
# Private 5G Networks for Connected Industries

## Deliverable D2.1

# Intermediate Report on Private 5G Network Architecture

Co-funded by the Horizon 2020 programme
of the European Union in collaboration with Taiwan

**Date of Delivery:** 04.09.2020
**Project Start Date:** 01.10.2019
**Duration:** 36 Months

# Document Information

| | |
|---|---|
| **Project Number:** | 861459 |
| **Project Name:** | Private 5G Networks for Connected Industries |

| | |
|---|---|
| **Document Number:** | D2.1 |
| **Document Title:** | Intermediate Report on Private 5G Network Architecture |
| **Editor:** | Sven Wittig (HHI) |
| **Authors:** | Sven Wittig (HHI)<br>Mathis Schmieder (HHI)<br>Henrik Klessig (BOSCH)<br>Bettina Kauth (BOSCH)<br>Frank Heitkämper (BOSCH)<br>Cheng-Yi Chien (Chunghwa Telecom, CHT)<br>Jiun-Cheng Huang (Chunghwa Telecom, CHT)<br>Yueh-Feng Li (Chunghwa Telecom, CHT)<br>Ling-Chih Kao (Chunghwa Telecom, CHT)<br>Daniele Munaretto (ATH)<br>Daniele Ronzani (ATH)<br>Marco Centenaro (ATH)<br>Jack Shi-Jie Luo (ITRI)<br>Tzu-Ya Wang (III) |
| **Dissemination Level:** | Public |
| **Contractual Date of Delivery:** | 30.04.2020 |
| **Work Package** | WP2 |
| **File Name:** | 861459-5G CONNI-D2.1-Intermediate Report on Private 5G Network Architecture-v1.0.docx |

# Revision History

| Version | Date | Comment |
|---|---|---|
| 0.1 | 15.05.2020 | Input from CHT to sections 2.1.4 and 2.2.4, Input from HHI to section 2.2.1 |
| 0.2 | 26.05.2020 | Input from ITRI to section 2.2.1<br>Input from III to section 2.2.3<br>Input from BOSCH to sections 2.1 & 2.2 |
| 0.3 | 19.06.2020 | Update from CHT to section 2.1.4<br>Input from BOSCH to sections 2.1.1-3 & 2.2.5<br>Update from HHI to section 2.2.1 |
| 0.4 | 02.07.2020 | Input from ATH to sections 2.2.2 & 2.2.3 |
| 0.5 | 16.07.2020 | Input from ATH to section 3<br>Input from CHT to section 3.5 |
| 0.6 | 27.07.2020 | Input from CHT to section 3.5.4 |
| 0.7 | 17.08.2020 | Extended Sec. 2.2<br>Adjusted Sec. 3 according to discussion |
| 0.8 | 21.08.2020 | BOSCH input to Sections 2.2.2, 2.2.6, 2.2.8, 3.1.3, 3.1.4<br>CHT Input to Sections 2.2.5, 2.2.6, 3.2.4, 3.4.1, 3.4.4<br>ATH input to Sections 2.1.4, 2.2.2, 2.2.3, 3, 3.1, 3.3<br>III input to Section 3.4<br>ITRI input to Section 3.2 |
| 0.9 | 28.08.2020 | ATH input to Sections 2.2.2, 2.2.3, 2.2.4, 3.1, 3.3<br>CHT input to Sections 2.2.6, 3.2.3, 3.2.4, 3.4<br>ITRI input to Sections 3.2,1, 3.2.2<br>Integrated user stories in Section 2.3 |
| 0.10 | 03.09.2020 | Executive Summary<br>Editorial changes<br>HHI input to Sections 1, 3.1.2, 3.1.3<br>CHT input to Sections 2.1.4, 3.2.2 and 3.2.3<br>ATH input to Sections 3.3.1 and 3.3.2<br>III Input to Section 3.4.2<br>ITRI input to Sections 3.2.2 and 3.2.3 |
| 1.0 | 04.09.2020 | Finalization for submission |
| 1.1 | 19.10.2020 | Additional authors from BOSCH<br>Edits for publication on project website |

# Executive Summary

The document at hand (D2.1) represents the intermediate results of Work Package 2 “Private 5G Networks: Architecture & Operator Models”. In conjunction with D1.1 “Report on Use Cases & Requirements”, it serves as the basis for the planning, research and implementation activities of Work Packages 3 – 5. In contrast to D1.1, it focuses on the impact exerted by different system architecture choices on the stakeholders involved in the private 5G network. To that end, a more detailed discussion of the involved stakeholders and their roles is conducted. On the enterprise side this include the end users, IT department and owner of premises, which depending on size and structure of the enterprise might have different degrees of exposure to the 5G network. On the other hand there are third party service providers, including traditional mobile network operators. Next, the different ownership and governance dimensions, comprising spectrum, RAN, core and transport networks, subscriber data, edge computing and applications as well as network OAM, which may be distributed among these stakeholders are explored. These general considerations are concluded by a set of user stories describing typical interactions of involved stakeholders with the network beyond the more general requirements of D1.1.

Based on this framework, four different architectural models are taken into consideration and characterized. The models included in this document are

1. Fully Private Infrastructure
2. MVNO Model
3. Hybrid Model
4. MNO’s Private Core Network.

This will be used as the basis for the definition of the final 5G CONNI demonstrator architecture.

# Table of Contents

# List of Figures

# List of Acronyms

| | |
|---|---|
| **3GPP** | 3rd Generation Partnership Project |
| **5G CONNI** | 5G for Connected Industries |
| **AMF** | Access and mobility management function |
| **AUSF** | Authentication server function |
| **AWS** | Amazon Web Services |
| **BNetzA** | Bundesnetzagentur (German regulator) |
| **BSS** | Business support system |
| **CAPEX** | Capital expenditure |
| **CBRS** | Citizens broadband radio service |
| **CBSD** | Citizens broadband radio service device |
| **CN** | Core network |
| **CSP** | Communication service provider |
| **DECOR** | Dedicated core network |
| **DL** | Downlink |
| **eMBMS** | Evolved Multimedia Broadcast Multicast Service |
| **eSIM** | Embedded subscriber identity module |
| **ETSI** | European Telecommunications Standards Institute |
| **eUICC** | Embedded universal integrated circuit card |
| **FCC** | Federal Communications Commission (USA regulator) |
| **GAA** | General authorized access |
| **IMSI** | International Mobile Subscriber Identity |
| **IP** | Internet Protocol |
| **I-UPF** | Intermediate use plane function |
| **LTE** | Long Term Evolution |
| **MANO** | Management and orchestration |
| **MCX** | Mission critical service |
| **MEC** | Multi-access edge computing |
| **MNO** | Mobile network operator |
| **MOCN** | Multi operator core network |
| **MPLS** | Multiprotocol label switching |
| **MVNO** | Mobile virtual network operator |
| **NAS** | Non-access stratum |
| **NAT** | Network address translation |
| **NB-IoT** | Narrowband Internet of Things |
| **NCC** | National Communications Commission (Taiwanese regulator) |
| **NFV** | Network function virtualization |
| **NG-RAN** | Next generation radio access network |
| **NPN** | Non-public network |
| **OAM** | Operation, Administration and Maintenenance |
| **OPEX** | Operational expenditure |
| **OSS** | Operation support system |
| **PAL** | Priority access license |
| **PLMN** | Public land mobile network |

| | |
|---|---|
| **PNI** | Public network integrated |
| **PSA** | PDU session anchor |
| **PTT** | Push-to-talk |
| **QoS** | Quality of service |
| **RAN** | Radio access network |
| **SAS** | Spectrum access server |
| **SIM** | Subscribed identity module |
| **SINR** | Signal to interference and noise ratio |
| **SLA** | Service level agreement |
| **SMF** | Sessions management function |
| **SNPN** | Standalone non-public network |
| **SUPI** | Subscriber permanent identifier |
| **TDD** | Time division duplex |
| **UDM** | Unified data management |
| **UE** | User equipment |
| **UICC** | Universal integrated circuit card |
| **UL** | Uplink |
| **UPF** | User plane function |
| **USIM** | Universal subscriber identity module |
| **VLAN** | Virtual local area network |
| **VRF** | Virtual routing and forwarding |
| **WAN** | Wide area network |

# 1 Introduction

A central aspect of the 5G CONNI approach to industrial wireless networking is the notion of private 5G networks. While these networks will built upon the technologies developed over the past years of 5G system research and standardization in areas such as radio access, core and transport networks as well as edge and cloud computing, they bring along a shift in the traditional ownership and governance structures of mobile radio networks dominated by monolithic operator organizations. With more stakeholder involved in the deployment, operation and usage of the network and each network component possibly owned and governed by a different party with its own business model, private 5G networks open up a larger space of possible deployment and architectural options. These options directly impact a multitude of factors that may guide an enterprises choice for one of them. The more prominent among them are the associated costs, confidentiality and security issues and organizational effort. In the design of an industrial private 5G network it is therefore prudent to first carry out an analysis of different architectural choices with respect to these factors.

Comprising one European and one Taiwanese site, the 5G CONNI demonstrator offers the opportunity to realize different architecture options and assess their suitability for the identified use cases and demonstration scenarios. With the additional option for a global interconnection of both sites, requirements of larger enterprises may also be evaluated in the end-to-end deployment. To facilitate the choice of final architecture for the demonstrator, a selection of appropriate options has to be reviewed first.

