5G-ACIA White Paper

NPNs for Industrial Scenarios

5G Alliance for Connected Industries and Automation

Table of Contents

1 Executive Summary

In the industrial context, 5G is mainly used in so-called non-public networks (also called private networks), which have already been implemented worldwide. Continuing the work begun by 5G-ACIA when it published the first white paper on this subject [1], this paper looks more closely at some examples of actual NPN deployments for use cases in industrial scenarios. It begins by describing a small but representative set of industrial scenarios based on input received from OT companies, as the basis for presenting NPN deployment examples. This set is not exhaustive; many other use cases and combinations of them are also valid and possible. The example NPN deployments are based on 3GPP standards and include options contributed by ICT companies. Finally, the available alternatives are analyzed and an overview of aspects that could affect the choice of NPN deployment options for each scenario is provided.

Here are some of the key findings of this study in summarized form:

- At least for the example operations and use cases described in this paper, the best approach is to deploy a NPN locally on the premises of an industrial operation (on both the user plane and the control plane). This is the best way to meet the prerequisites for complying with the associated demanding QoS and privacy requirements.

- The use cases discussed here don't require any communication beyond the industrial site itself. This would only be needed if some of the 5G network's functionality (on the user plane and/or control plane) were performed elsewhere. This would be the case if, for example, an NPN were only partly deployed on-premises. All of the presented NPN deployment examples are capable of supporting this, and connections to external networks can be optionally added as required for communicating with other sites or accessing cloud services. If this is done, it is of course necessary to address related security and privacy concerns.

- The performance requirements of the presented example use cases can be met with either an SNPN or a PNI-NPN. However, it's essential for them to be deployed as on-premises NPNs as shown here. Both SNPNs and PNI-NPNs are logical architectures defined by 3GPP. An SNPN doesn't rely on a PLMN, but a PNI-NPN does.

- An OT enterprise using an NPN must have appropriate access for operating and managing it in accordance with the industrial operation's requirements. For example, it must be possible for the OT enterprise to add and remove UEs and configure both them and the 5G network supporting the industrial network. SNPN- and PNI-NPN-based solutions differ from one another in terms of how the OT enterprise accesses and manages the NPN, and these requirements therefore need to be taken into account in addition to the communication requirements of the use cases. Whenever managing a network requires access to external networks, it's also essential to address security and privacy concerns.

- Whether or not there is access to appropriate spectrum resources affects decisions on how the NPN is deployed. SNPNs can be used with a dedicated spectrum, which can be available as local spectrum assigned to industry, as a national MNO's spectrum in the case of leasing arrangements, or as part of an MNO SNPN offering. PNI-NPNs typically use a MNO's spectrum.

- Both SNPN and PNI-NPN deployments can take the form of network-as-a-service (NaaS) models (which can require a remote management connection). SNPNs can also be acquired as a wholly owned and operated set of equipment (with all management being performed on site by the OT enterprise, in other words without requiring any communication for external management).

About 5G-ACIA

The **5G Alliance for Connected Industries and Automation** (5G-ACIA) was established to serve as the main global forum for addressing, discussing, and evaluating relevant technical, regulatory, and business aspects of 5G for the industrial domain. It embraces the entire ecosystem and all relevant stakeholders, which include but aren't limited to the operational technology industry (industrial automation companies, engineering companies, production system manufacturers, end users, etc.), the information and communication technology industry (chip manufacturers, network infrastructure vendors, mobile network operators, etc.), universities, government agencies, research facilities, and industry associations. 5G-ACIA's overarching goal is to promote the best possible use of industrial 5G while maximizing the usefulness of 5G technology and 5G networks in the industrial domain. This includes ensuring that ongoing 5G standardization and regulatory activities adequately consider relevant interests and requirements and that new developments in 5G are effectively communicated to and understood by manufacturers.

2 Introduction

Non-public networks (NPNs), also known as private networks, are the primary way in which 5G technology is deployed in the industrial automation domain. Since 5G-ACIA published its first white paper on 5G NPNs for industrial scenarios [1] in 2019, the scenarios presented in it have been widely referenced in related documents. All of them address two NPN types corresponding to the 3GPP definitions, namely standalone NPN and public network integrated NPN (PNI-NPN), as well as some other standardized features including RAN (radio access network) sharing. The original document also analyzed their defining features.

Since publication of the original white paper, 5G products have become widely available and industrial 5G deployments have become a reality. While the descriptions and analyses of the original white paper are still valid, we now know more about how 5G is most likely to actually be used in the industrial domain. This document continues 5G-ACIA's work on this topic and discusses NPN deployments while taking a different approach in an attempt to provide a more detailed description of how 5G NPNs can and are used in industrial use cases. It begins by describing a landscape containing several example industrial operations for which industrial 5G networks are deployed. The chosen scenarios are a manufacturing building, a large-scale process industry plant, and an industrial park (chapter 3). Some example 5G NPN deployments for these examples are then sketched based on the use cases and industrial network topologies (chapter 4). Finally, aspects that can affect the choice of NPN (chapter 5) are described. For reference, the latest additions to the 3GPP standards relevant to NPNs (section 8.1) are also summarized.

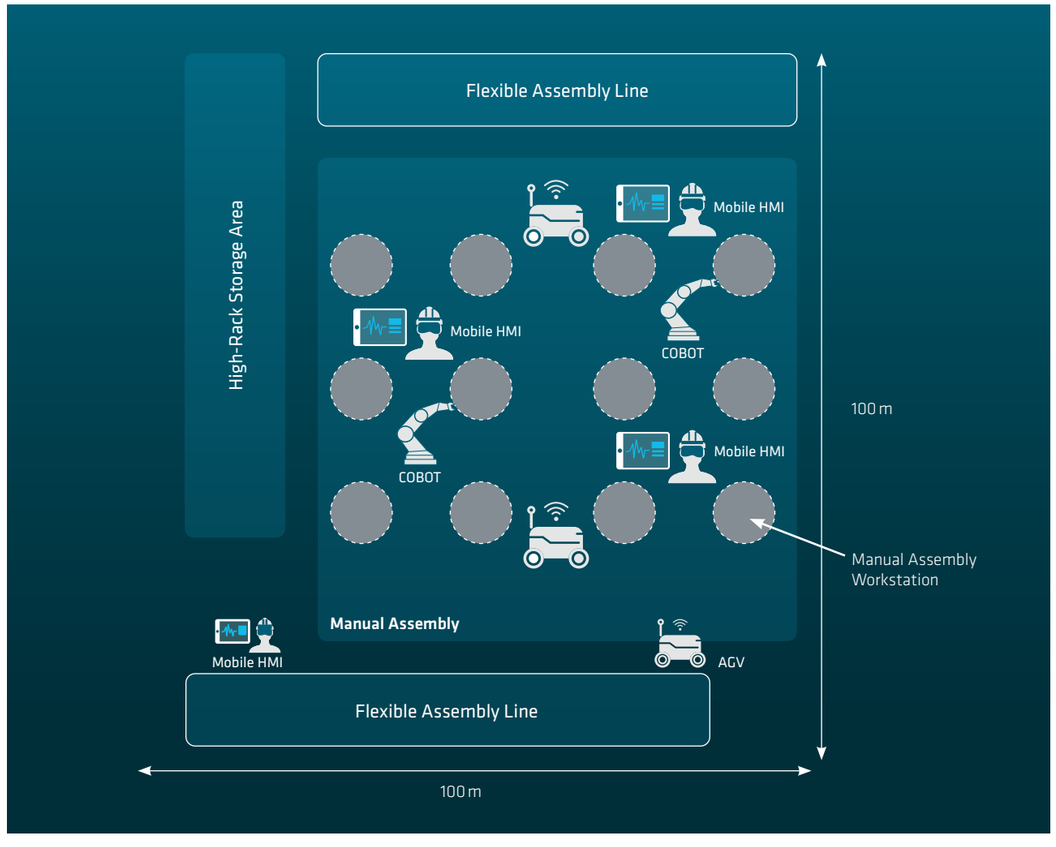
3 Examples of Industrial Operation Scenarios

3.1 Manufacturing Facility

This scenario involves a plant with a production system comprising mechanical, electrical, and electronic components. Typical examples are mechanical and electrical drives and peripheral devices. The possible applications range from processes involving a large amount of manual work all the way to fully automated, flexible assembly lines.

Figure 1 shows a manufacturing facility layout, indicating different production areas and their relative locations.

Figure 1: Shopfloor layout in a manufacturing facility



Source: 5G-ACIA / ZVEI e. V.

3.1.1 Use Case Description

Several production operations can take place concurrently in the manufacturing facility's areas, as shown in Figure 1. The processes shown in this example range from operations that involve a considerable share of manual work all the way to fully automated, flexible assembly lines.

Flexible Assembly Lines: This section of the shopfloor contains two highly flexible assembly lines, each of which contains a modular process for assembling predominantly mechanical automation components such as pneumatic valves (shown at the top and bottom of Figure 1). A total of eight interconnected production cells within an area measuring 30 x 3 meters operate in sequence (no details shown). Each cell performs part of the overall production process and is typically equipped with a dedicated controller. Since parts of these lines could be reconfigured as described below, it is useful if communication takes place from controller to controller or controller to edge server, unlike in a monolithic PLC that can't be broken down into modules for reconfiguration (see also section 3.1.3, which shows the industrial network configuration).

Automated guided vehicles (AGVs) are needed to safely perform logistical tasks within the factory infrastructure while traveling along predefined routes between production cells. They don't include any additional control functionality. The collaborative robot (COBOT), which integrates more autonomous functionality and interacts with mobile workers, moves components into production entities.

Manual assembly: Material flows are controlled by an edge-server-based manufacturing execution system. The requirements of this use case are comparable with those of the process industry scenario shown in section 3.2. Latency is less critical when AGVs are moving slowly.

Wireless sensors are needed, for example, to monitor the states of process and environmental parameters. They can be connected in three different configurations:

a. Connection to a local controller on the shop floor for providing aggregated information to higher levels of the information hierarchy, for example to free cloud-based applications from having to interpret process data.
b. Connection to edge-server-based applications for use cases such as monitoring and optimizing energy consumption via a connection to an edge server without local data processing in the devices on the shop floor.
c. Connection to remote applications via the public network. Here the use case involves remote predictive maintenance by the equipment manufacturer as allowed by the plant owner.

Manual work is still required for assembling mechanical or electronic components. Two example use cases that can benefit from adding an NPN and the wireless connectivity it provides are:

- **Mobile worker HMI:** Use of smart glasses to support virtual and/or augmented reality in combination with other connected wearable devices. Additional applications can also be involved to support human workers with additional information. Most of the payload consists of videos or additional documentation related to the ongoing task.

