy compliance of the different deployment scenarios. Additional consideration is also needed on how the selection of security mechanisms and network deployment scenarios relate.

The chosen deployment scenario impacts the following privacy and security aspects:

• Data privacy through isolation: Data in the NPN and the public network need to be segregated (physically or logically) and processed separately, in order to fulfil the security and privacy requirements of both networks. Note that the OT 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 means 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 safeguarding the privacy of the OT company and other users of the public network, especially with regard to possible visibility into the volume of data traffic in the NPN, and when this traffic is taking place.

• 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. With NPNs, attention needs to be given to the use of USIM and/or certificates for device

authentication and identification, and for access authorisation. Dedicated NPN certificates can be administered locally, and may allow greater security customisation 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.

• 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.

7 Conclusions

This paper describes a number of network implementation options for NPNs based on 3GPP specifications. These range from completely self-contained standalone NPNs (section 5.2) that have no connection to the public network, to NPNs that are hosted entirely by public network operators (section 5.3.3). Between these two extremes, there are a number of other options.

It is important to highlight that all 3GPP-specified services are available in all deployment scenarios presented in this paper, but the service attributes are delivered to varying degrees of compliance in each scenario.

Parties (in most instances, OT companies) interested in implementing or using NPNs should, through careful analysis, identify which use cases are business-critical for them, and what service requirements those use cases have. It is also essential to consider what effort and resources they are willing to invest in implementing and operating an NPN, and to identify the degree of security needed for their mission-critical data in the long term.

Any interested party should address the following questions:

1. What is the maximum round-trip delay my data can tolerate?
2. Is it acceptable for my data to leave my defined premises / my IT environment, i.e. can an external network operator be trusted with my data?
3. Is it acceptable for an external party, i.e. a network operator, to know the number and location of my devices even if my data are kept within my defined premises / my IT environment?
4. Do I need device connectivity within my premises (and immediate surroundings) only, or globally as well, e.g. in road vehicles / trains, in other countries, at my customer's site, etc.?
5. Do I have the financial resources and manpower to build / operate an NPN network on my own, or would buying it in the form of a service be a better option?
6. Can I secure adequate guarantees (SLAs and transparency) to ensure my service requirements are met end-to-end, across all network resources, e.g. radio resources, network nodes, communication links, etc.?

This list is not exhaustive, but answering these questions may help potential user organisations to draw up a shortlist of viable options, and to evaluate the shortlisted options in collaboration with network service providers.

Annex 2 provides a more thorough analysis on the degree of compliance with each service attribute in the deployment scenarios.

8 Keywords and abbreviations

3GPP
The 3rd Generation Partnership Project (international body responsible for defining 5G specifications/standards)

5G-ACIA
5G Alliance for Connected Industries and Automation API Application programming interface (a defined interface between two software systems. In this context between networks for information exchange and control purposes)

APN
Access point name (identifier for the data network, where connection through 5G system is provided)

Control plane
Logically separate area of a 3GPP system, where control functions and interfaces operate. These are used for controlling the service provided to devices, such as connectivity.

ICT
Information and communications technology

IoT
Internet of Things

IIoT
Industrial Internet of Things

IT
Information technology

Management plane
A logically separate area of 3GPP system where O&M functions and interfaces operate

Mobile broadband
Broadband connectivity service provided by a 5G system

Network slicing
Network slicing is a means of providing "a network within a network" for the delivery of specific services, and to achieve varying degrees of segregation between the various service traffic types and the network functions associated with those services.

NPN
Non-public network (a 5G network that is used to provide dedicated services to defined, closed group of devices)

NPN ID
NPN identity (identifier assigned to the NPN)

O&M
Operation and management (a set of 3GPP system functions and interfaces for configuring, managing and operating the 5G system)

OT
Operational technology

Public network
Network employed to provide services for devices used by the general public

QoS
Quality of service

RAN
Radio access network

SLA
Service level agreement

TS
Technical specification (the normative and binding specifications defined and published by 3GPP)

User plane
A logically separate area of a 3GPP system, where functions and interfaces for transferring payload data sent to and from devices operate

USIM
A universal subscriber identity module (an application on a physically secured device that is used to access network services in a secure way)

9 References

[1] 5G for Connected Industries and Automation, White Paper, 5G Alliance for Connected Industries and Automation (5G-ACIA), November 2018

[2] 3GPP TS 23.251 v15.1.0 Network sharing; Architecture and functional description. Latest version available at: http://www.3gpp.org/ftp/specs/archive/23_series/23.251/