## 1.1 Scope

This deliverable is a result of Work Package 2 “Private 5G Networks: Architecture & Operator Models” and provides an overview and discussion of different system architecture options suitable for private 5G networks in industrial applications. Thus, in conjunction with the results from Work Package 1 “Use Cases & Requirements”, it will serve as the basis for the selection of an appropriate architecture for the international 5G CONNI end-to-end industrial 5G demonstrator. The deliverable puts emphasis on ownership and governance aspects of the overall system architecture, highlighting their impact on the different stakeholders involved in private 5G network deployment and operation. Based on the current state of the art in 5G standardization, the different ownership and governance dimensions of private 5G networks are discussed, leading to four different architecture models characterized by different distribution thereof among the stakeholders.

## 1.2 Structure

This document is structured as follows: Section 2 discusses general design considerations for private 5G networks. To that end, the involved stakeholders and their respective roles with respect to the 5G system are identified first. Then, the different dimensions of 5G network ownership and governance which will be key for the assessment of different architectural choices are characterized. This provides a broad view of the entire system, covering network and application infrastructure components as well as subscriber data and spectrum aspects. Finally, a set of common interactions with the private 5G system and the involved stakeholders is presented in the form of user stories that provide a more detailed view than the general requirements identified in 5G CONNI D1.1. Section 3 then presents four selected options for the overall private 5G system architecture and discusses them with respect to the distribution of ownership and governance of the identified system dimensions among the stakeholders.

# 2 Design Considerations for Private 5G Networks

## 2.1 Stakeholders and Roles

### 2.1.1 Owner of Premises

The owners or managers of the premises, such as factories, are responsible for the long-term innovation, efficiency and profitability of their operations. For factories, production efficiency needs a steady improvement, while costs have to be kept reasonably low. Therefore, investments a factory owner takes in new technology in general, and in IT infrastructure such as a private 5G network in particular, are required to be well justified, for example, in terms of a return-on-investment calculation, which requires to be positive in a relatively short time. Here, the combination of different use cases, which ideally scale in the actual benefits they bring to the factory, appears to be the key instead of a single one, while such a combination is highly dependent on the types of factory and production.

While the monetary benefits of 5G use cases can be derived from improvements in production efficiency, the investment – taken by the premises owners – into the 5G technology for a factory strongly depends on deployment and operation models and strategies of the 5G network. However, financial and efficiency goals are not the sole performance metrics that need explicit consideration. Data confidentiality, IT security and safety regulations have to be obeyed to, which likely will have an impact on the chosen deployment and operation model.

Another important aspect is the exploitation of scaling effects of centralized operation and management of multiple 5G access networks at different sites of the same corporation. Here, leveraging reduced management overhead for a central team to manage and operate 5G networks across multiple sites on the one hand, and minimal installation effort of the 5G Core network on the other, plays a crucial role in terms of cost efficiency, and hence the decision by the premises owners.

### 2.1.2 Enterprise IT Management Teams

In large enterprises, dedicated teams are set up to centrally and decentrally manage IT systems, which can span the entire globe if such a company is operating worldwide. For manufacturing companies, the IT system needs strong protection against various threats, internal and external ones, in particular within the manufacturing IT domain. Often, the manufacturing IT system is encapsulated within the enterprise IT system, with strong separation of logical network domains, and therefore a separation of management tasks and responsibilities. Therefore, one can distinguish between the manufacturing IT system management and the enterprise IT system management, both exhibiting different regulation and governance aspects.

While the responsibilities for managing and operating standalone non-public networks (SNPNs), i.e. without an external mobile network operator (MNO), are shared corporation-internally between the stakeholders of manufacturing and enterprise IT management, the operation models for private networks (partially) operated by MNOs or by mobile virtual network operators (e.g. Public Network Integrated(PNI)-NPN) demand for more sophisticated solutions regarding shared responsibilities, joint network management from a technical perspective and service-level agreements (SLAs). Another aspect related to SLAs is the question of responsibility for the availability, confidentiality and integrity of user plane and control plane traffic that is routed through wide area networks (WANs) in scenarios with external network operators and/or with multiple 5G RAN sites. Especially, if the WAN is managed and governed by a third party, which is neither the enterprise IT department nor the M(V)NO, responsibility sharing and SLAs can become even more complex and more advanced mechanisms for fault management and monitoring need to be employed.

### 2.1.3 Users / Subscribers

In a factory environment, such as a shop floor, the user of the technology is usually the factory personnel. Factory personnel include machine builders, machine operators, local manufacturing IT management personnel, logistics workers, and others. Factory personnel are generally concerned with the smooth operation of production processes and that material flow is timely, which includes short lead times, short planned maintenance times and minimized unplanned maintenance, to name a few. In this regard, factory personnel are not concerned with the proper functioning of the underlying IT infrastructure per se, as long as it serves the purpose of communication foundation for the applications. Nevertheless, factory personnel will interact with 5G user equipment and the 5G network in indirect and perhaps direct ways. In regard to such interactions, configuration tasks, such as onboarding of user equipment, should be as easy as possible hiding much of the complex nature of cellular networks and their management.

### 2.1.4 Service Provider

The advantages of service providers can provide services for building private 5G networks through years of network experiences, including security, operation, deployment, maintenance, and recovery. The services what service providers could provide to enterprises can be divided into 5 categories:

1. **Radio & Core Services:** service providers for private 5G networks can provide network deployment, including radio and core. The radio can use licensed spectrum from telecom operators. Although each supplier follows the 3GPP standard development, there are still differences between different suppliers. The service provider can provide verification and adjustment services of such differences.
2. **Cloud Services:** it mainly emphasizes the characteristics of large bandwidth, low latency, and massive connectivity in 5G, so edge computing technology services are essential. Cloud services that service providers provide include edge cloud and multi-access edge computing (MEC). Furthermore, it can be divided into dedicated MEC and sharing edge cloud for enterprises.
3. **Management Service: t**he management services include design and install network components, monitor status and report problem, SIM provision and management, and cloud and application service management. The network must be continued to plan, optimize, maintain and upgrade, so it needs to allocate considerable human and material resources. Enterprises can reduce the cost of independent management through the experience of telecom operators.
4. **IoT Services:** the operators can provide IoT SIMs, IoT sensors and industrial products that combined with the third party. It also provided the management platform or gateway that supports self-management functions for IoT devices of enterprises such as connection status, abnormal notification, service content adjustment, etc. to improve maintenance efficiency.
5. **Security Services**: Service providers provide and meet the needs of most vertical domain application quickly because of the ultra-dense network coverage and security management of service operators. Security already has quite strict regulations in the telecom industry. If the vertical industry wants to build its own proprietary network, they must think about designing and building secure networks to resist attacks from all parties.

Some network services are provided by other external service providers such as Amazon Web Service (AWS), Google Cloud, and Microsoft Azure. Some enterprises already use the external platform to build their industrial applications. If they change the platform, they will spend a lot of costs. They still want to develop their applications in private 5G network so that telecom

operators could cooperate with cloud platform vendors. Cloud platform vendors build their edge platform on telco edge networks. The cloud platform can combine with the 5G technique to provide 5G network services which can also offer more analytics options resources in the public cloud.

As service providers, the mobile networks operators offer 4 deployment scenarios of private 5G networks, as shown in Figure 1. The first type is dedicated RAN and edge cloud sharing. The second type is dedicated RAN and dedicated MEC, the third type is dedicated private 5G network and the fourth type is RAN and Edge/Core Cloud Sharing. Enterprise can use the spectrum from its own and the operator's licensed spectrum, depending on the governance – see Sec. 2.2.1.