- **COBOTs** support and interact with human workers. These special robots enable a safety configuration in which protective barriers can be dispensed with. The assumption is that each COBOT is equipped with a local controller for handling time-critical control tasks.

3.1.2 Industrial Network for Manufacturing Facility

Figure 2 shows an example logical layout for the industrial network in the manufacturing facility.

With larger plants or more buildings, it is necessary to add more OT domains. This is relevant when different business units of a plant operator share a campus.

3.2 Large-Scale Process Industry Scenario

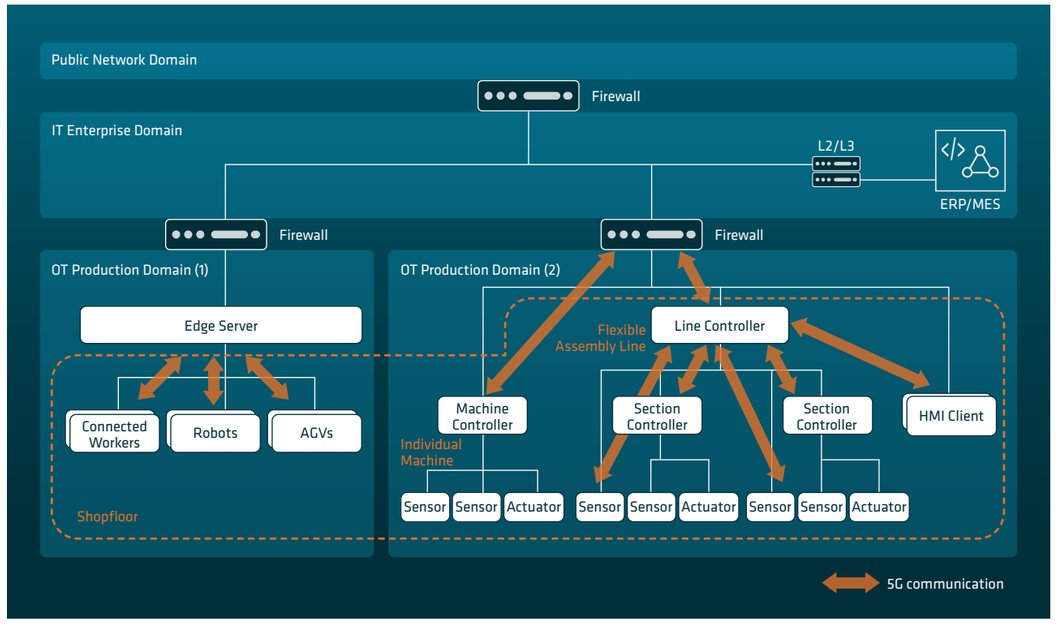
This scenario describes potential 5G applications in a process manufacturing plant with a large outdoor production area, such as an oil refinery or chemical plant. To enable smart operating solutions, 5G could be deployed as a communication infrastructure covering the entire production area.

Figure 3 illustrates an example layout for a midsized oil refinery in the presented scenario. Oil refineries can vary greatly in size, occupying up to tens of square kilometers.

3.2.1 Use Case Description

- **Connected workers:** Wearable devices connected to 5G (such as head-mounted displays) provide digital support to human field workers to enable them to work more efficiently. The workers can potentially perform tasks anywhere within the plant, also in its storage and refining areas. The possible applications include on-demand mobile data access (for example, manuals and information on assets), live video communication between workers at different locations and/or between them and a remotely located expert, overlaying of instructions or other information on top of real objects using augmented reality (AR) technology and so on. These use cases require high bandwidth and a sufficiently low latency to enable real-time communication between humans. Rapid positioning of these devices with an accuracy of about one meter would also be desirable to allow prompt localization and evacuation of workers in the event of an emergency.

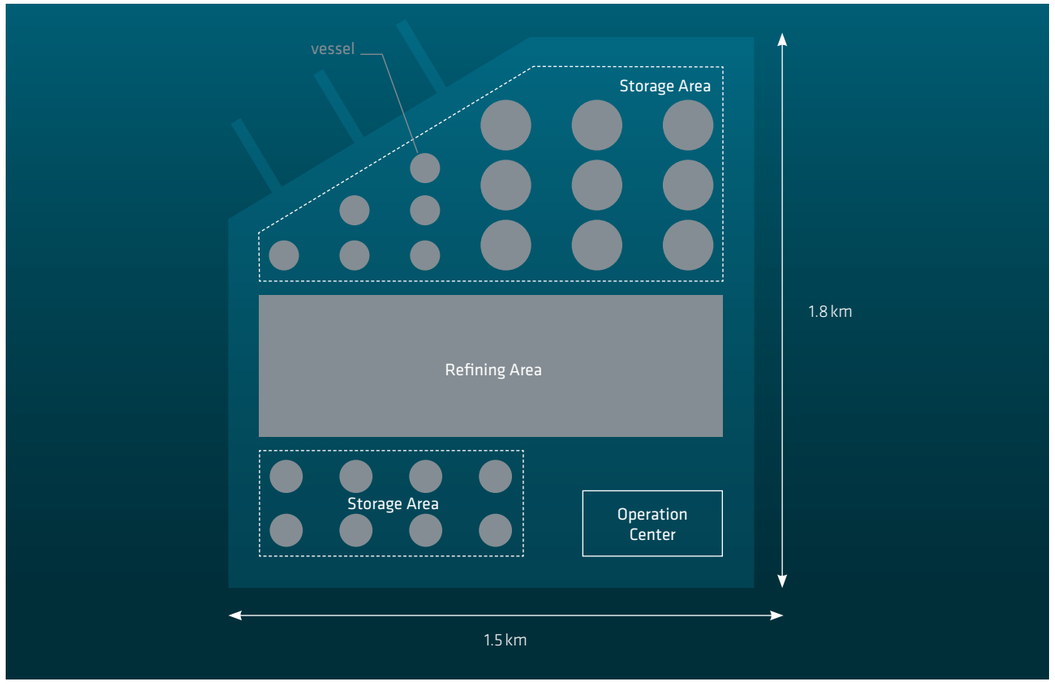
Figure 2: Logical view of an industrial network for a manufacturing building



Source: 5G-ACIA / ZVEI e. V.

- **Mobile HMI:** Field workers may also want to access the monitoring dashboard of a production control system such as a DCS (distributed control system) or SCADA (supervisory control and data acquisition). Highly reliable wireless connectivity is required for re-al-time tracking of the production situation in the field via a mobile terminal. Connection downtimes should not exceed what is needed to update the dashboard, which can typically take between 10 ms and a few seconds depending on the production process.
- **Inspection robots:** Inspection robots are mobile robots (including drones) that roam the entire area of an plant to perform inspection tasks (and/or carry out rescue operations if there is an emergency) instead of human workers. They are equipped with various sensors, including several cameras, a microphone, a gas detector and so on. The 5G network should have sufficient capacity so that the robots can send environmental information captured by their sensors to a remote operations center for real-time analysis. If they deliver accurate information on their locations, this improves the quality of decision-making by AI (artificial intelligence).

Figure 3: Layout of a process industry plant (oil refinery)

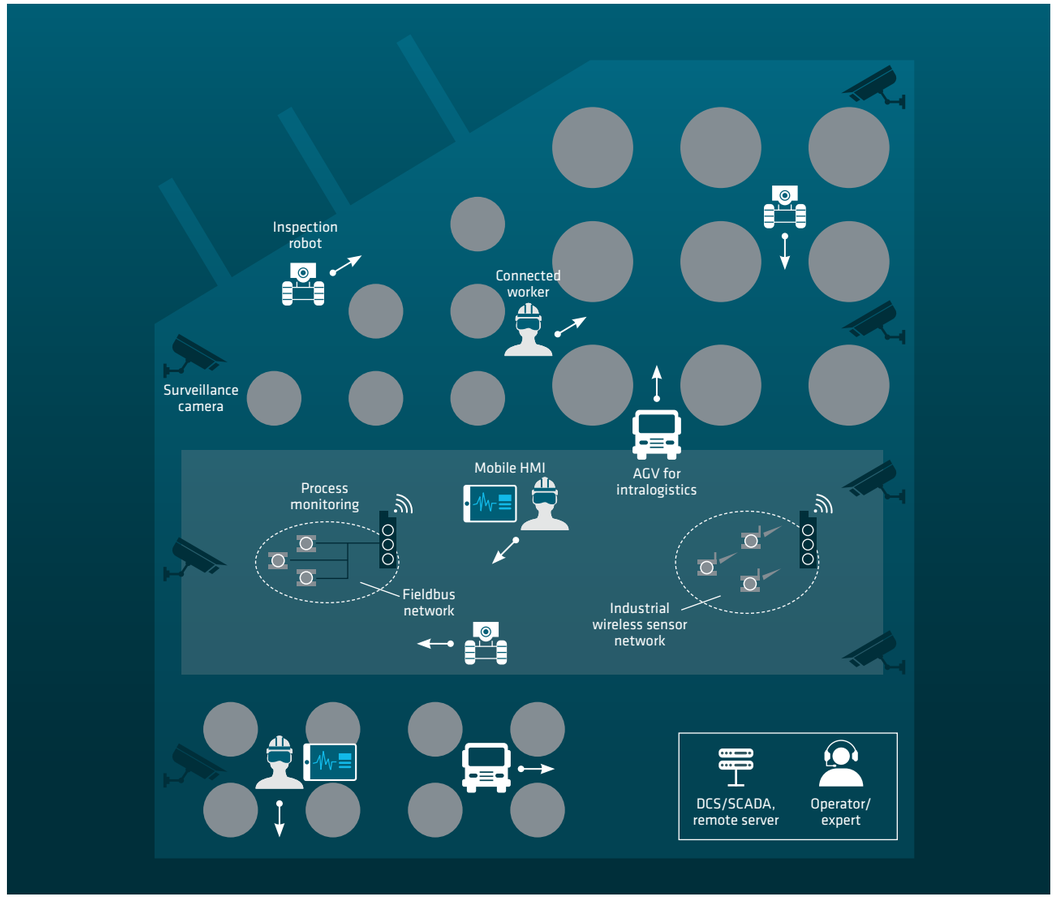


Source: 5G-ACIA / ZVEI e. V.

Each robot typically navigates to a designated destination and autonomously performs scheduled tasks. In some cases, however, a remote human operator may want to manually control a robot. High availability of the communi-cation services is essential in such a case, because some robots automatically shut down to prevent accidents if they lose the control signal for as little as 100 ms. The 5G network should also support low latency to enable smooth remote control of the robot (for example, an end-to-end latency of a few hundreds of milliseconds).