[3] 3GPP TS 22.104 v16.0.0, Service requirements for cyber-physical control applications in vertical domains, Stage 1. Latest version available at: http://www.3gpp.org/ ftp/SPecs/archive/22_series/22.104/

[4] 3GPP TS 23.501 v15.4.0. System architecture for the 5G System, Stage 2. Latest version available at: http://www.3gpp.org/ftp/Specs/archive/23_series/23.501/

10 Annex 1 - Mapping of logical network elements to the 3GPP-defined architecture

For the sake of simplicity, the logical network elements shown and described in this paper are an abstraction of the architecture defined in 3GPP TS 23.501 [4]. Figure 5 below shows how these relate to each other. The 3GPP architecture is depicted by turquoise rectangles connected by white lines.

The yellow lines surround multiple 3GPP functions and build a visual link to the corresponding single logical element used in this paper. Please refer to section 5.1 for further explanations of the notation used.

Fig. 5: Mapping to 3GPP system architecture
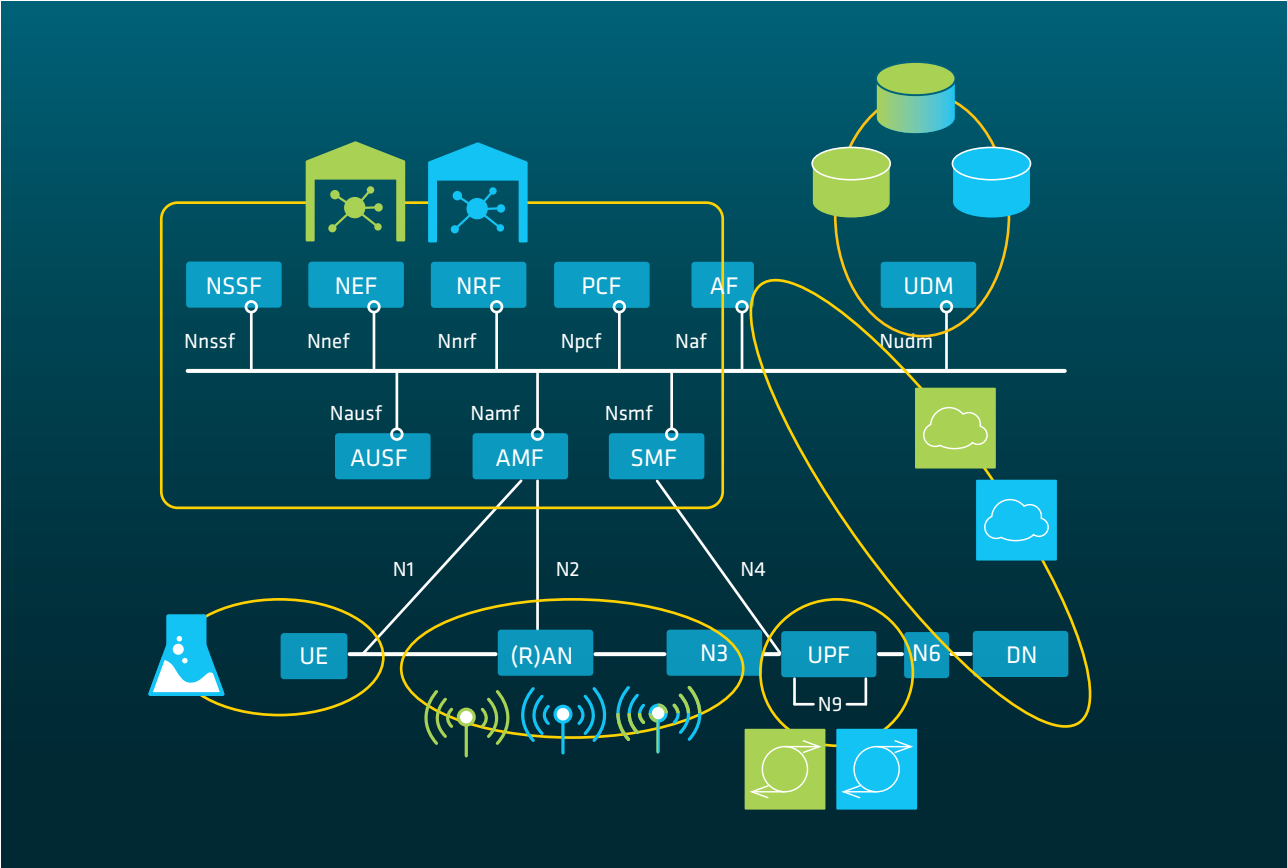
Source: 5G-ACIA

It should be noted that the 3GPP-defined architecture shown here is itself a simplification.