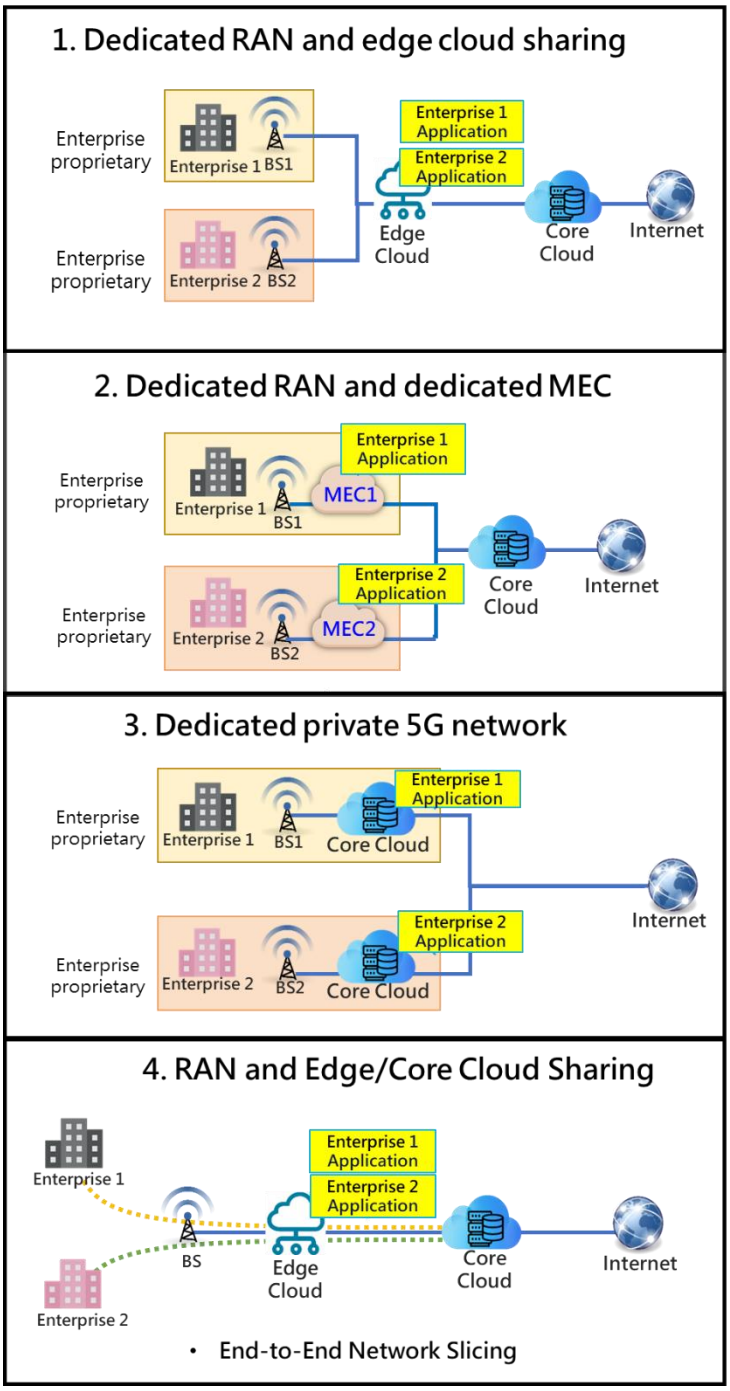


*Figure 1: 4 deployment scenarios of private 5G networks*

1. Dedicated RAN and edge cloud sharing

As shown in above Figure 1-(1), base stations are built in the enterprise, thus they are physically separated from the public network. The applications of enterprises are deployed in operator's edge cloud, which is shared between private and public networks. The edge cloud and core cloud resources are shared among enterprises. This solution can save enterprise construction and maintenance costs. However, it could lead to higher communication delay and variability, since the data needs to be returned to the enterprise's internal network through the edge cloud.

2. Dedicated RAN and dedicated MEC are built in the enterprise

Base stations and MEC are built in the enterprise, and core cloud resources are shared between private and public network, as shown in Figure 1-(2). The applications of enterprises are deployed in on-premise MEC. The advantages of this case are lower latency and keeping important data within the company. This solution distinguishes the internal and external areas of the enterprise through a dedicated base station. It is convenient to use the same SIM card between private and public network.

3. Dedicated private 5G network

As shown in above Figure 1-(3), base stations, core cloud and applications are all built in the enterprise. The advantage of this solution is the higher security because of the full set solution in the enterprise. Nevertheless, this can be a costly strategy. Due to the possible expenditure of network components, maintenance and software licenses.

4. RAN and Edge/Core Cloud Sharing

The end-to-end network slicing, shown in Figure 1-(4), logically separates base station, edge cloud and core cloud. The physical network is divided into multiple virtual logical networks, where each virtual network serves a different enterprise. The advantages of this solution are low cost and maintenance and scalability, at a cost of higher latency and variability than case (2).

As described above in the four deployment scenarios, the complexity of maintenance for enterprises has to be considered. Some enterprises do not have the excellent ability at network processing, but they want to ensure that their applications or production lines are continuous operation. The complexity of dedicated private 5G network scenario (Fig. 1-(3)) is highest because the enterprise will build their own RAN and core network. Instead, the solutions (1) and (2) are less complex to set up. These two deployment scenarios serve more enterprises and the applications may be set up in the edge site. Dedicated RAN and dedicated MEC are built in the enterprise, guaranteeing all traffic data and applications kept inside the premise site.

The continuous operation for factories is essential. It will cause considerable losses to the enterprise if the production line is stopped. The service provider usually provides two models for the reliability of the private 5G network. One is an active-standby model, and another is an active-active model. These two models can ensure the services continuous operation even though the service provider consider to update the software and hardware. It depends on the requirements of enterprise which are discussed in detail by service providers and enterprises to choose the appropriate models.

## 2.2 Dimensions of 5G Network Ownership & Governance

### 2.2.1 Spectrum

The electromagnetic spectrum is, for most parts, not a free resource, but in fact allocated and regulated into frequency bands by government bodies. Some of these frequency bands are unlicensed, which means that anyone who wants to use the spectrum can do so, such as for Wi-Fi. Most of the spectrum however is licensed, which means that the license holder is the only authorized user of that spectrum range. Although the allocation and regulation of frequency bands is done on a per-country basis, because radio propagation does not stop at national borders, the regulatory bodies have sought to harmonize the allocation of frequency bands.

The spectrum of interest for 5G networks can be divided into three categories- low, medium, and high frequencies. Low frequencies cover sub-2 GHz which is useful for wider coverage but limit the option to use MIMO due to the large wavelengths below 1 GHz. Medium frequencies include 3 - 6 GHz which offers a good tradeoff between coverage and capacity. The highest interest globally is in the range 3300 - 4200 MHz. High frequencies above 6 GHz will be best suited for hotspot coverage with extremely high data rate required. The focus will be in the mm-wave range above 24 GHz.

Most of the frequency bands that are designated for mobile communication networks, including 5G, are divided into individual sub-bands that are then auctioned off to users, mostly service providers, at great cost. This high financial obstacle makes it unfeasible for most potential users of private 5G networks to acquire their own part of the spectrum and suggests the use of 5G in unlicensed spectrum. But, as these frequencies can be used by anyone, at any time, it is impossible to guarantee any kind of quality of service or latency. In an industrial setting, this is just not acceptable.

Fortunately, several countries have started the process of opening allocated spectrum as licensed shared spectrum or dynamic spectrum sharing for local use in specific bands that enable the deployment of private 5G networks.

#### *2.2.1.1 Spectrum allocation models for private 5G network*

##### 2.2.1.1.1 Licensed shared operation

Several European countries, including Germany and the UK, have started the process of allocating parts of the 5G spectrum for local use to industries. Non-service providers can apply for a license for up to 100 MHz of spectrum in the 3.7 to 4.2 GHz band. For a small (yearly) fee, companies can then use those frequencies exclusively on their premises to deploy a private 5G network.

Taiwan’s NCC (National Communications Commission) is taking action to make additional spectrum available for 5G services which is shown in Figure 1. The first release of 5G spectrum was concluded early this year followed by the second stage in 2022. In order to promote the 5G vertical industries in Taiwan, up to 100 MHz of the spectrum are allocated for local private networks instead of nationwide coverage. To this end, field owners are encouraged to apply for a license to deploy the end-to-end 5G network in the range 4.8GHz - 4.9GHz. Similar to the approach of European countries, field owners have to pay the frequency-usage fee and allowed exclusive use of spectrum on their premises. 1

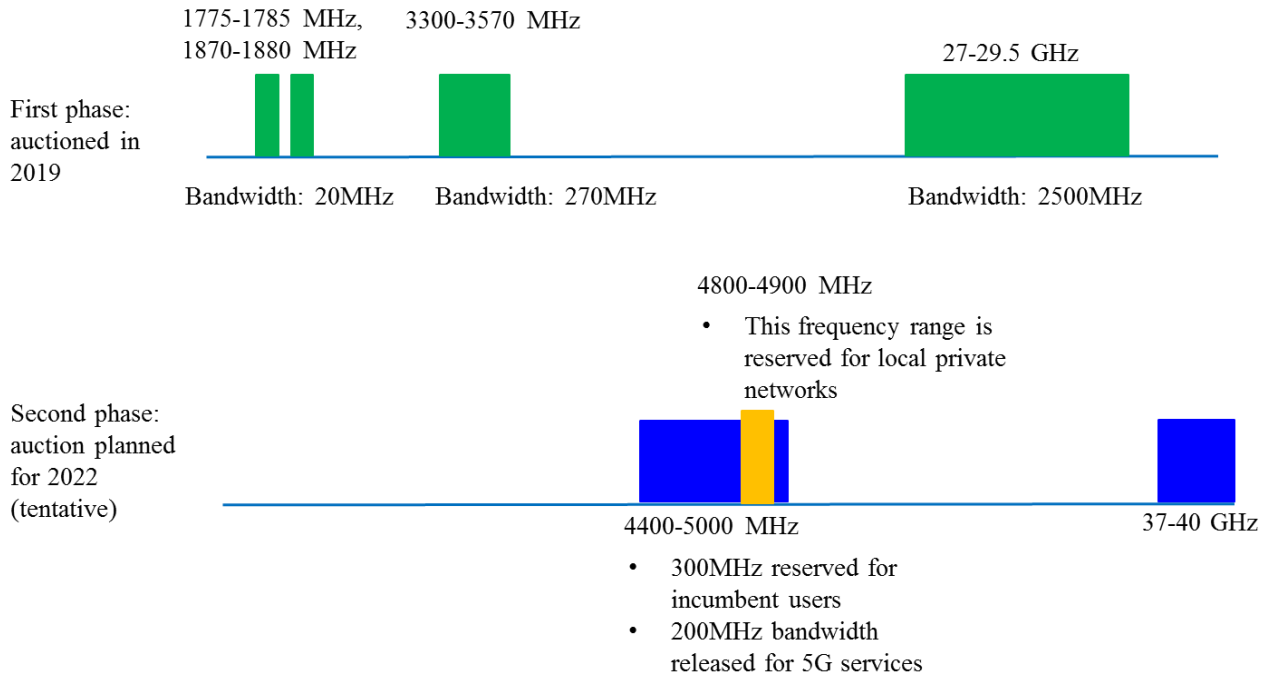


*Figure 1: Spectrum for 5G services in Taiwan*

Other than the spectrum used by public land mobile networks (PLMNs), locally licensed shared spectrum will likely result in a high fragmentation of the geographical areas covered by the individual licenses. Thus, multiple networks, generally operated by different entities, in close geographical proximity to each other will be required to share the same spectrum. The licensed shared spectrum model requires a close coordination between the operators of neighboring networks or the respective license holders for these networks in order to minimize interference. The first approach to this is a joint optimization of coverage areas by appropriate choice of base station placement, antenna type and orientation or transmit power. If not already done by the regulator, partitioning of the allocated spectrum is another measure for interference coordination. Especially for networks operating in Time Division Duplex (TDD) mode, which will be the case for most 3GPP based 5G networks, frequency and phase synchronization of adjacent (both geographically and spectrally) networks is critical.