- **AGVs for intralogistics:** In this use case, AGVs are used to transport products within the plant premises. AGVs carrying tank containers move flexibly among storage facilities, refining equipment, and receiving/ shipping points, resulting in significantly faster trans-portation than is possible with railroad tank cars. This use case has communication requirements similar to those of the inspection robot case, since the AGVs also send environmental information to a remote vehicle management system for real-time control and opti-

Figure 4: Use cases in an oil refinery layout (based on figure 3)



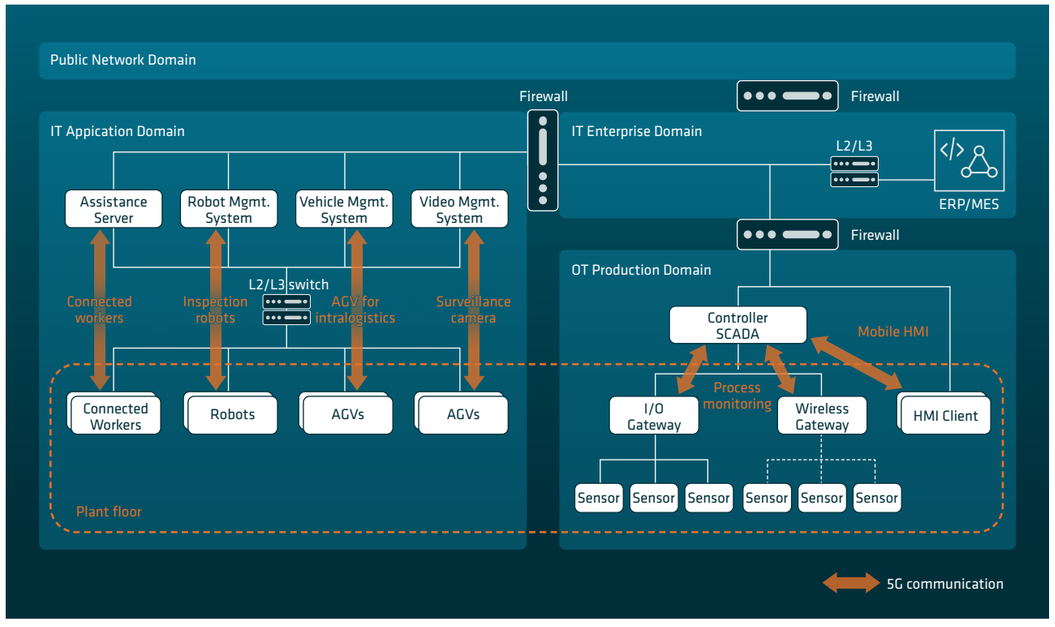
Source: 5G-ACIA / ZVEI e. V.

mization of traffic. Typically, however, remote vehicles travel faster – at around 7 km/h – than inspection robots (which usually only reach a maximum speed of 3 km/h), and significantly more AGVs than inspection robots are usually deployed.

- **Surveillance cameras:** Surveillance cameras are installed around the plant's perimeter and along pathways within the plant. They are used to monitor security and safety. 5G surveillance cameras can be flexibly installed anywhere that electric power is available, thus eliminating the need to install communication cables. 5G could extend the scope of video monitoring beyond the typical applications (such as detecting intruders, accidents, fire and excess heat etc.) by enabling wireless real-time transmission of high-resolution video. Examples of possible advanced applications include video-based monitoring of the condition of production assets (like detecting leaks, cracks and so on) and remotely sensing subtle changes in the production process (like the shape of a flame or color of a liquid surface). Surveillance cameras are usually stationary, but in some cases could also be mounted on a moving vehicle.

- **Process monitoring:** The 5G network could also be used to implement wireless backhaul for process monitoring sensors installed in the refining area. Gateway devices are often deployed to capture process values from sensors using domain-specific network technologies while implementing special precautionary measures in hazardous areas (examples include HART/WirelessHART, FOUNDATION Fieldbus, and ISA100 Wireless). The gateway typically carries consolidated data to a higher-level system (such as DCS or SCADA) in the operations center via a wired cable connection. With 5G, these cables can be replaced with wireless links, thus eliminating the need to build and maintain cable infrastructure throughout a large plant. The wireless gateway is stationary and installed close to but still outside the most hazardous zone of the refining area.

Figure 5: Logical view of industrial network for process industry scenario



Source: 5G-ACIA / ZVEI e. V.

There are stringent performance requirements for this use case in terms of reliability and communication determinism (the network's ability to operate within the agreed time window), since it is related to the core production process. However, these requirements are less stringent than in most factory automation and motion control cases. Communication intervals of one second or more are common in applications of these types.

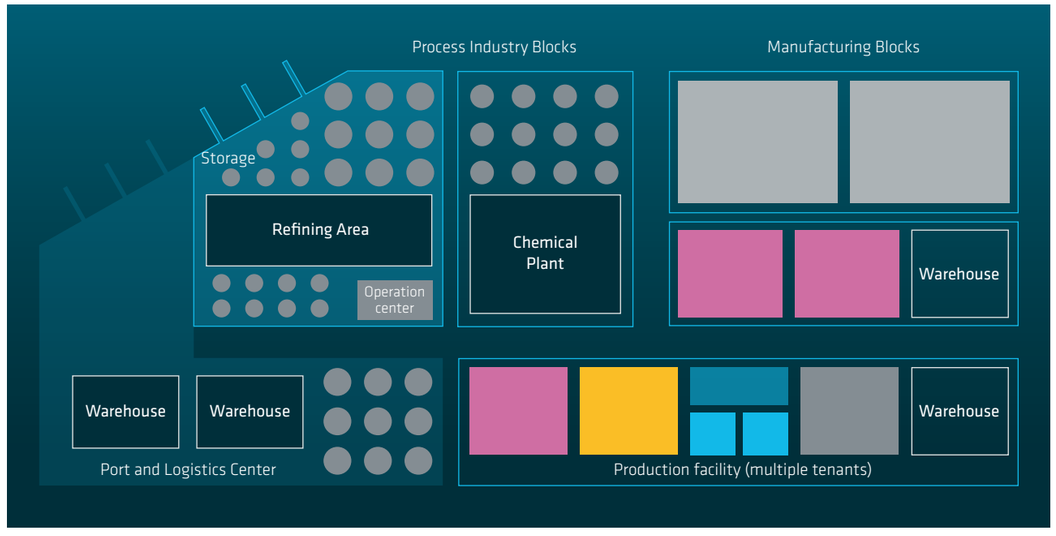
3.2.2 Network for Process Industry Scenario

Figure 5 shows an example logical network layout for the process industry scenario. The IT enterprise and OT production domains are used for automated production processes within enterprise and control systems. In this example, the OT production domain hosts mobile HMI and process monitoring use cases. The IT application domain hosts IT applications for enabling smart operation and maintenance with emerging digital technologies (AI, robotics etc.). The example layout includes use cases such as connected workers, inspection robots, AGVs for intralogistics, and surveillance camera. A domain hosting these kinds of IT applications must be entirely separate from other domains, and information flows between them must be strictly controlled while applying security best practices and industry standards to prevent any interference with the core production system as defined in [2].

3.3 Industrial Park Scenario

The term "industrial park" refers to an area of a city that is exclusively reserved for industrial use, as opposed to residential, commercial or other uses. It can range in size from a city block to an entire municipal district and contain factories, chemical plants, refineries, and/or logistical facilities such as a port. What typically sets industrial parks apart from other

Figure 6: Example industrial park layout



Source: 5G-ACIA / ZVEI e. V.

large industrial facilities is that they contain multiple commercial entities in close proximity to one other. These enjoy logistical benefits and can also take advantage of other synergies such as the presence of related industries. In addition to having well-connected logistics, an industrial park is often specifically designed to include infrastructure and utilities that support manufacturing operations. It's also possible for an industrial park to be owned and operated by a single large commercial entity. In this white paper, we specifically consider a case in which an industrial park comprises several commercial entities, one of which makes 5G communication services available to all of them as shared infrastructure.

Figure 6 shows an example layout of an industrial park.

3.3.1 Use Cases and Key Characteristics

In an industrial park, the use cases and communication requirements of each individual commercial entity engaged in an industrial activity (like operating a factory or plant) are essentially the same as those described in the preceding sections. In each of the discussed scenarios, the entire operation is run by that entity, which is also the natural stakeholder in the 5G service. In contrast, an industrial park scenario involves multiple commercial entities whose operations can be quite diverse, also resulting in differing requirements in terms of 5G communication, although they all share the same 5G communication system. It is also possible for some of the industrial players in the park to have their own 5G networks. Multiple distinct 5G networks may then need to coexist. These and other considerations for planning the deployment of a 5G NPN are discussed in greater detail in chapter 4.

3.3.2 Industrial Network for an Industrial Park

Here an industrial park hosts a number of distinct enterprises, each of which runs its own industrial operation. It is safe to assume that they also operate their own industrial networks, the properties of which may correspond to those mentioned above in the sections on manufacturing buildings and process industry scenarios.

3.4 Key Communication Characteristics of Industrial Operation Use Cases

The use cases described above differ in terms of their network requirements. Drawing on the 3GPP specifications (see [3] and [4]) and the IEC specifications summarized in [5], Table 1 below presents selected characteristics of them.

In addition, different security levels and privacy requirements may need to be implemented for use cases belonging to different domains, in accordance with the security principles specified in the industry security standards (see the summary in [5]).

3.5 Operations and Maintenance Aspects

In addition to 5G communication use cases, an NPN deployment can be affected by aspects of operating and maintaining a 5G network (generally referred to as operations and maintenance or O&M). The enterprise running the manufacturing or processing operation needs to be able to add or remove 5G devices and change the configuration of the network and devices. This is especially important during installation of the system just before use of the 5G NPN begins, and subsequently during normal production on an as-needed basis.