11 Annex 2 - Service attribute degree of compliance in network scenarios

The degree of compliance with the service attributes described in section 6 is given in a table for each scenario. The degree is either "high", "medium" or "low". High compliance indicates that the service in question is fully supported with existing standardized network and device functions without further adaptations. Low compliance indicates that the service is either not supported or only supported with significant adaptations. Such adaptations are e.g. deployment and configuration of multiple NPN IDs and credentials on devices and networks, integration of security gateways to interconnect networks, administration and deployment of non-USIM based security mechanisms, or roaming agreements between two or more parties. Medium compliance indicates that a service is supported under certain conditions or with some adaptations. Clarifying comments are given in the evaluation table explaining the conditions and adaptations needed to reach the respective degree of compliance.

Degree of compliance

		Standalone non-public network	Non-public network in conjunction with public networks		
		Isolated deployment	Shared radio access network	Shared radio access network and control plane	NPN hosted by the public network
Service attribute					
Device connectivity	Global connectivity	Low / high Low when devices can connect to the NPN only, and there is no direct connection to the public network. High when an optional connection to the public network and a public network subscription are in place. This requires additional configuration in NPN devices for automatic network selection.	Low / high Low when devices can connect to the NPN only, and there is no direct connection to the public network. High when an optional connection to the public network and a public network subscription are in place. This requires additional configuration in NPN devices for automatic network selection.	High Public network subscription can be used for global connectivity, e.g. via roaming.	High Public network subscription can be used for global connectivity, i.e. via roaming.
	Service continuity	Low / medium Low when devices can connect to the NPNonly and cannot directly connect to the public network. Medium when optional connection to the public network and a public network subscription are in place. The service must support device mobility.	Low / medium Low when devices can only connect to the NPN and cannot directly connect to the public network. Medium when there is an optional connection to the public network and the device has a public network subscription. The service must support device mobility.	High Because the public network hosts both networks, service continuity can be achieved relatively easily between the NPN and the host public network.	High Because the public network hosts both networks, service continuity can be achieved relatively easily.

QoS	Latency and availability	**High** High because this deployment scenario provides traffic isolation through physical network resource isolation.	**High / medium** High if traffic isolation is provided through logical network resource isolation in the shared RAN (via efficient resource allocation mechanisms). Medium if the resource allocation mechanisms in the shared RAN do not fully take into account the QoS requirements of both networks. Note that in this deployment scenario, the network segments other than RAN provide traffic isolation through physical network resource isolation.	**High / medium** High if traffic isolation is provided through logical network resource isolation in the shared RAN (via efficient resource allocation mechanisms and network slicing), or if a dedicated RAN is used to allow physical isolation and traffic isolation for the user plane traffic. Medium if the resourceallocation mechanismsin the shared RAN do notfully take into account theQoS requirements of bothnetworks. Note that in this deployment scenario, the network segments other than RAN and control plane provide traffic isolation through physical network resource isolation.	**High / medium / low** This deployment scenario provides traffic isolation through logical network resource isolation on all network segments (via end-to-end network slicing). Because NPN data and network functions are external to the defined premises, i.e. factory, this may result in an inevitable degradation in latency (which – among other factors – depends on the distance between the factory and the public network premises). The degree of compliancy for latency depends on the service requirement level. For very stringent latency requirements (e.g. 1ms) it is low. However for moderate to modest latency values (e.g. 10-100ms) it may be considered as medium to high. The degree of compliancy for a very stringent availability requirement may be considered to be low if required in combination with a very stringent latency requirement, and medium to high if required in combination with a moderate to modest latency requirements. For a moderate to modest availability requirement, compliancy may be medium or high, depending on the latency requirement.
Operation and management	Access to monitoring data and O&M functions	**High / medium** High when NPN operator has full access to its monitoring data and O&M functions/tasks, e.g. in the case an isolated NPN is operated by the OT. Medium when the NPN operator has only delayed or limited access to required information and functions, e.g. due to a lack of support from the NPN or lack of adequate remote access.	**High / medium** High when the NPN operator has full access to its monitoring data and O&M functions/tasks. In a shared infrastructure, this can be achieved through 3rd party APIs deployed in the network. Medium when the NPN operator has delayed access to required information and functions, e.g. due to lack of adequate remote access or due to the conditions of the RAN sharing agreement between the NPN operator and the public network operator.	**High / medium** High when the NPN operator has full access to its monitoring data and O&M functions/tasks. In a shared infrastructure, this can be achieved through 3rd party APIs deployed in the public network. Medium when the NPN operator has delayed access to required information and functions, e.g. due to the conditions of the network sharing agreement between the NPN operator and the public network operator.	**High / medium** High when the NPN operator has full access to its monitoring data and O&M functions through 3rd party APIs deployed in the public network. Medium when the NPN operator has delayed access to required information and functions, e.g. due to lack of support because of the way the network has been implemented (lack of 3rd party APIs). Note that with network slicing, the NPN operator may be responsible for some or all network slice management tasks. The choice of network slice management model depends on the bilateral agreement between the operator of the NPN and the operator of the public network.