Although intra-network self-organization technology is already commonly used by mobile network operators today, no such solution for inter-network coordination of SNPNs has been generally agreed upon as of today, requiring manual planning and optimization.

Due to the importance of interference coordination, corresponding regulations and restrictions will apply to the spectrum licenses issued. However, with the licensed shared spectrum model being a new approach for most countries choosing to adopt it, there is no international harmonization of these regulations yet.

As an example, the German regulator BNetzA requires applicants for local licenses to negotiate coordination agreements with other (prospective) licensees in the immediate geographical vicinity and include them in their application. If applicants fail to meet this requirement, a default field strength limit will apply at the edge of the licensed area in order to minimize interference risk, likely creating suboptimal constraints on the network deployment. The specific nature of the coordination or possible technical solutions are not covered by the regulations, putting an additional burden on the licensee.

#### 2.2.1.1.2 Dynamic spectrum sharing (CBRS)

In the US, the 3.5 GHz frequency band was recently opened up for commercial use by the FCC (US Federal Communications Commission). This band is now part of the Citizens Broadband Radio Service (CBRS) and does not necessarily require spectrum licenses. Access and operation is governed by a dynamic spectrum access system, but the users will be required to take care not to interfere with others already using nearby bands.

The 3.5 GHz band was traditionally not licensed to wireless operators as it had several incumbent users like the US Navy and was used for naval radar applications and fixed satellite services. The typical utilization is very low, however, and in many geographical areas there are no incumbent users at all. As a result, access to this part of the spectrum was opened up through CBRS in a three-tier model.

Tier 1 access is restricted to the original incumbent users of the spectrum and must be protected from interference at any given location and time. To facilitate this, a cloud-based Spectrum Access Server (SAS) is responsible for managing Tier 2 and 3 users. While access to the third tier (General Authorized Access, GAA) is unlicensed, enterprises can apply for a prioritized access to the spectrum by acquiring a license to the second tier (Priority Access License, PAL) at auction.

Base stations operating in the CBRS band are called Citizens Broadband Radio Service Devices (CBSD). Whenever a CBSD is turned on, it must immediately connect to the SAS and provide it with its coordinates and a globally unique identifier. The SAS then provides the CBSD with a list of CBRS channels available at the CBSD location. Whenever higher priority access to the spectrum is demanded either by an incumbent or a higher tier user, the SAS can reconfigure the CBSD and reassign it to another part of the CBRS spectrum within a timeframe of five minutes. By well designing the network infrastructure, the impact of this channel reassignment can be minimized.

### 2.2.2 SIM

The Subscriber Identity Module (SIM) is a fundamental element of the cellular system, because it allows to authenticate the validity of a terminal as it tries to access the network. It contains the unique identifier of the subscriber (that is, the International Mobile Subscriber Identity (IMSI) or the Subscription Permanent Identified (SUPI) for 4G and 5G systems, respectively) and the related security keys. When a terminal cannot access its home PLMN, its mobile network provider may decide or not, according to the use case, to foster roaming in order to provide a seamless network coverage for the user device without changing the SIM card. In particular, in 5G systems the SIM card is capable of supporting seamless global roaming by using the Steering of Roaming (SoR) procedure, which can deal with the parameters like operator controlled PLMN in order to provide roaming service.

In the context of private 5G networks, the SIM cards are typically issued to each user equipment by the stakeholder involved in the management of the core network – see Sec. 2.2.4.

**eSIM**

An embedded-SIM (eSIM) or embedded universal integrated circuit card (eUICC) is a form of programmable SIM card that is embedded directly into a device. eSIM is a global specification by the GSMA which enables remote SIM provisioning of any mobile device. eSIM allows consumers to store multiple operator profiles on a device simultaneously, and switch between them remotely, though only one can be used at a time. Remote SIM provisioning implies that much smaller devices can be supported, which is quite appealing for machine-type devices for the Industry 4.0.

eSIM is the only globally-backed remote SIM specification for consumer devices. This universal approach will grow the Internet of Things by allowing manufacturers to build a new range of products for global deployment based on this common embedded SIM architecture. In this context, the 5G CONNI project will investigate during its lifetime the opportunity of testing such advanced technology for the smart industry, along with the deployment of standard consumers SIM cards.

### 2.2.3 RAN

The Radio Access Network is for many aspects the most important asset in a mobile system as its deployment and interconnection is subject not only to coverage and KPI requirements but also to a number of constraints imposed by the regulator, the real estate market and the telco market.

In fact, the radio coverage design has to take into account the SINR caused by incumbent RAN deployments, the maximum radiated power allowed in that region, the availability of sites to install the equipment and the resulting CAPEX and OPEX.

In order to reduce costs, RAN sharing models have been explored, allowing different PLMNs to be supported by the same RAN system.

National roaming and MVNO enable a communication service provider to deliver the service in a region even if it doesn't have a RAN system there.

Dedicated Core networks (DECOR) and network slicing technologies enable a mobile communication service to private subjects when the latter do not have a mobile system at all.

Yet another RAN-sharing model is the so-called neutral host, in which the RAN infrastructure does not belong to any of the MNOs whose PLMNs are supported by such infrastructure, and the infrastructure owner announces its own private PLMN too. This is an architecture defined by the MulteFire and CBRS Alliances, and targets tower companies which are enabled to be service providers too.

The stakeholders involved in the RAN ownership and governance are quite heterogeneous:

- The MNO
- MVNOs and Roaming MNOs
- Equipment and service providers
- The tower companies (especially for macro cells and outdoor coverage)
- Building management companies (both for indoor and outdoor coverage)
- The national regulator
- Local administrations

### 2.2.4 Core

The Core Network (CN) enables mobile devices authentication, connection establishment, and ultimately data and voice traffic delivery to the intended destination. These tasks are performed by distinct network functions such as:

- The User Plane Function (UPF), which routes user-plane traffic coming from/sent to the terminal;
- The Session Management Function (SMF), which configures the traffic steering at the UPF;
- The Authentication Server Function (AUSF) and Unified Data Management (UDM), which are responsible to authenticate the users;

- The Access and Mobility Management Function (AMF), which tracks the user mobility pattern, interacting with the SMF and the AUSF.

Similarly to the RAN, the CN does not necessarily belong to the stakeholder that defines which subscribers and devices are enabled for the 5G communication service. In fact, this organization may use the mobile network offered by a traditional MNO or by an equipment/service provider *as a service*, so that even the subscriber management is delegated to a third party; technologies such as dedicated core network (DECOR) and network slicing enable this scenario. Nevertheless, such organization is still responsible for the administration and provisioning of the subscribers' database, including their service profile, and to distribute and configure the physical SIM cards or eSIM to the users. The AUSF/UDM are then responsible for authenticating the device exploiting the information contained in its SIM card, such as the IMSI/SUPI and relative keys (like the op and ki values). In other cases, however, the main stakeholder may own the entire core network, or also act as an MVNO, owning only a few core network functions. As a consequence, depending on the specific case, the SIM cards may be issued by the private 5G network provider or by the mobile network operator.

The stakeholders involved in the CN ownership and governance usually are:

- The MNO
- MVNOs and roaming MNOs
- Equipment and service providers
- Resellers and channel partners of the equipment and service providers.

### 2.2.5 MEC Platform

The purpose of the edge computing platform is to carry applications and connect telecom operators' network equipment, and thus telecom operators usually own the edge computing platform. Owners of the edge computing platform must maintain the network connectivity and assist in generating applications of the platform. The generation method of applications is generally based on the ETSI NFV MANO. Besides, they also need to ensure that the user's packets are transmitted to correct applications and target terminals.

The owner of the edge computing platform is telecom operators, so they have to manage the operation and performance of the device on the platform and consider the overall transmission security of the network between devices. Edge computing platform must be regarded as the appropriate amount of resources to generate devices for achieving the maximum resource usage. Besides, it also needs to consider the traffic steering among devices. In the process of data routing, the telecom operator is responsible for the network routing of the edge computing platform outside applications, sending data to the target applications, and processing the data completed by applications to target users.

In addition to the typical scenarios mentioned above, non-network-related enterprises can also obtain the edge computing platform through buyouts or leases and then installing the applications on the platform. In this case, the platform that telecom assist in building, which is according to the requirements of enterprises, so they are a cooperative relationship. The enterprise is responsible for the cost of establishing the edge computing platform and the requirements to configure the edge computing platform. The telecom operator is in charge of the establishment of network connectivity, network transmission security, application onboarding functions, and transmission performance according to the requirements of enterprises.