Another example of a situation in which operational aspects are important is when machines or plants have to be relocated. This may be required in order to optimize the positions of machines and plants and the paths running between the machines, meet space requirements for installing new equipment, or move machines to a remote destination. This makes it necessary to coordinate production planning, the contractor handling the move, the maintenance teams, and IT and OT departments. It's also necessary to appropriately manage

Table 1: Summary of key characteristics of use cases

	Service bitrate [Mbit/s] [3] *C.2*	**Communication service availability [%] [3]**	**Communication service reliability: mean time between failures**	**Maximum allowed end-to-end latency [ms] [3]** *C.5*	**Typical payload size [bytes]**	**Transfer interval**	**Number of devices**	**Typical service area [m x m x m]**	**Mobility area [m x m]**
Flexible assembly line									
Control to control [3] *A.2.2.2*	> 100	99.9999 to 99.999999	~ 10 years	< 10	1 k	≤ 10 ms	5–10	100 x 30 x 5	10 x 10
Wired to wireless link replacement [3] *A.2.2.4 – e.g. Ind. Ethernet (6) /TSN (5.6A)*	500	99.9999 to 99.999999	~ 10 years	< 1	10–1 k	≤ 1 ms	2–5	100 x 30 x 5	10 x 10
AGVs									
Mobile robots – incl. video [3] *A.2.2.3*	> 10	99.999	~ 10 years to ~ 1 week	< 10	40–250	1–50 ms to 40–500 ms	≤ 2000	100 x 30 x 5	100 x 30
Mobile worker manual assembly									
Augmented reality [3] *A.2.4.2*	> 100	99.9	~1 month	< 10	15 k–250 k	N/A	≤ 100	100 x 30 x 5	100 x 30
COBOTs									
Cooperative carrying – fragile workpieces; [3] *A.2.2.5*	2.5	99.9999 to 99.999999	~ 10 years	< 1	250–500	> 5 ms > 2.5 ms > 1.7 ms	2–8	100 x 30 x 5	10 x 10
Mobile HMI									
Mobile operation panels – visualization [3] *A.2.4.1A*	10 k	99.999999	1 day	10 to 100	10 to 100	10 ms to 100 ms	2 or more	100 to 2,000 [m²]	100 to 2,000 [m²]
Process monitoring									
Process and asset monitoring – process value [3] *A.2.3.2*	≤ 1 M	99.99	≥ 1 week	< 100	≥ 20	10 ms to 60 s	Up to 1 [UE/m²]	≤ 10 km x 10 km x 50 m	Stationary

Source: 5G-ACIA / ZVEI e. V.

the access rights and permissions that are required to alter the physical configuration and industrial network for each of these groups (see sections 3.1.3 and 3.2.3). Typically, a machine's or plant's network must be replicated at the destination, including various network settings such as IP addresses, subnets, NAT and firewall rules, and communication. In addition, it is important to prevent plants and machines that remain in place at the original site from being negatively impacted by the decommissioning of systems, network equipment, and/or machines.

Ideally, the NPN should permit automated deployment and configuration and efficient operation and maintenance throughout its lifetime. In actual scenarios, this means:

- Easy configuration or reconfiguration of the NPN for varying use cases and maintenance of system components
- Debugging capabilities and visibility tools for monitoring network performance and diagnosing failures
- Easy device configuration, onboarding, and management

It can also include, for example, monitoring the QoS of traffic for critical applications, communication and connectivity status, and the general service availability of devices and network equipment, among other things.

The relevant parameters for network operation and management via the network exposure interface for enterprises were discussed in an earlier white paper published by 5G-ACIA [6]. These parameters need to be integrated into APIs to provide the technical basis for network management and performance monitoring tools.

The NPN operator provides the services outlined in the foregoing to an industrial enterprise. Note that if multiple industrial enterprises use the same 5G network as tenants, all of the operational aspects discussed above need to be supported while separately considering the needs of each individual network tenant.

There may also be a need to integrate on-premises edge computing services.

4 NPN Deployments for Example Scenarios

4.1 Introduction

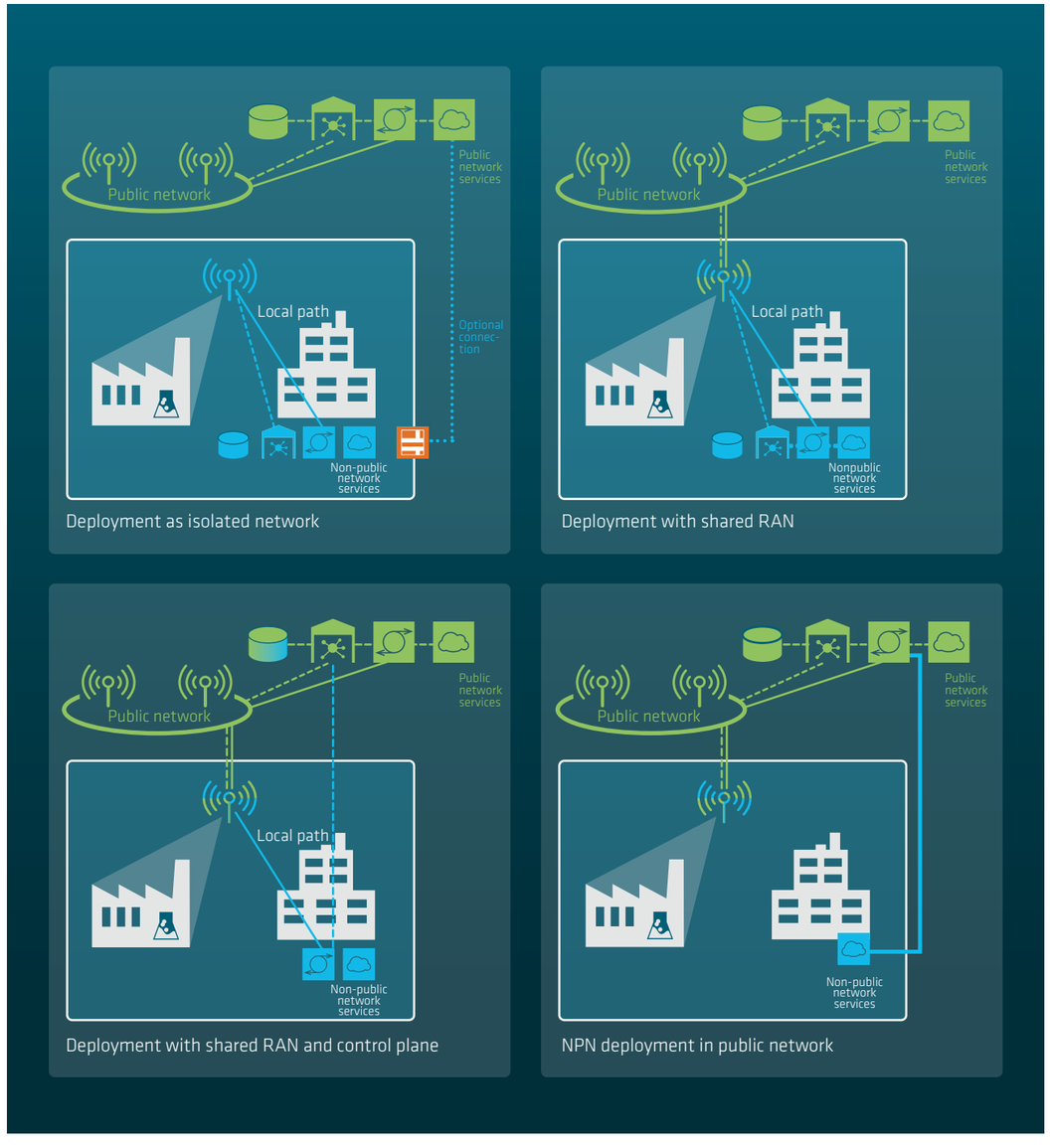
This section presents example NPN deployment designs for the industrial operation scenarios described in the previous chapter. See annex 9.2 for the legend corresponding to the 5G network nodes that appear in the figures of this chapter.

4.1.1 Background

The basic idea of NPN deployments is to assign dedicated network resources for industrial use so as to create a private network for use by an industrial player; in other words, it is closed to the general public. From a 3GPP perspective, two main types of NPNs are possible: standalone NPN (SNPN) and private network integrated NPN (PNI-NPN). An SNPN is an NPN run by an NPN operator without relying on a public network, while a PNI-NPN is an NPN deployed with the support of a public network, for example with logical separation of the public and non-public parts [4] [7].

While keeping in mind these standardized alternatives and ways in which they could potentially be used for the industrial domain, the cited earlier 5G-ACIA NPN white paper [1] discusses four deployment scenarios assigned to two groups: those that are independent of public networks, and those that are built using public networks. Figure 7 shows these two groups with the four deployment scenarios.

Figure 7: NPN types introduced in the original 5G-ACIA NPN white paper [1]



Source: 5G-ACIA / ZVEI e. V.

4.1.2 Practical Approach to NPN Deployment Options

The categorization used in the earlier white paper [1] was based on the types of relationships that an NPN can have with public 5G networks and how alternative network architectures with standardized features perform in different communication scenarios. It is still important to perform an analysis from that perspective, and the results presented in the earlier white paper are still valid (see section 4.1.1).

This white paper takes this analysis further while taking a more practical approach and considering the different demands placed on the NPN network in the use cases described in the previous chapter. Two main deployment options can be identified for meeting them.

The first option is to deploy an on-premises NPN in which all of the 5G network nodes responsible for 5G communication are located on the industrial enterprise's premises, as shown in figures 8, 9, and 11 to 13 in the following sections (see also section 4.1.3 on the roles in NPN deployment and section 5.3 on the NPN operation model and the 5G management system).

The second option is a partly on-premises NPN in which only some of the 5G network nodes responsible for the 5G communication are deployed within the industrial enterprise while others are deployed or reused in other networks, for example in a cloud or the network of a mobile network operator (MNO). Such a scenario could, for example, have 5G RAN (radio access network) nodes on-premises and core nodes off-premises. In some variations, the user plane core node can also be on-premises while control plane nodes remain off-premises.

Chapter 5 focuses on presenting deployment examples and identifying relevant aspects of them, for example control of a private 5G network. The figures in this chapter use the same graphical representations as the original NPN white paper, showing the 5G control and user plane elements (except O&M, which is separately discussed in section 5.3). Whether an industrial enterprise opts for fully or partially on-premises deployment depends on the requirements of the particular use case and operating model. These and other aspects of the deployment alternatives are analyzed further in chapter 5, where the use of SNPN and PNI NPNs in these deployments are also discussed.

4.1.3 Roles in NPN Deployment and Operation

When 5G NPN is deployed and used, several different roles can be identified. This document discusses roles in an NPN corresponding to certain responsibilities in terms of functionality and scope. A role is performed by a corresponding entity. The set of roles can vary depending on how the NPN is deployed; some roles may not be needed, while some entities may perform multiple roles.

Considering all of the deployment possibilities throughout a 5G NPN's lifecycle, there may be an extensive set of roles. Those that can be required for online operation of the NPN are the following:

- **Industrial enterprise:** This is an organization (such as a factory, assembly plant, processing industry facility, logistics and warehouse provider, mine, industrial campus, etc.) that uses industrial IoT technologies to implement OT use cases involving 5G radio connectivity. The industrial enterprise has first-hand access to information on the industrial operation's needs in connection with operating a 5G NPN.