Privacy & Security					
Data privacy through isolation	**High** Complete physical isolation. The NPN data is physically isolated from the public network data.	**High** High since logical network resource and hence data isolation can be provided in the shared RAN. Note that the data of both networks shares the RAN through a logical isolation but not a physical isolation. Still, it´s difficult to get information on production activities based on data on RAN level without subscription and operational data. Note also that in this deployment scenario, the network segments other than RAN provide physical data isolation.	**Medium** Medium because the NPN's user subscription and operational data (e.g. active assets) are accommodated in the public network core. Note that the data of both networks share the RAN and the control plane through a logical isolation and that the user plane data of both networks are physically isolated.	**Medium** Medium because the subscription data (e.g. profiles of OT active assets) of both networks share the same database accommodated in the public network although RAN and core network are logically isolated.	
Control and management privacy through isolation	**High** Complete physical isolation.	**High** High since logical network resource isolation in the shared RAN enables the possibility of providing a logical isolation of the control and management functions.	**High / medium** High when control and management planes for the NPN (resp. for the PLMN) are exclusively deployed and used for the NPN (resp. by the PLMN). This can typically be achieved through 3rd party Application Programming Interfaces (APIs) deployed in the public network. Medium if control and management functions are performed by a single operator for both networks. Most naturally, this would be the public network operator.	**High / medium / low** Degree of compliance depends on the way the public network is implemented, especially the segregation of network functions for the NPN and the public network as well as the setting up of 3rd party APIs deployed in the public network. For network slicing, the choice of slice management model depends on the bilateral agreement between the operator of the NPN and the operator of the public network.	
Flexibility in choice of security mechanisms	**High / low** High when accessing only the NPN since either USIM or non-USIM-based methods can be employed. Low when devices utilise also the public network services since a mandatory authentication method (USIM-based) is employed for each device. It may also be necessary to allow lawful interception, depending on the regulatory imperatives for the specific deployment scenario.	**Low** Low when devices only access the NPN or also utilise public network services since, due to the shared RAN, a mandatory authentication method (USIM-based) needs to be deployed for each device. It may also be necessary to enable lawful interception, depending on regulatory imperatives for the specific deployment scenario.	**Low** Low because USIM-based credentials are always required when devices connect to the public network and/or to the NPN. It may also be necessary to enable lawful interception, depending on regulatory imperatives for the specific deployment scenario. Note that NPN's user subscription data (e.g. active assets) are accommodated in the public network core.	**Low** Low because USIM-based credentials are always required when devices connect to the NPN and/or to the public network. It may also be necessary to enable lawful interception, depending on regulatory imperatives for the specific deployment scenario.	
Global availability of security mechanisms	**Medium / high** Medium when accessing only the NPN since the NPN operator can select customized security mechanisms, but these may only be available locally. High when using public network security mechanisms that need to be used for accessing public networks, which are globally available.	**High** Public network security features are available globally.	**High** Public network security features are globally available.	**High** Public network security features are globally available.	

11 5G-ACIA Members

As of September 2021

KETI

KEYSIGHT TECHNOLOGIES

Lenovo

LS telcom

MAVENIR

MC TECHNOLOGIES

Microsoft

MITSUBISHI ELECTRIC

MOXA

MUGLER TELCO NETWORKS.

Nitto

NOKIA

NXP

orange

Panasonic

PEPPERL+FUCHS

PHŒNIX CONTACT

Qualcomm

Radisys

RELIABLE REAL-TIME RADIO

ROHDE & SCHWARZ

SAL SILICON AUSTRIA LABS

salzburg research

Schneider Electric

SICK

SIEMENS

SINTEF

SoftBank

SONY

ST life.augmented

TRUMPF

TZi

u-blox

UPLINK

verizon

VIAVI VIAVI Solutions

vodafone

VOLKSWAGEN AKTIENGESELLSCHAFT

WAGO

Weidmüller

XITASO

YOKOGAWA

ZTE

www.5g-acia.org