### 2.2.6 Applications

There exists a plethora of different applications, which can be offloaded to a MEC platform. In the industrial domain, such applications range from simple data collection and database systems to control logic functions of controllers to more complex systems, such as manufacturing execution systems or even enterprise resource planning software. Depending on the type of the application, the MEC platform is either deeply integrated with the 5G System and located close to a machine or production line, or it provides computing capabilities for a large number of machines, sensors etc. that can even span across multiple factories.

Ownership and governance of the applications is more flexible than that of the edge computing platform because applications can be provided through many suppliers, such as telecom operators, enterprises, or application providers, and each of them may manage their respective applications individually. In terms of application ownership, no matter who owns these applications, all of them still need to maintain the basic network connectivity, data security, and resource utilization. The purpose of network connectivity is to ensure that the user's packets can be sent to the target application or terminal correctly and sequentially. Data security is about the confidentiality, integrity, and reliability of data from users. Resource utilization is considered to maximize the effectiveness of the applications.

When the owners of applications are telecom operators, they can lease these applications to the enterprises. The telecom operators can provide various applications, such as network speed bonuses applications, highly secure transmission applications, and customized applications. These applications can be shared between different enterprises, but it will be determined based on the confidentiality of the applications. In addition to the above basic maintenance, telecom operators also have to maintain the stability, processing efficiency, and data security of the applications. When the application ownership is a network-related enterprise such as Amazon and Google Cloud, enterprises can lease applications from these network-related enterprises to meet their network service requirements. In this case, the network connectivity will be responsible for the telecom operators and network-related enterprise, and the responsibility of the data security is the same as the network connectivity. In terms of resource utilization, the network-related companies have to maintain it through themselves, because those applications belong to them. In addition, they are responsible for maintaining the stability, processing efficiency and data security of the application. When the application ownership is the application provider, and these applications can be leased to any enterprise. In this situation, data security is maintained by the telecom operators and the application provider, but the network connection is still managed by the telecom operators. In terms of resource utilization, the enterprises that lease the applications are responsible for them. Finally, application providers are also responsible for managing application stability, processing efficiency, and data security.

From a manufacturing company point of view, nearly all application data and all related information processed by such applications contain confidential information that are essential for the success of the business and the competitive operation of the company’s factories. Because any leakage of such data to a third party or even an attacker can directly or indirectly lead to a substantial loss of intellectual property and business-essential information, which can ultimately result in economic and reputational damages, the manufacturing company must in any case have ownership of and governance over this data. Moreover, this has strong implications on secure integration and operation of MEC platforms, on which manufacturing-related applications are running. In particular, if the MEC platform, which is used to process critical production data and other related information is not owned or governed by the enterprise itself, e.g. by an MNO instead, corresponding contractual frameworks, for example, in the form of service-level agreements, need to be installed that allow for a compensation of any damage, which

occurs through the loss, leakage or unwanted modification of the affected information, and which is in the responsibility of the owner of the MEC platform.

### 2.2.7 Transport Network

The ownership, governance and management of the transport network, such as a wide area network (WAN), can be crucial aspects for the operation of private 5G networks. An enterprise backbone WAN can be owned and operated by the same enterprise but it can also be owned and managed by one or multiple third parties, which are neither the enterprise nor the M(V)NO. There exist two cases, in which some specific challenges arise because the backbone network needs to be utilized to transfer signaling, operation and management data or even user data:

(1) The enterprise wants to set up a 5G access network at one site, which is operated by an M(V)NO and where no direct connection between the site's IT infrastructure and the M(V)NO provider network exists, because establishing such a direct connection would be too costly, for instance, and
(2) The enterprise wants to set up more than one 5G access network at multiple geographically distributed sites, which are centrally operated by either the enterprise itself or by an M(V)NO[1].

In both cases, the M(V)NO can operate the 5G access network by accessing and utilizing the enterprise's backbone network, which is either a dedicated (non-public) network infrastructure, e.g. realized as Multiprotocol Label Switching Virtual Routing and Forwarding (MPLS VRF), or a tunneled overlay network in the public Internet, via network transfer points. Nevertheless, such a network transfer point must not necessarily be geographically located close to where the 5G access needs to be provided. In contrast, such a network transfer point can be several 100 km apart from the actual site and therefore has a clear impact on the deployment strategy and the 5G architecture and topology.

In either case, the enterprise needs to provide a secure connection through the transport network between the network transfer points and the 5G sites, for which a number of requirements need to be adhered to, including

(1) The IT security concept of the enterprise for secure access by externals,
(2) The IT security concept of the M(V)NO for securely accessing local, third-party infrastructure, and
(3) Data and integrity protection requirements on the transferred information.

While, from a technical perspective (data confidentiality), the ownership of the transport network reduces to the challenges explained above, additional complexity arises from an availability and SLA viewpoint. For example, a private 5G network operated by an M(V)NO relies on the availability of the WAN operated by a third party and any SLA between the M(V)NO and the enterprise must take into account the responsibility for the available WAN connection, which is shared between the enterprise and the third party that governs the WAN. In this regard, additional mechanisms for fault management must be employed. Because ownership and governance of the transport network have an impact on the design of SLAs and, hence, are clear cost factors, these aspects strongly influence the appropriate 5G architecture, including the distribution of critical and non-critical 5G network functions, redundancy concepts and fall back mechanisms in case the transport network becomes unavailable.

[1] If the different 5G access networks are operated by an M(V)NO, access to the enterprise backbone is can be required due to cost or convergence reasons.

### 2.2.8 OAM System

Network operation and management systems, such as the operation support system (OSS) and the business support system (BSS), are complex applications that are required for a proper network configuration, operation and management, and for billing of customers (subscribers). In the classical carrier business, the OSS and BSS is owned and used by the MNO to carry out the respective tasks. In light of the developments around private 5G networks and local, private spectrum, a number of other stakeholders can own and use the network management tools and, therefore, would also be responsible for all legal, technical and operational consequences. Owners can, in particular, be any other service provider, who is not an M(V)NO or even the enterprise, for which a private network is planned. Especially in the latter case, the OAM system can be located and run in the enterprise data center or inside the plant' data center, so that also O&M traffic essentially stays inside the corporate network and can be easily protected by security mechanisms according to enterprise-specific security regulations.

## 2.3 Interactions with the Private 5G Network

To facilitate assessment of the impact of a given architecture choice for the private 5G network on the involved stakeholders, in this section a number of typical interactions with the 5G system is presented in the form of user stories. For each user story, a preliminary classification of the affected stakeholders is made, distinguishing between a fully private deployment model for the 5G system (see Sec. 3.1) and deployment models in which at least part of the infrastructure is provided as a service by another party ("Network-as-a-service", see Secs. 3.2ff.)

### 2.3.1 Initial Setup of End Devices and Network

| *Action:* | **Order and deploy SIM card, eSIM, etc.** | |
|---|---|---|
| *Rationale / Objective:* | A UE requires a SIM/eSIM to become operational and user wants to equip UE with SIM/eSIM | |
| *Preconditions:* | UE is not provided a SIM/eSIM | |
| *Outcome:* | SIM/eSIM deployed | |
| *Provisioning model:* | **Fully private 5G network** | **Network-as-a-Service** |
| *Involved Stakeholder(s):* | User (factory personnel), Service provider or Enterprise IT department | User (factory personnel), Service provider |

| *Action:* | **Onboard / Register UE** | |
|---|---|---|
| *Rationale / Objective:* | UE needs to be registered for the first time in the 5G network; user requests to onboard UE for the first time | |
| *Preconditions:* | UE is provided with SIM/eSIM an now needs to be onboarded for the first time with the 5G network | |
| *Outcome:* | UE is onboarded and ready to be used | |
| *Provisioning model:* | **Fully private 5G network** | **Network-as-a-Service** |
| *Involved Stakeholder(s):* | User (factory personnel), Enterprise IT department | User (factory personnel), Service provider |

| *Action:* | **Deboard / Deregister UE** | |
|---|---|---|
| *Rationale / Objective:* | UE will not be used anymore; user requests to remove the UE | |
| *Preconditions:* | UE is onboarded and ready to be used | |
| *Outcome:* | UE is deboarded and cannot be used anymore | |
| *Provisioning model:* | **Fully private 5G network** | **Network-as-a-Service** |
| *Involved Stakeholder(s):* | User (factory personnel), Enterprise IT department | User (factory personnel), Service provider |

| *Action:* | **(Re-)Assign network slice to UE** | |
|---|---|---|
| *Rationale / Objective:* | UE needs to be associated with a network slice or network slice needs to be changed for a UE; user wants that the UE is provisioned with sufficient QoS | |
| *Preconditions:* | UE is associated with no or wrong Network Slice | |
| *Outcome:* | UE is associated with desired Network Slice | |
| *Provisioning model:* | **Fully private 5G network** | **Network-as-a-Service** |
| *Involved Stakeholder(s):* | User (factory personnel), Enterprise IT department | User (factory personnel) or Service provider |

| *Action:* | **Couple 5G network management system with production management system** | |
|---|---|---|
| *Rationale / Objective:* | Network needs access to production information or production management system needs access to communication-related information | |
| *Preconditions:* | 5G network management system is not coupled with a production management system | |
| *Outcome:* | 5G network management and production management systems are coupled and can exchange information through well-defined APIs | |
| *Provisioning model:* | **Fully private 5G network** | **Network-as-a-Service** |
| *Involved Stakeholder(s):* | User (factory personnel), Enterprise IT department | User (factory personnel), Service provider |

| *Action:* | **Decouple 5G network management system from production management system** | |
|---|---|---|
| *Rationale / Objective:* | No information exchange between both systems is required or temporary decoupling is required, e.g. for maintenance purposes or during updates | |
| *Preconditions:* | 5G network management and production management systems are coupled | |
| *Outcome:* | 5G network management and production management systems are decoupled | |
| *Provisioning model:* | **Fully private 5G network** | **Network-as-a-Service** |
| *Involved Stakeholder(s):* | User (factory personnel), Enterprise IT department | User (factory personnel), Service provider |