- **NPN operator:** An entity that operates a private 5G network. The NPN operator has access to 5G O&M controls that are relevant to daily operation of the NPN, which in turn depend on the needs of the OT use case being executed. This can include modifying how the 5G network and 5G devices are configured.

- **Mobile network operator (MNO):** An organization that provides wireless communication services to the general public and private networking services to enterprises. When offering private networking services, the MNO may provide access to a relevant set of O&M functions to a separate entity acting as an NPN operator.

- **Network management service provider:** An organization that provides professional network management services to other organizations. It may assume the role of NPN operator.

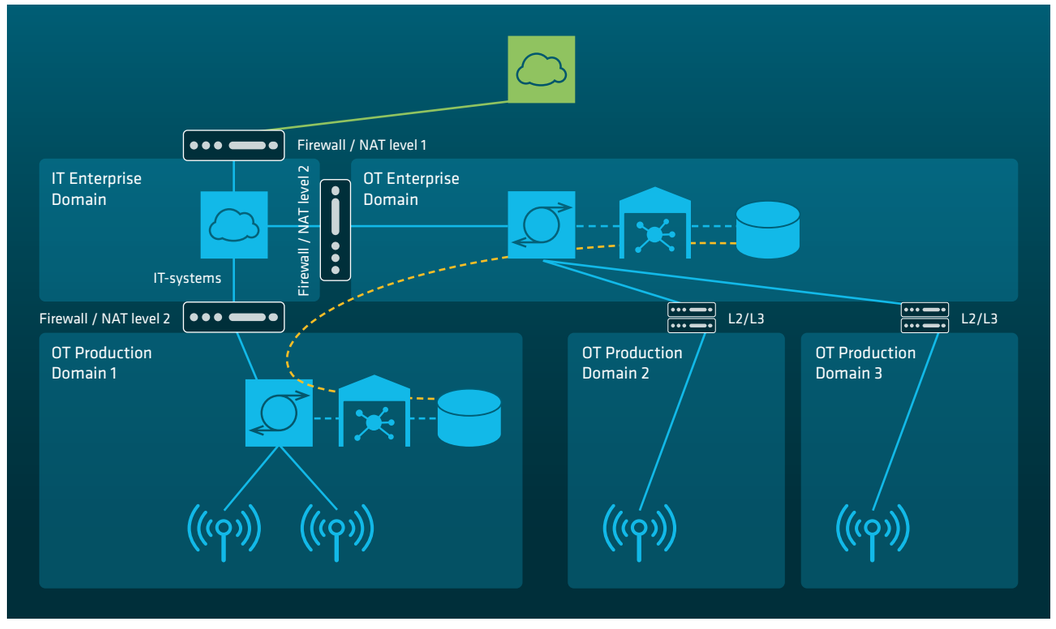
Focusing on roles defined in this way makes it clear that an industrial enterprise doesn't need to perform all of the roles related to an NPN. The NPN operator can be a separate entity if the industrial enterprise chooses not to operate the NPN itself. Also in the case of a PNI-NPN, the NPN operator can be separate from the MNO that provides the NPN. The entities involved need to conclude effective service agreements in these cases.

4.2 NPN Deployment Example for a Manufacturing Building Scenario

Within a medium to large manufacturing enterprise, different OT production domains can have diverging communication requirements corresponding to the use cases described in chapter 4. Use cases and their requirements for different domains can vary greatly, so almost every enterprise can be expected to be different in this respect.

In the example shown in figure 8, the use cases (such as COBOTs) of OT production domain 1 have very stringent latency, availability, and privacy requirements. An on-premises NPN is therefore deployed to ensure connectivity, privacy, and resilience.

Figure 8: Private 5G NPN deployment: manufacturing enterprise



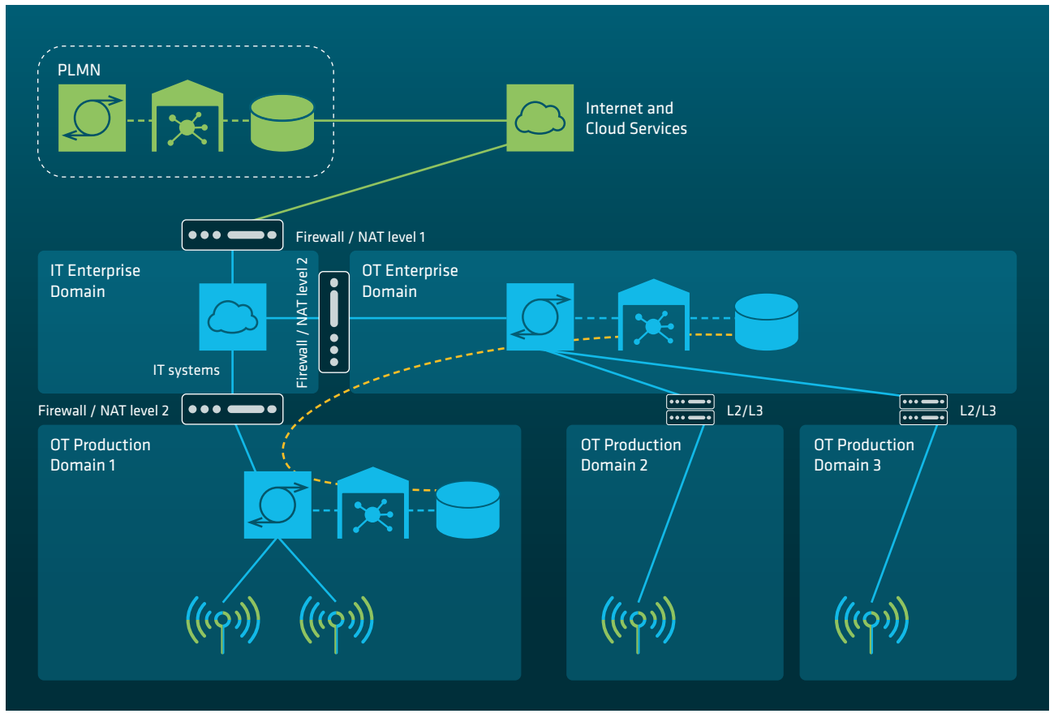
Source: 5G-ACIA / ZVEI e. V.

The use cases (such as connected workers) performed in OT production domains 2 and 3 in figure 8 have less stringent requirements that don't necessarily include deploying an exclusively on-premises NPN. However, a radio access network (RAN) is installed there to ensure optimal radio coverage. The RAN is connected to a central NPN core network installation in the OT enterprise domain. A firewall separates the OT enterprise domain from the IT domain. The central NPN core network installation can connect to and serve multiple production domains that have dedicated RAN installations and host use cases with similar communication requirements.

The deployment example shown in Figure 8 ensures that all security domains are separate from one another as explained in [8]. All traffic from an OT production domain must traverse at least two firewalls in order to access the public domain, in other words applications or servers that are located in a public or private cloud outside the enterprise infrastructure. Similarly, any traffic originating within an OT production domain must pass through at least one firewall to reach the enterprise's own IT domain.

On-premises NPN installations may be SNPNs or PNI-NPNs as discussed in section 5.2 (note that other considerations introduced in chapter 5 may also apply). In the case of PNI-NPNs, the expectation is that the public network service provider will install all network functions on site in order to make sure to meet the stringent availability and resilience requirements.

Figure 9: Private 5G NPN deployment with RAN sharing: manufacturing enterprise

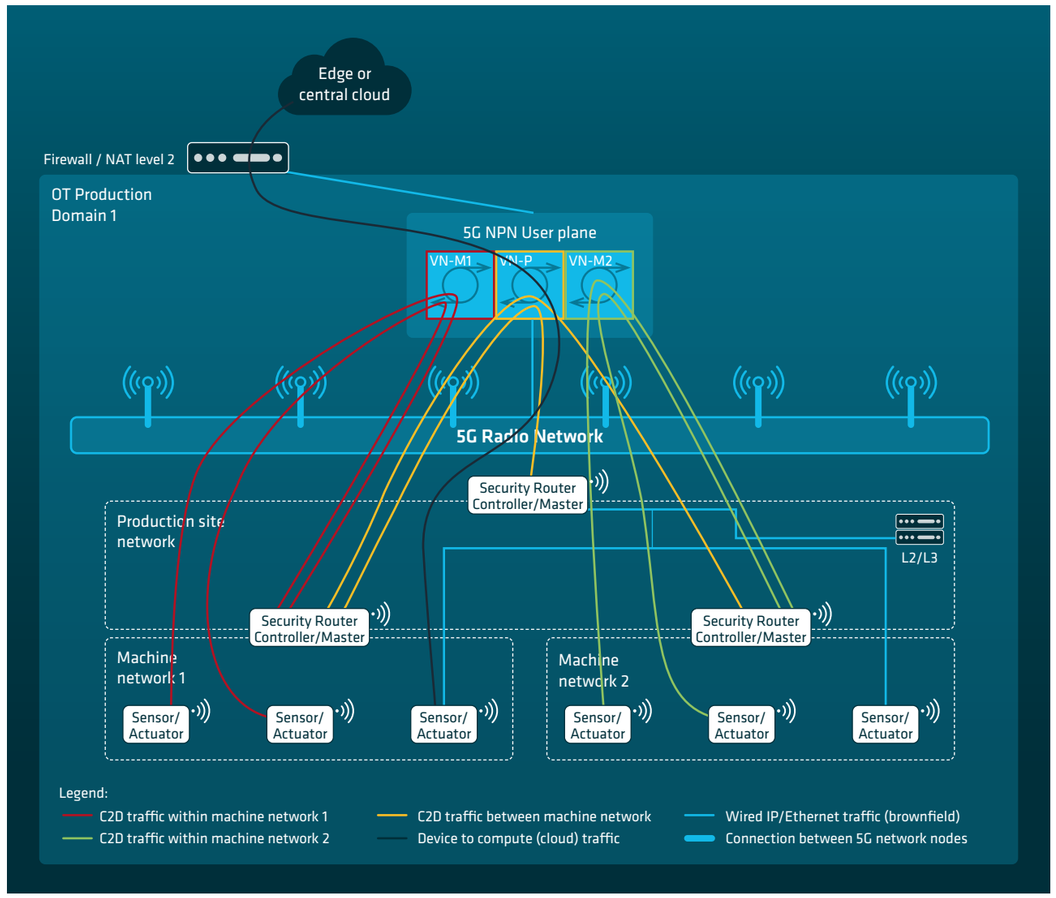


Source: 5G-ACIA / ZVEI e. V.