### 2.3.2 Subscriber Profile Management

| *Action:* | **Add subscriber profile** | |
|---|---|---|
| *Rationale / Objective:* | The user wants to add and initially configure a subscriber profile for a UE the user intends to set up. | |
| *Preconditions:* | No subscriber profile defined for a UE. | |
| *Outcome:* | Initial subscriber profile added. | |
| *Provisioning model:* | **Fully private 5G network** | **Network-as-a-Service** |
| *Involved Stakeholder(s):* | User (factory personnel), Enterprise IT department | User (factory personnel), Enterprise IT department, Service provider |

| | | |
|---|---|---|
| *Action:* | **Modify subscriber profile** | |
| *Rationale / Objective:* | The user wants to modify a subscriber profile for a UE in order to adapt to changes of requirements of the UE on the communication system and to any other relevant changes. | |
| *Preconditions:* | Subscriber profile exists. | |
| *Outcome:* | Subscriber profile modified. | |
| *Provisioning model:* | **Fully private 5G network** | **Network-as-a-Service** |
| *Involved Stakeholder(s):* | User (factory personnel), Enterprise IT department | User (factory personnel), Enterprise IT department, Service provider |

| | | |
|---|---|---|
| *Action:* | **Delete subscriber profile** | |
| *Rationale / Objective:* | The user wants to delete a subscriber profile for a UE, e.g. in the case of deactivation of a UE. | |
| *Preconditions:* | Subscriber profile exists. | |
| *Outcome:* | Subscriber profile deleted. | |
| *Provisioning model:* | **Fully private 5G network** | **Network-as-a-Service** |
| *Involved Stakeholder(s):* | User (factory personnel), Enterprise IT department | User (factory personnel), Enterprise IT department, Service provider |

| | |
|---|---|
| *Action:* | **Add application requirements on the communication system to a subscriber profile** |
| *Rationale / Objective:* | The user wants to add application requirements to the subscriber profile and, based thereon, modify the subscriber profile accordingly. |
| *Preconditions:* | Subscriber profile exists. |
| *Outcome:* | Application requirements are specified for a subscriber profile. |
| *Provisioning model:* | **Fully private 5G network and Network-as-a-Service** |
| *Involved Stakeholder(s):* | User (factory personnel) |

| | | |
|---|---|---|
| *Action:* | **Create backup of subscriber profile** | |
| *Rationale / Objective:* | Create a backup of a subscriber profile, such that it can be recovered in case of an outage etc. | |
| *Preconditions:* | Subscriber profile exists. | |
| *Outcome:* | Backup of subscriber profile is created on a different platform. | |
| *Provisioning model:* | **Fully private 5G network** | **Network-as-a-Service** |
| *Involved Stakeholder(s):* | Enterprise IT department | Service provider |

| | | |
|---|---|---|
| *Action:* | **Recover subscriber profile** | |
| *Rationale / Objective:* | Recover a subscriber profile because the original one is corrupted or unavailable. | |
| *Preconditions:* | Subscriber profile backup exists. | |
| *Outcome:* | Subscriber profile is recovered. | |
| *Provisioning model:* | **Fully private 5G network** | **Network-as-a-Service** |
| *Involved Stakeholder(s):* | Enterprise IT department | Service provider |

| *Action:* | **Migrate subscriber profile** | |
|---|---|---|
| *Rationale / Objective:* | The user wants a subscriber profile to be migrated from one system or location to another, e.g. in the case, where UEs are reused at other locations (factories) and in other networks. | |
| *Preconditions:* | Subscriber profile exists. | |
| *Outcome:* | Subscriber profile is migrated to another system or location. The subscriber profile does not exist anymore in the previous system. | |
| *Provisioning model:* | **Fully private 5G network** | **Network-as-a-Service** |
| *Involved Stakeholder(s):* | User (factory personnel), Enterprise IT department | User (factory personnel), Service provider |

| *Action:* | **Retrieve subscriber management log file** | |
|---|---|---|
| *Rationale / Objective:* | The Enterprise IT department personnel want to review the subscriber management log file to check for unauthorized modifications to subscriber profiles, misconfigurations, SLA and legal purposes. | |
| *Preconditions:* | Subscriber management log file exists. | |
| *Outcome:* | Subscriber management log file is viewed by the Enterprise IT department personnel. | |
| *Provisioning model:* | **Fully private 5G network** | **Network-as-a-Service** |
| *Involved Stakeholder(s):* | Enterprise IT department | Enterprise IT department, Service provider |

| *Action:* | **Couple and activate third-party identity/credential/authentication system** | |
|---|---|---|
| *Rationale / Objective:* | Enterprise IT department personnel want to use, integrate and activate a third-party identity/credential/authentication system, which is natively used in the factory, because such a system can ideally be reused, especially for confidentiality protection reasons. | |
| *Preconditions:* | 5G System is not coupled with a third-party identity/credential/authentication system. 5G System is able to integrate a third-party identity/credential/authentication system. | |
| *Outcome:* | 5G System is coupled with a third-party identity/credential/authentication system. The third-party identity/credential/authentication system is active and ready to be used for 5G UEs. | |
| *Provisioning model:* | **Fully private 5G network** | **Network-as-a-Service** |
| *Involved Stakeholder(s):* | Enterprise IT department | Enterprise IT department, Service provider |

| *Action:* | **Decouple third-party identity/credential/authentication system** | |
|---|---|---|
| *Rationale / Objective:* | Enterprise IT department personnel want to decouple the third-party identity/credential/authentication system from the 5G System. | |
| *Preconditions:* | 5G System is coupled with a third-party identity/credential/authentication system. | |
| *Outcome:* | Third-party identity/credential/authentication system is decoupled from the 5G System. | |
| *Provisioning model:* | **Fully private 5G network** | **Network-as-a-Service** |
| *Involved Stakeholder(s):* | Enterprise IT department | Enterprise IT department, Service provider |

### 2.3.3 Network Slice Management

| *Action:* | **Create a network slice** | |
|---|---|---|
| *Rationale / Objective:* | Factory personnel want sufficient communication resources assigned to a group of subscribers with well-defined requirements on the communication system. | |
| *Preconditions:* | The group of subscribers is not associated with an appropriate network slice and their known requirements do not fit any existing network slice. | |
| *Outcome:* | Network slice that fulfills the subscribers' requirements has been created. | |
| *Provisioning model:* | **Fully private 5G network** | **Network-as-a-Service** |
| *Involved Stakeholder(s):* | User (factory personnel), Enterprise IT department | User (factory personnel), Service provider |

| *Action:* | **Activate network slice** | |
|---|---|---|
| *Rationale / Objective:* | Factory personnel want an existing network slice to be activated in order to for a group of subscribers to become operational. | |
| *Preconditions:* | Network slice exists but is not instantiated. | |
| *Outcome:* | Network slice is instantiated and can be used by the group of subscribers. | |
| *Provisioning model:* | **Fully private 5G network** | **Network-as-a-Service** |
| *Involved Stakeholder(s):* | User (factory personnel), Enterprise IT department | User (factory personnel), Service provider |

| *Action:* | **Modify network slice** | |
|---|---|---|
| *Rationale / Objective:* | The Service provider notices changes in the subscribers' perceived network performance, such that modifications to the network slice becomes necessary. | |
| *Preconditions:* | Network slice is instantiated and modification is deemed necessary. | |
| *Outcome:* | Modifications successfully done to the network slice. | |
| *Provisioning model:* | **Fully private 5G network** | **Network-as-a-Service** |
| *Involved Stakeholder(s):* | User (factory personnel), Enterprise IT department | User (factory personnel), Service provider |

| *Action:* | **Deactivate network slice** | |
|---|---|---|
| *Rationale / Objective:* | The Service provider wants to free unused resources and de-activates a network slice. | |
| *Preconditions:* | Network slice active but is not required anymore by any subscriber of the network | |
| *Outcome:* | Network slice successfully deactivated and resources are freed. | |
| *Provisioning model:* | **Fully private 5G network** | **Network-as-a-Service** |
| *Involved Stakeholder(s):* | User (factory personnel), Enterprise IT department | User (factory personnel), Service provider |

| *Action:* | **Assign priorities to end devices, device groups and services** | |
|---|---|---|
| *Rationale / Objective:* | The factory personnel wants to prioritize devices and services over others in terms of reliability, etc. | |
| *Preconditions:* | | |
| *Outcome:* | Devices or services are prioritized. | |
| *Provisioning model:* | **Fully private 5G network** | **Network-as-a-Service** |
| *Involved Stakeholder(s):* | User (factory personnel), Enterprise IT department | User (factory personnel), Service provider |