To simplify operation, the subscriber databases in both NPN installations can be synchronized; this is indicated in figure 8 by a dotted yellow line (also in figures 9, 11, and 13). This ensures that subscription and authentication records are identical in both installations and enables that enterprise's devices to access all production domains if required.

Optionally, the dedicated RAN deployed in the OT production domains can use RAN sharing. This means that the on-premises NPN and a public network service provider share the same RAN nodes and RAN infrastructure. Whether the public network service provider – the MNO – and the NPN operator of the on-premises NPN are the same organization or different

Figure 10: User plane data streams for dedicated NPN installation: manufacturing enterprise



Source: 5G-ACIA / ZVEI e. V.

ones that have concluded a sharing agreement is beyond the scope of this white paper. In order for RAN sharing to work, the RAN nodes must be connected to both the on-premises NPN core network and the public network service providers' core network. Figure 9 illustrates a RAN sharing setup. The details of its implementation are beyond the scope of this document.

5G devices may then choose (for example, based on their subscriptions and/or desired services) to use either the on-premises NPN or the public service provider's network. When a 5G device selects a public network, it can take advantage of all of the services provided by the PLMN operator. Typically, 5G devices involved in the use cases shown in the industrial operation examples in chapter 3 only use the on-premises NPN and associated services. Precisely which methods, configurations, and prerequisites are involved for selecting public or NPN network services exceeds the scope of this paper.

For the sake of simplicity, the option of shared RAN is only shown in this deployment scenario. However, shared RAN may also be deployed for the process industry and industrial park scenarios discussed in sections 4.3 and 4.4.

Figure 10 shows details of how the user plane node of an on-premises NPN deployed within an OT production domain could be configured. The depicted configuration ensures that traffic among sensors, actuators, and controllers of the same machine network can flow within a virtual network in the NPN. The use cases described in section 3.1.3 can involve a configuration of this kind if multiple machine networks coexist and the traffic within an individual machine must be concealed within the corresponding machine network. Some user plane traffic may need to be routed to other machine networks or to hosts outside the OT production domain. In this example, three virtual networks (VNs) are configured in the 5G NPN user plane node. For simplicity's sake, the 5G control plane is not shown in Figure 10 (O&M is also hidden). It should be noted that other configuration options can also be used to separate traffic.

The VN-M1 (a 5G virtual network for machine network 1) connects all of the sensors/actuators and controllers as well as security routers belonging to machine network 1. The red lines indicate *Controller-to-Device* (C2D) traffic use cases. VN-M2 is used similarly in the second machine network, with the logical links within it indicated by green lines. This type of configuration makes it possible to isolate traffic pertaining to only one machine, and also supports machine cloning use cases as mentioned in section 3.5.

Communication between machine networks, which typically occurs in *Controller-to-Controller* (C2C) use cases, takes place via the third group of virtual devices, namely VN-P (= 5G virtual network production site), indicated in figure 10 by beige lines. The VN-P logically separates the C2C traffic from the traffic within each machine network, and can also be used by sensors that communicate with edge cloud servers and applications (not shown). This approach can be taken for *Device-to-Compute* traffic use cases in brownfield deployments, like when sensor data needs to sent to an edge application while bypassing the installed controllers and infrastructure for capacity, safety, and/or certification reasons.

The same deployment and configuration principles also apply to production domains (for example, production domain 2 in figure 8) that share the same NPN deployment. In such a case, the 5G user plane node deployed in the OT enterprise domain is configured with corresponding virtual networks and serves machine network traffic use cases accordingly.

For the sake of simplicity and to avoid repetitions, individual detailed traffic cases corresponding to the process industry examples aren't shown in the following sections. However, the same principles can be applied to the use cases described in section 3.2, such as connected worker, mobile HMI, AGV, surveillance camera, etc. as shown in figure 5.

4.3 NPN Development Example of Large-Scale Process Industry Scenario

The principles shown for the manufacturing building scenario can also be applied to a large-scale process industry scenario. The main difference is that the geographical area is much larger in the large-scale process industry scenario and has multiple overlapping domains. In other words, the domains are not physically separated into, for example, buildings and production halls like in the manufacturing building scenario.

In the example shown in figure 11, the production domains are divided into IT application domains and OT production domains as described in section 3.2. A dedicated NPN is also deployed in each domain.

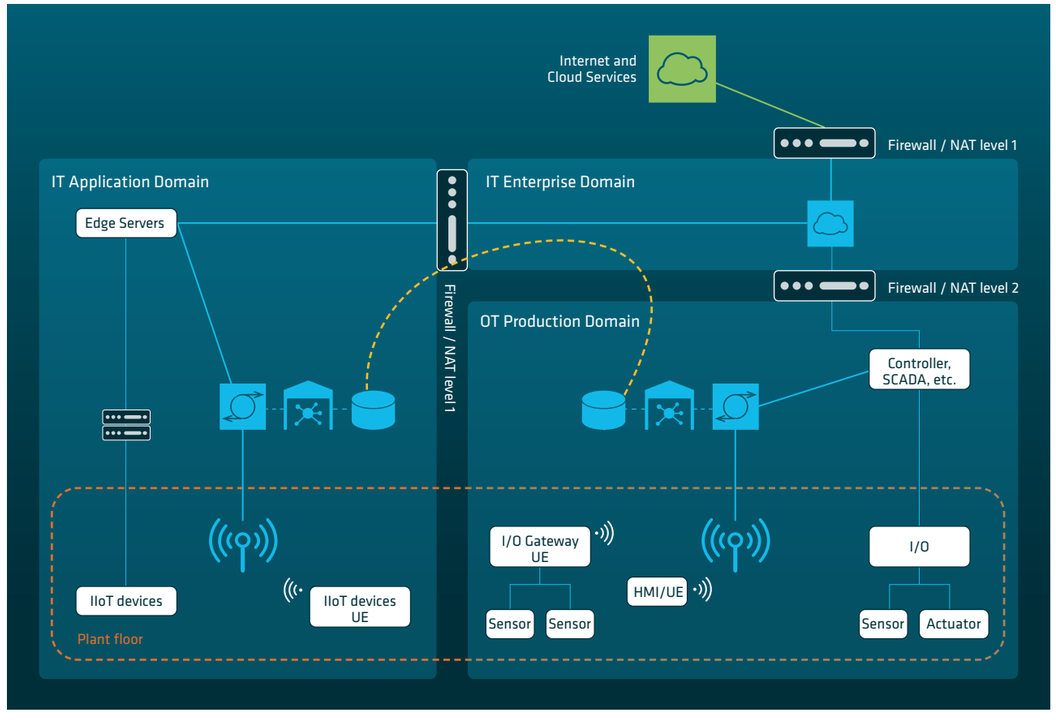
Production domain use cases typically have strict latency, availability, and privacy requirements. A dedicated NPN is therefore installed in each domain to ensure optimal connectivity, security, privacy, and resilience.

The IT application domain has less stringent demands, so the NPN deployed there covers a large physical area comprising several production or application domains with similar requirements.

Similarly to the manufacturing building scenario, for the sake of operational simplicity it is possible to synchronize the subscriber database across both NPN installations. RAN sharing with a public network service provider can also take place (not shown in figure 11).

If there are no such stringent application requirements in terms of performance, security, and privacy, plant owners may want to deploy a single NPN for OT production domains and IT applications. Figure 12 shows another example in which a shared NPN is deployed for all use cases in the plant.

Figure 11: Private 5G NPN deployment: process industry (multiple NPNs)



Source: 5G-ACIA / ZVEI e. V.

In this example, the OT enterprise domain is added for hosting the shared NPN. Devices in IT application domain 1 and OT production domain 1 are non-5G devices that only communicate via wired connections. 5G wireless devices in IT application domain 2 and OT production domain 2 communicate with non-5G components across the NPN core network while passing through a firewall.

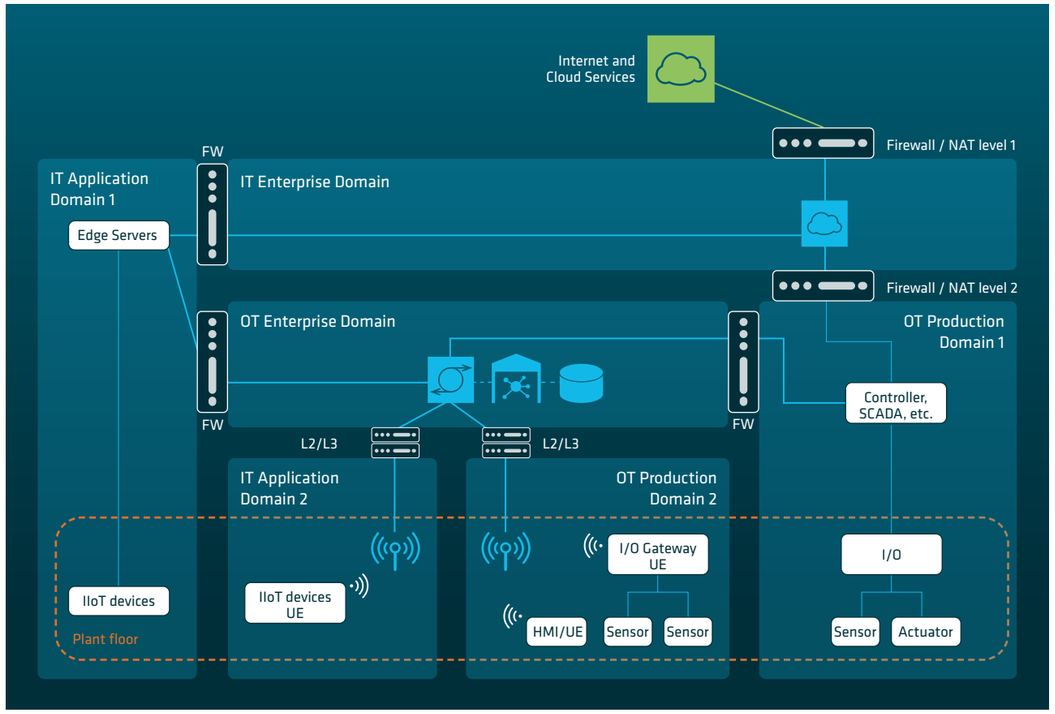
The 5G NPN ensures logical isolation between communication traffic of the OT production domain and IT applications in the common OT enterprise domain. This can be achieved by, for example, applying the principles explained in figure 10 for the manufacturing building scenario.

4.4 NPN Deployment Example of the Industrial Park Scenario

The industrial park scenario is a mixture of the previous two scenarios: many enterprises with significantly varying needs and capabilities hosted by a campus operator/manager with its own IT and OT enterprise domains.