### 2.3.4 Maintenance, Management and Operation

| *Action:* | **Grant management/configuration/monitoring access rights** | |
|---|---|---|
| *Rationale / Objective:* | Enterprise IT department personnel (admin) or Service provider want to grant another person (factory personnel or Enterprise IT department personnel) access to the network management/configuration/monitoring system. | |
| *Preconditions:* | Access rights for a person do not exist or the person has no access granted. | |
| *Outcome:* | Access granted. | |
| *Provisioning model:* | **Fully private 5G network** | **Network-as-a-Service** |
| *Involved Stakeholder(s):* | Enterprise IT department (admin), User (factory personnel) | Service provider, User (factory personnel) |

| *Action:* | **Modify management/configuration/monitoring access rights** | |
|---|---|---|
| *Rationale / Objective:* | Enterprise IT department personnel (admin) want to modify access rights to the network management/configuration/monitoring system of another person. | |
| *Preconditions:* | Access rights for a person exist. | |
| *Outcome:* | Access rights modified. | |
| *Provisioning model:* | **Fully private 5G network** | **Network-as-a-Service** |
| *Involved Stakeholder(s):* | Enterprise IT department (admin), User (factory personnel) | Service provider, User (factory personnel) |

| | | |
|---|---|---|
| *Action:* | **Revoke management/configuration/monitoring access rights** | |
| *Rationale / Objective:* | Enterprise IT department personnel (admin) want to modify access rights to the network management/configuration/monitoring system of another person. | |
| *Preconditions:* | Access rights for a person exist. | |
| *Outcome:* | Access rights revoked. | |
| *Provisioning model:* | **Fully private 5G network** | **Network-as-a-Service** |
| *Involved Stakeholder(s):* | Enterprise IT department (admin), User (factory personnel) | Service provider, User (factory personnel) |

| | | |
|---|---|---|
| *Action:* | **Retrieve configuration log file** | |
| *Rationale / Objective:* | Enterprise IT department personnel want to review management/configuration log file to check for unauthorized access (attempts) to the management/configuration/monitoring system, for misconfigurations, SLA and legal purposes. | |
| *Preconditions:* | Configuration log file exist. | |
| *Outcome:* | Configuration log file is viewed by the Enterprise IT department personnel. | |
| *Provisioning model:* | **Fully private 5G network** | **Network-as-a-Service** |
| *Involved Stakeholder(s):* | Enterprise IT department | Enterprise IT department, Service provider |

| | | |
|---|---|---|
| *Action:* | **Schedule maintenance and updates in a pre-defined time window** | |
| *Rationale / Objective:* | The user wants maintenance and updates for the 5G System only in predefined and well-coordinated time windows, for example, aligned with planned maintenance tasks on the shop floor. | |
| *Preconditions:* | Shop floor maintenance planned. | |
| *Outcome:* | Maintenance task and updates take place only within agreed time window. | |
| *Provisioning model:* | **Fully private 5G network** | **Network-as-a-Service** |
| *Involved Stakeholder(s):* | User (factory personnel), Enterprise IT department | User (factory personnel), Service Provider |

| | | |
|---|---|---|
| *Action:* | **Configuration of new application or service** | |
| *Rationale / Objective:* | The user wants a new application or service to be made available via the 5G system. | |
| *Preconditions:* | The new application or service is prepared for deployment | |
| *Outcome:* | The new application or service is accessible via the 5G system An appropriate application profile and subscriber profiles are configured. | |
| *Provisioning model:* | **Fully private 5G network** | **Network-as-a-Service** |
| *Involved Stakeholder(s):* | Enterprise IT department (admin) | Service provider, Enterprise IT department (admin) |

| | | |
|---|---|---|
| *Action:* | **Integrate new network elements into NMS** | |
| *Rationale / Objective:* | The operator wants to integrate a network element into the network management system. | |
| *Preconditions:* | The network element has open northbound interfaces that are compliant with standards. | |
| *Outcome:* | The network element is integrated into the network management system. | |
| *Provisioning model:* | **Fully private 5G network** | **Network-as-a-Service** |
| *Involved Stakeholder(s):* | Enterprise IT department | Service provider |

| | | |
|---|---|---|
| *Action:* | **Modify network element configuration** | |
| *Rationale / Objective:* | The operator wants to configure and manage network elements of the end-to-end system. | |
| *Preconditions:* | The network element has been integrated into the network management system. | |
| *Outcome:* | The operator can perform network-wide configuration management, e.g. parameter changes, manage hardware data, or launch new technologies and services | |
| *Provisioning model:* | **Fully private 5G network** | **Network-as-a-Service** |
| *Involved Stakeholder(s):* | Enterprise IT department | Service provider |

### 2.3.5 Data Confidentiality, Security and Safety

| | |
|---|---|
| *Action:* | **Enable/disable network-driven end-to-end encryption** |
| *Rationale / Objective:* | To have end-to-end encryption initiated or ended by network |
| *Preconditions:* | |
| *Outcome:* | • After UE requests registration to the network, the network would initiate the end-to-end encryption<br>• When end-to-end encryption service is not needed anymore, the core network can disable the encryption service. |
| *Provisioning model:* | **Fully private 5G network and Network-as-a-Service** |
| *Involved Stakeholder(s):* | User (factory personnel), Enterprise IT department |

| | |
|---|---|
| *Action:* | **Modify UE security settings** |
| *Rationale / Objective:* | The security setting for UE can be modified in a period |
| *Preconditions:* | |
| *Outcome:* | ● Both UE and core network will have a UL/DL NAS count<br>● After end of NAS count, core network will modify the UE security key. |
| *Provisioning model:* | **Fully private 5G network and Network-as-a-Service** |
| *Involved Stakeholder(s):* | User (factory personnel), Enterprise IT department |

| | |
|---|---|
| *Action:* | **Verify the activation of data confidentiality and integrity protection mechanisms** |
| *Rationale / Objective:* | The user wants to check if the data confidentiality and integrity protection mechanisms are operational |
| *Preconditions:* | |
| *Outcome:* | The integrity procedure between UE and core network is operating successfully. |
| *Provisioning model:* | **Fully private 5G network and Network-as-a-Service** |
| *Involved Stakeholder(s):* | User (factory personnel), Enterprise IT department |

| | |
|---|---|
| *Action:* | **Verify absence of jammers/rogue clients/unauthorized access attempts** |
| *Rationale / Objective:* | The user wants to detect abnormal UE behavior like jammers, track rogue clients and unauthorized UE access |
| *Preconditions:* | • The core network will record the UE behavior since UE send the access request, and detect the un-normal behavior ones.<br>• The core network will recode the rogue UE information like IMSI/SUPI, and add in black list<br>• The core network will reject the unauthorized UE accessing behavior and also have a record. |
| *Outcome:* | Information about irregular UE behavior is made available to the user. |
| *Provisioning model:* | **Fully private 5G network and Network-as-a-Service** |
| *Involved Stakeholder(s):* | User (factory personnel), Enterprise IT department |

### 2.3.6 Private Communication

| | | |
|---|---|---|
| *Action:* | **Add and configure a group of subscribers for private (isolated) communication** | |
| *Rationale / Objective:* | The factory personnel want to create a grouping of UEs, which belong to the same zone, e.g. a production line zone, and whose communication is limited to that group. | |
| *Preconditions:* | UEs are not part of a subscriber group for private (isolated) communication). | |
| *Outcome:* | A group of subscribers for private (isolated) communication is set up and defined by, e.g., an IP address range or VLAN ID | |
| *Provisioning model:* | **Fully private 5G network** | **Network-as-a-Service** |
| *Involved Stakeholder(s):* | User (factory personnel), Enterprise IT department | User (factory personnel), Service Provider |

| | | |
|---|---|---|
| *Action:* | **Modify the configuration for a group of subscribers for private (isolated) communication, e.g. IP address range or VLAN ID** | |
| *Rationale / Objective:* | The factory personnel want to change the configuration, e.g. the IP address range or the VLAN tag, for a group of subscribers that communicate privately. | |
| *Preconditions:* | A group of subscribers for private (isolated) communication exists. | |
| *Outcome:* | Configuration of the group of subscribers for private (isolated) communication successfully changed. | |
| *Provisioning model:* | **Fully private 5G network** | **Network-as-a-Service** |
| *Involved Stakeholder(s):* | User (factory personnel), Enterprise IT department | User (factory personnel), Service Provider |

| | | |
|---|---|---|
| *Action:* | **Modify group membership for individual UEs** | |
| *Rationale / Objective:* | The factory personnel want to add, change or remove the group membership of a UE. | |
| *Preconditions:* | A group of subscribers for private (isolated) communication exists. | |
| *Outcome:* | The group membership has successfully changed for a selected UE. | |
| *Provisioning model:* | **Fully private 5G network** | **Network-as-a-Service** |
| *Involved Stakeholder(s):* | User (factory personnel), Enterprise IT department | User (factory personnel), Service Provider |