In the example shown in figure 13, enterprise *A* has stringent latency, availability, and privacy requirements that justify a dedicated NPN installation in its own OT *A* production domain 1 to ensure maximum connectivity, privacy, and resiliency. The NPN deployment for enterprise *A* may follow exactly the same logic as the deployment shown for the manufacturing building scenario in figure 8 in section 4.2

Figure 12: Private 5G NPN deployment: process industry (common NPN)

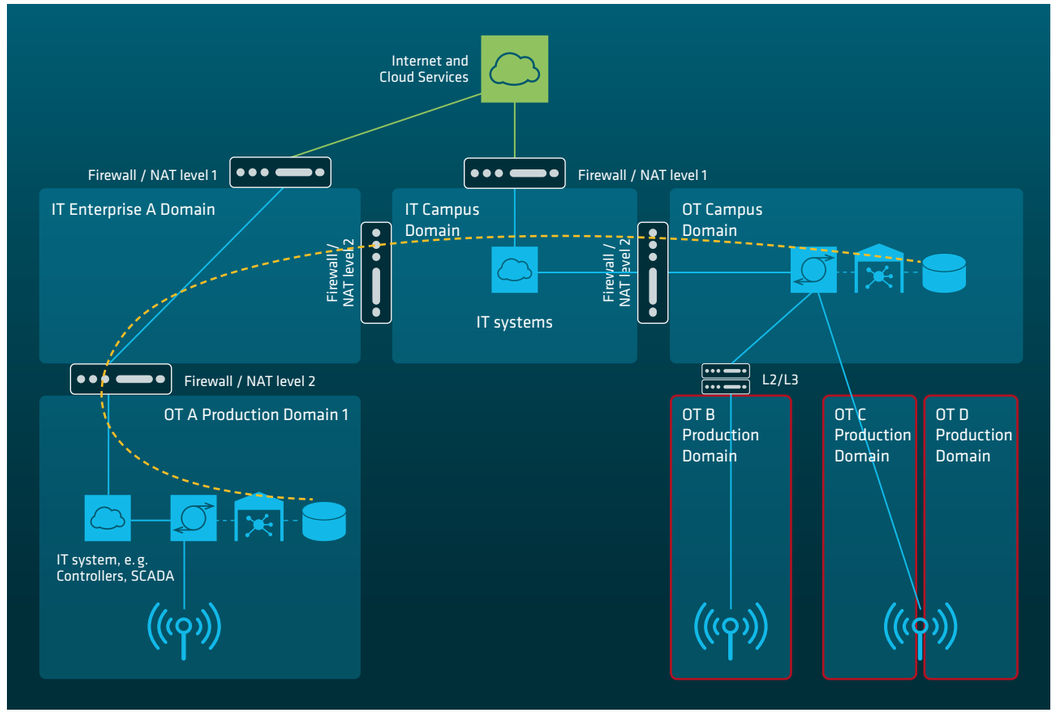


Source: 5G-ACIA / ZVEI e. V.

Enterprises *B*, *C*, and *D* don't have their own IT domains. Instead, they use IT services provided by the campus manager's IT domain, which includes an OT campus domain that in turn hosts an NPN installation. That NPN is provided as a service to enterprises *B*, *C*, and *D*. The radio coverage required for the enterprise is provided by a dedicated RAN installation at the corresponding physical site. Note that enterprises *B*, *C*, and *D* are not in the same security zone as enterprise *A*, and the traffic flows of enterprises *B*, *C*, and *D* are also physically separate from enterprise *A*. Traffic flows of enterprises *B*, *C*, and *D* within the dedicated NPN in the OT campus domain are logically distinct. Tracking areas, network slices etc. are used to achieve logical separation of different 5G technologies such as separate DNNs (data network names).

Similarly to the manufacturing and process industry scenario, synchronization of subscriber databases and RAN sharing can be applied (not shown in figure 13).

Figure 13: Private 5G NPN deployment: industrial park/campus



Source: 5G-ACIA / ZVEI e. V.

5 NPN Deployment Analysis and Recommended Considerations

5.1 Introduction

The examples and use cases of industrial operations presented in chapter 3 are based on input received from 5G-ACIA OT member companies, and the 5G NPN deployment examples in chapter 5 have been designed for them based on input from 5G-ACIA ICT companies. In this chapter we discuss the practical differences among them in greater detail.

5.2 Support for User Cases with SNPN and PNI-NPN

As already discussed, how 5G network elements are physically deployed in relation to the industrial network depends on the needs of the use cases. The primary purpose of the NPN is to provide communication capabilities that perform appropriately while also meeting privacy and security requirements. Each of the examples presented in chapter 4 involves an on-premises NPN: the 5G network elements that support industrial communication are deployed locally at the manufacturing site (as shown in the figures there). The location of the network management system responsible for 5G O&M is discussed in sections 5.3 and 5.4.

An on-premises NPN supporting any of the examples can be either an SNPN or a PNI-NPN. As long as it is deployed with local network elements as shown, its performance can be adequate for the presented use cases. In terms of performance, there is no difference between on-premises SNPNs and PNI-NPNs.

The practical differences between on-premises SNPNs and PNI NPNs have more to do with how they are operated. For example, whether a party other than the industrial enterprise is involved in operating the 5G service (and therefore has access to data carried by it) poses a privacy or security concern and if so whether it is enough to logically separate different functions or if they also need to be physically separated. These considerations apply fairly uniformly to all of the presented examples with only minimal variations. In the following sections, these aspects are discussed in general terms for all of the examples while calling attention to use case dependencies where applicable.

5.3 NPN Operation Model and 5G Management System

The NPN operation model defines how a 5G NPN is operated and managed. The corresponding entity is the NPN operator (see section 4.1.3). These are O&M functions for managing the NPN's configuration and performance, monitoring its status, and handling alarms. It is commonly (but not entirely correctly) assumed that an NPN can only be operated and managed by the same entity that has deployed it; for an SNPN this is the industrial enterprise and for a PNI-NPN it is the MNO. This is based on the thinking that an SNPN is completely independent of any third parties, while a PNI-NPN is always supported by the PLMN, so it therefore also has to be operated by the MNO.

This is not always the case, however, as has already been pointed out in section 4.1.3. It is possible to have an SNPN with an as-a-service model in which a network management service provider operates the network and the industrial enterprise receives the connectivity services it requires on the basis of a service level agreement. Conversely, it is also possible for the PNI-NPN hosting the MNO to allow the PNI-NPN tenant (the industrial enterprise) to act as the NPN operator and control, manage, and operate the NPN network infrastructure, which is then at least logically separated from the public network. The extent of control handed to the NPN operator depends on the needs of the industrial operation, and it is necessary to conclude a corresponding service level agreement.

Regarding operation of the NPN, it depends on the extent to which the industrial enterprise wants to be involved in the technical aspects and to what level of detail it wants to be able to control the NPN, while accepting the corresponding responsibilities, instead of concluding a service level agreement that only requires direct involvement at the outset plus monitoring during actual operation. This applies to all of the case examples presented in chapter 5.

5.4 Connectivity to External Networks

Regarding connectivity to external networks, the reader is referred to the cases in which a 5G NPN is deployed like in the examples in chapter 5: connected to another network outside the premises of the industrial enterprise or simply to a network domain that is separate from the industrial network. This is not needed in all cases; it is possible to deploy an on-premises NPN without this connectivity. When it exists, however, it is essential to meet privacy and security requirements.

All of the deployment examples provided in chapter 5 include an optional connection to the public cloud or Internet via the IT domain. These connections can be firewall-controlled to meet industry requirements and used by local applications, for example to access cloud services.

Connectivity with external networks comes into play when a PNI-NPN is deployed as a partially on-premises NPN. Different versions of this case apply depending on whether parts of the user data and/or data or functions related to controlling and managing the NPN are handled off or on the industrial enterprise's premises. These cases are not described in detail in chapter 5; more information on them is available in [1]. Privacy and security concerns need to be addressed in the service level agreement with the MNO that is hosting the NPN.

In some cases, connections to one or more external networks may be required to operate an on-premises NPN. The figures in chapter 4 show the 5G user plane and control plane elements that handle the functions of 5G system when it is operational, but without showing details of the O&M-related functions of the 5G management system (MS). The NPN operator uses the 5G MS to operate the NPN. Depending on the case, the MS would be located locally as a local application in the 5G nodes or in the local cloud, remotely in the public cloud, or a combination of both. Typically, the MS will be local when the industrial enterprise performs the role of NPN operator, and at least partly remote whenever a network management service provider acts as the NPN operator, which is the case when the NPN adheres to the as-a-service model.

Any external connectivity needed for network management can also be implemented in compliance with industry standards by using firewalls, and the connections involved can also be time-throttled or else only opened from inside the enterprise when this is actually needed (for example, to respond to alarms).

5.5 Logical and Physical Separation of Domains and Networks

As shown in chapter 3, industrial networks comprise different domains, which in a wired deployment are also physically separated from each other and connected only via a firewall or L2/L3 infrastructure. In the physical factory and plant layouts, we can also see that these domains partially overlap. For a 5G deployment, especially if it includes radio coverage, it wouldn't be practical to assume that a distinct NPN can be created for each of the domains to physically separate them like in a wired deployment. However, different NPNs could be deployed in order to, for example, separate different OT domains from each other as shown in figure 9 in section 4.2. This type of deployment can also be implemented with a single set of physical hardware, thus creating separate virtual network instances for the two domains.

When logical separation of different domains is enough, without additionally requiring physical separation, a practical solution is for all of the domains to be supported by a single NPN deployment while they remain logically distinct from one other. In this case, network slicing can be used to separate the domains, for example as shown in figure 11 in section 4.3. Logical separation is also achievable with VLANs and 5G virtual networks, which can be used to separate different industrial network domains within the same NPN as

shown in figure 10. A typical PNI-NPN would use the same type of logical separation.

Since many IT and ICT solutions are now being developed using edge cloud and cloud-based technologies, and these are also playing an increasingly prominent role in the industrial domain [9], sharing of physical resources and the use of logical separation appear to be practical and cost-effective solutions, also for 5G NPNs.

5.6 Availability and Use of Spectrum

Although this topic hasn't been discussed in the previous sections, it is a very relevant aspect for NPN deployments, since every NPN requires access to sufficient 5G-suitable spectrum in order to host use cases. We have assumed this to be the case in the preceding sections, and there are no technical constraints on doing so in any of the example deployments.

The availability of spectrum depends on local legislation where the NPN is deployed. This can restrict the available deployment options. To sum up, if an enterprise wants to have an SNPN it needs to gain access to sufficient spectrum, either directly or via the party that offers the SNPN to it as a service. In some countries, spectrum is made directly available to enterprises by a national administration or can be subleased from mobile network operators. If there is no way to access spectrum, then a PNI-NPN is the only option. As already discussed in this chapter, and especially in sections 5.2 and 5.3, the differences between SNPN and PNI-NPN can be tiny and not matter much from an industrial enterprise's perspective.

6 Conclusions

This white paper discusses examples of NPN deployments for three different types of industrial operation scenarios: a manufacturing building, a large-scale process industry scenario, and an industrial park containing a number of enterprises of the preceding two types. First these example industrial operation scenarios are described in terms of which use cases could use 5G communication, the layout of these facilities, and how the industrial network could be arranged within them in a typical scenario. Applying the domains in the industrial network diagrams as a reference, this paper shows how the network functions of the 5G NPN could be deployed to support the use cases.

Finally, several aspects that are likely to affect which NPN deployment option is chosen for each scenario are described and analyzed. The conclusion is drawn that many possible alternatives exist and the differences between them may not be very large in terms of technical performance. There are also other important considerations relating to how different types of NPNs are operated, and the recommendation is therefore made to carefully consider the requirements that each industrial enterprise needs them to meet.

7 Definitions of Acronyms and Key Terms

3GPP
The 3rd Generation Partnership Project (3GPP) is an umbrella term for a consortium embracing a number of standards organizations worldwide that are collaborating to develop globally accepted specifications for mobile telecommunications. As its name implies, it was originally created to establish specifications for the third generation (3G) of mobile communication systems. It has continued working on subsequent generations, including the Fifth Generation (5G), which is considered in this white paper.

5G-ACIA
The 5G Alliance for Connected Industries and Automation is the globally leading organization for shaping and promoting industrial 5G.

AGV
Automated guided vehicle

AI
Artificial intelligence

COBOT
Collaborative robot

DCS
Distributed control system

ERP
Enterprise resource planning

HMI
Human-machine interface

I/O
Input/output

ICT
Information and communication technology

IT
Information technology

L2
Layer 2 infrastructure

L3
Layer 3 infrastructure

MES
Manufacturing Execution System

MNO
Mobile network operator

NPN
Non-public network

O&M
Operations and maintenance

OT
Operational technology: hardware and software that detect or cause a change by directly monitoring and/or controlling industrial equipment, assets, processes, and events

PNI-NPN
Public network integrated NPN

QoS
Quality of service

RAN
Radio access network

SCADA
Supervisory control and data acquisition

SNPN
Standalone NPN

TSN
Time-sensitive networking

UE
User equipment

VN
Virtual network

8 Annex

8.1 Additions to NPN Standards Since Publication of the Original 5G-ACIA NPN White Paper

Our first NPN white paper was based on 3GPP Release 16. 3GPP is currently working on Release 18. The features that 3GPP working group SA2 has added to Release 17 and Release 18 are summarized in the following.

Release 17 (for a more detailed description, see clause 5.30 of Technical Specification (TS) 23.501 V17 [7]):

- The 5G UE is authenticated and authorized to access a SNPN in "SNPN access mode" using credentials from a Credentials Holder, which may be a third-party entity. The Credentials Holder and SNPN owner have an agreement and are interconnected. The Credentials Holder must deploy at least one AAA server if its credentials are not based on IMSI. If the credentials are based on IMSI/(USIM), the Credentials Holder must deploy at least one AUSF and UDM. The SNPN broadcasts an indication of whether access using credentials from a Credentials Holder is supported. The SNPN also broadcasts a list of identifiers called Group IDs for Network Selection (GINs) representing the Credentials Holder's identities.
- The onboarding procedure is used to provide the SNPN's credentials for primary authentication and other information to enable the UE to connect to a desired SNPN. The onboarding procedure can be performed via an SNPN network that advertises that it supports onboarding. The SNPN enables the UE to connect using default credentials, in other words credentials that don't belong to the SNPN providing the onboarding service. This connectivity is limited to onboarding. Provisioning and configuration of UE primary credentials in the 5G core network of the SNPN from an external server is not covered by the 3GPP standards. Onboarding for a UE belonging to an SNPN can be also facilitated by a PLMN, but in this case the UE must be equipped with the PLMN's credentials in USIM for connecting to the PLMN.
- In the case of PNI-NPN, the UE uses "PLMN access mode" and the onboarding procedure can only involve provisioning the credentials for slice authentication and secondary authentication/authorization, which can be used when establishing a PDU session. Provisioning of IMSI/(USIM) for primary authentication to PLMN is a different procedure specified by OMA and GSMA.

Release 18 (for more details, see clause 5.30 of TS 23.501 V18 [10]):

- Support for mobility between equivalent SNPNs
- Support for trusted and untrusted non-3GPP access for SNPN, also for onboarding purposes
- Support for connecting devices that don't support 5GC NAS signaling over non-3GPP access to SNPN (devices of this kind are called "non-5G-capable over WLAN")
- Support for localized services provided within a specific limited area during a specific period of time. The provided services can be applications (for example, live or on-demand audio/video streams, electric games, IMS, etc.), or connectivity (such as UE to UE, UE to data network, etc.). The service provider can be an application provider or network operator that provides localized services via an SNPN or a PNI-NPN. Use cases have mainly been defined for campuses, expositions, stadiums, and concerts with the general public in mind.

It should be noted that the majority of the features added to SNPN in Rel-18 had already been supported for PLMN deployments in previous releases and can therefore also be provided in PNI-NPN deployments.

8.2 Legend for Figures

Figure 14: Symbols used in figures

Source: 5G-ACIA / ZVEI e. V.

9 References

[1] 5G-ACIA, „Whitepaper - 5G Non-Public Networks for Industrial Scenarios," 2021. [Online]. Available: https://www.5g-acia.org/fileadmin/5G-ACIA/Publikationen/5G-ACIA_White_Paper_5G_for_Non-Public_Networks_for_Industrial_Scenarios/WP_5G_NPN_2019_01.pdf.

[2] NAMUR, „NE 175 - NAMUR Open Architecture – NOA Concept," NAMUR, 2020.

[3] 3GPP, „TS 22.104 - Service requirements for cyber-physical control applications in vertical domains, v18.3.0," September 2023. [Online]. Available: https://www.3gpp.org/ftp/Specs/archive/22_series/22.104/22104-j10.zip.

[4] 3GPP, „TS 22.261 - Service requirements for the 5G system, v18.11.0," September 2023. [Online]. Available: https://www.3gpp.org/ftp/Specs/archive/22_series/22.261/22261-j40.zip.

[5] Wikipedia, "IEC 62443," [Online]. Available: https://en.wikipedia.org/wiki/IEC_62443. [Accessed 8 November 2023].

[6] 5G-ACIA, „Whitepaper - Exposure of 5G Capabilities for Connected Industries and Automation Applications," 26 6 2020. [Online]. Available: https://www.5g-acia.org/fileadmin/5G-ACIA/Publikationen/5G-ACIA_White_Paper_Exposure_of_5G_Capabilities_for_Connected_Industries_and_Automation_Applications/5G-ACIA_Exposure_of_5G_Capabilities_Download.pdf.

[7] 3GPP, „TS 23.501 - System architecture for the 5G System (5GS), v17.9.0," June 2023. [Online]. Available: https://www.3gpp.org/ftp/Specs/archive/23_series/23.501/23501-h90.zip.

[8] 5G-ACIA, „Whitepaper - Security Aspects of 5G for Industrial Networks," May 2019. [Online]. Available: https://www.5g-acia.org/fileadmin/5G-ACIA/Publikationen/5G-ACIA_White_Paper_Security_Aspects_of__5G_for_Industrial_Networks/5G-ACIA_WhitePaper_Security_Aspects_of_5G_for_Industrial_Networks_Download.pdf.

[9] 5G-ACIA, „Whitepaper - Industrial 5G Edge Computing – Use Cases, Architecture and Deployment," February 2023. [Online]. Available: https://5g-acia.org/whitepapers/industrial-5g-edge-computing-use-cases-architecture-and-deployment/.

[10] 3GPP, „TS 23.501 - System architecture for the 5G System (5GS), v18.2.2," July 2023. [Online]. Available: https://www.3gpp.org/ftp/Specs/archive/23_series/23.501/23501-i22.zip.

5G-ACIA White Paper
NPNs for Industrial Scenarios

Contact
5G-ACIA
Lyoner Strasse 9
60528 Frankfurt am Main
Germany
Phone: +49 69 6302-209
Email: info@5g-acia.org
www.5g-acia.org

Published by
ZVEI – German Electro and Digital Industry Association, 5G-ACIA - 5G Alliance for Connected Industries and Automation, a Working Party of ZVEI
www.zvei.org

Published in March 2024

Design: COBRAND

10 5G-ACIA Members

As of February 2024

AALBORG UNIVERSITY DENMARK
ABB
Alleleran
AI-LINK
ANALOG DEVICES
ASKEY
asmote
ASOCS
ATAYA
ATHONET
axians
BASLER
BAYFU
BECKHOFF
BOSCH
brown-iposs
CAMPUS GENIUS
Capgemini engineering
cellnex
celona
中国移动 China Mobile
cisco
CONGIV
CTONE
DEMAG
DENSO
Deutsche Messe
DFKI
CATAPULT Digital
docomo
Druid
EMERSON
Endress+Hauser
ERICSSON
equinor
FESTO
firecell
flex
Fraunhofer
GHMT
HARTING
HIRSCHMANN A BELDEN BRAND
HMF smart solutions
hms
HUAWEI
IDLab INTERNET & DATA LAB
ifak
ifm

財團法人資訊工業策進會 INSTITUTE FOR INFORMATION INDUSTRY
infineon
inIT
intel.
ITRI Industrial Technology Research Institute
KETI
KEYSIGHT
kontron
Lenovo
MITSUBISHI ELECTRIC
MOXA
MUGLER TELCO NETWORKS.
NOKIA
NXP
OMRON
orange
Panasonic
PEPPERL+FUCHS
PHOENIX CONTACT
Qualcomm
RELIABLE REAL-TIME RADIO
Radisys
Rockwell Automation
ROHDE&SCHWARZ
SAL SILICON AUSTRIA LABS
salzburgresearch
Schneider Electric
SICK
SIEMENS
SINTEF
SoftBank
SONY
life.augmented
Telefónica
telent
TNO
TRUMPF
台灣電信技術中心 TELECOM TECHNOLOGY CENTER
ublox
UNIBERG
UPLINK
verizon
VOLKSWAGEN AKTIENGESELLSCHAFT
WAGO
Weidmüller
YOKOGAWA
ZTE

5G ACIA

5G-ACIA.org