| | | |
|---|---|---|
| *Action:* | **Remove a group of subscribers for private (isolated) communication** | |
| *Rationale / Objective:* | The factory personnel want to remove a grouping of UEs, which belong to the same zone, e.g. a production line zone, e.g., to free resources after disassembling an entire production line. | |
| *Preconditions:* | A group of subscribers for private (isolated) communication exists. | |
| *Outcome:* | The group of subscribers for private (isolated) communication has successfully been removed. | |
| *Provisioning model:* | **Fully private 5G network** | **Network-as-a-Service** |
| *Involved Stakeholder(s):* | User (factory personnel), Enterprise IT department | User (factory personnel), Service Provider |
| *Action:* | **Restrict the maximum number of group memberships for an individual UE to one** | |
| *Rationale / Objective:* | To ensure that a factory asset can only communicate inside a single line zone, it should be possible that the number of group memberships for an individual UE can be restricted to at most one. | |
| *Preconditions:* | | |
| *Outcome:* | The maximum number of group memberships for an individual UE is set to one. | |
| *Provisioning model:* | **Fully private 5G network** | **Network-as-a-Service** |
| *Involved Stakeholder(s):* | User (factory personnel), Enterprise IT department | User (factory personnel), Service Provider |

| | | |
|---|---|---|
| *Action:* | **Enable private (isolated) communication between members of a group of at least two subscribers** | |
| *Rationale / Objective:* | The factory personnel want to enable the communication between assets being part of the same machine or production line, while they are already members of the same group for private (isolated) communication. | |
| *Preconditions:* | A group of subscribers for private (isolated) communication exists and communication between group members is disabled. | |
| *Outcome:* | Communication between group members is enabled. | |
| *Provisioning model:* | **Fully private 5G network** | **Network-as-a-Service** |
| *Involved Stakeholder(s):* | User (factory personnel), Enterprise IT department | User (factory personnel), Service Provider |

| | | |
|---|---|---|
| *Action:* | **Enable private (isolated) communication between two selected subscribers, which are part of two distinct groups** | |
| *Rationale / Objective:* | The factory personnel want to enable the communication between a pair of subscribers, which are in distinct groups for private (isolated) communication, while their group memberships do not change (e.g. two connected machines of two separate production line zones) | |
| *Preconditions:* | Two selected subscribers are associated with different groups of private (isolated) communication. | |
| *Outcome:* | Communication between the pair of subscribers is enabled. | |
| *Provisioning model:* | **Fully private 5G network** | **Network-as-a-Service** |
| *Involved Stakeholder(s):* | User (factory personnel), Enterprise IT department | User (factory personnel), Service Provider |

| | | |
|---|---|---|
| *Action:* | **Disable communication between any two subscribers, which are part of two distinct groups** | |
| *Rationale / Objective:* | The factory personnel want to disable the communication between a pair of subscribers, which are in distinct groups for private (isolated) communication, while their group memberships do not change (e.g. two connected machines of two separate production line zones) | |
| *Preconditions:* | Two selected subscribers are associated with different groups of private (isolated) communication and communication between them is enabled. | |
| *Outcome:* | Communication between the pair of subscribers is disabled. | |
| *Provisioning model:* | **Fully private 5G network** | **Network-as-a-Service** |
| *Involved Stakeholder(s):* | User (factory personnel), Enterprise IT department | User (factory personnel), Service Provider |

| | | |
|---|---|---|
| *Action:* | **Enable private (isolated) communication between a group of at least two subscribers and a central service** | |
| *Rationale / Objective:* | The factory personnel want a all subscribers of the same group to have access to a (edge computing) service. | |
| *Preconditions:* | Subscribers of a group for private (isolated) communication do not have access to a well-defined (e.g. through an IP address) service outside that group. | |
| *Outcome:* | All subscribers of a group for private (isolated) communication have access to a service outside that group. | |
| *Provisioning model:* | **Fully private 5G network** | **Network-as-a-Service** |
| *Involved Stakeholder(s):* | User (factory personnel), Enterprise IT department | User (factory personnel), Service Provider |

| | | |
|---|---|---|
| *Action:* | **Disable private (isolated) communication between a group of at least two subscribers and a central service** | |
| *Rationale / Objective:* | The factory personnel want to revoke access to a (edge computing) service from all subscribers of the same group. | |
| *Preconditions:* | Access to a central service for a group of subscribers is enabled. | |
| *Outcome:* | Access to a central service for a group of subscribers is revoked. | |
| *Provisioning model:* | **Fully private 5G network** | **Network-as-a-Service** |
| *Involved Stakeholder(s):* | User (factory personnel), Enterprise IT department | User (factory personnel), Service Provider |

| | | |
|---|---|---|
| *Action:* | **Enable private (isolated) communication between a selected subscriber being part of a group for private (isolated) communication and a central service** | |
| *Rationale / Objective:* | The factory personnel want a single, selected subscriber being part of a group for private (isolated) communication to have access to a (edge computing) service (e.g. an edge computing application, service zone) | |
| *Preconditions:* | Access to a central service for a single, selected subscriber is disabled. | |
| *Outcome:* | Access to a central service for a single, selected subscriber is enabled. | |
| *Provisioning model:* | **Fully private 5G network** | **Network-as-a-Service** |
| *Involved Stakeholder(s):* | User (factory personnel), Enterprise IT department | User (factory personnel), Service Provider |
| *Action:* | **Disable private (isolated) communication between a selected subscriber being part of a group for private (isolated) communication and a central service** | |
| *Rationale / Objective:* | The factory personnel want revoke access to a (edge computing) service (e.g. an edge computing application, service zone) from a single, selected subscriber. | |
| *Preconditions:* | Access to a central service for a single, selected subscriber is enabled. | |
| *Outcome:* | Access to a central service for a single, selected subscriber is revoked. | |
| *Provisioning model:* | **Fully private 5G network** | **Network-as-a-Service** |
| *Involved Stakeholder(s):* | User (factory personnel), Enterprise IT department | User (factory personnel), Service Provider |

### 2.3.7 Accounting

| *Action:* | **The billing information is provided to the Enterprise IT and Accounting departments** | |
|---|---|---|
| *Rationale / Objective:* | The traffic usage data in the 5G network is for every user in the factory. | |
| *Preconditions:* | Enterprise IT department provides the list of users in the factory | |
| *Outcome:* | The volume of usage for every user in the factory | |
| *Provisioning model:* | **Fully private 5G network** | **Network-as-a-Service** |
| *Involved Stakeholder(s):* | User (factory personnel), Enterprise IT department | User (factory personnel), Service provider<br>Enterprise IT department |

### 2.3.8 Monitoring

| *Action:* | **Verify Network Slice in place** | |
|---|---|---|
| *Rationale / Objective:* | The user or Enterprise IT department personnel want to verify the registration and connectivity status of NSs. | |
| *Preconditions:* | The Network Slicing System gathers such information and makes them available. | |
| *Outcome:* | Status is retrieved and can be viewed by the user or Enterprise IT department personnel for verifying NSs. | |
| *Provisioning model:* | **Fully private 5G network** | **Network-as-a-Service** |
| *Involved Stakeholder(s):* | User<br>Enterprise IT department | User<br>Enterprise IT department, Service provider |

| *Action:* | **Monitor network and UE health status** | |
|---|---|---|
| *Rationale / Objective:* | The user or Enterprise IT department personnel wants to know the operation or connectivity status of UEs and/or the network. | |
| *Preconditions:* | The 5G System gathers such information and makes them available. | |
| *Outcome:* | The user retrieves, views and understands details about network and UE operation/connectivity status.<br><br>Status is retrieved and can be viewed by Enterprise IT department personnel for maintenance of the network. | |
| *Provisioning model:* | **Fully private 5G network** | **Network-as-a-Service** |
| *Involved Stakeholder(s):* | User<br>Enterprise IT department | User<br>Enterprise IT department, Service provider |

| *Action:* | **Monitor networking anomalies** | |
|---|---|---|
| *Rationale / Objective:* | Enterprise IT department personnel wants to be notified in case of anomalies related to network or UE status | |
| *Preconditions:* | The 5G System gathers such information and makes them available. | |
| *Outcome:* | Status is retrieved and can be viewed by Enterprise IT department personnel. | |
| *Provisioning model:* | **Fully private 5G network** | **Network-as-a-Service** |
| *Involved Stakeholder(s):* | Enterprise IT department | Enterprise IT department, Service provider |

| | | |
|---|---|---|
| *Action:* | **Monitor network performance over time per UE** | |
| *Rationale / Objective:* | Enterprise IT department personnel want to know the networking performance of UEs. | |
| *Preconditions:* | The 5G System gathers such information and makes them available. | |
| *Outcome:* | Status is retrieved and can be viewed by Enterprise IT department personnel. | |
| *Provisioning model:* | **Fully private 5G network** | **Network-as-a-Service** |
| *Involved Stakeholder(s):* | Enterprise IT department | Enterprise IT department, Service provider |

| | | |
|---|---|---|
| *Action:* | **Verify network configuration in place** | |
| *Rationale / Objective:* | Enterprise IT department personnel want to verify the network configuration status of the network. | |
| *Preconditions:* | The network system gathers such information and makes them available. | |
| *Outcome:* | Information is retrieved and can be viewed by Enterprise IT department personnel for verification network configuration. | |
| *Provisioning model:* | **Fully private 5G network** | **Network-as-a-Service** |
| *Involved Stakeholder(s):* | Enterprise IT department | Enterprise IT department, Service provider |

| | | |
|---|---|---|
| *Action:* | **Monitor security mechanisms (confidentiality and integrity protection, especially if Mobile Network Operator operates network)** | |
| *Rationale / Objective:* | Enterprise IT department personnel want to know the security mechanisms status of 5G network. | |
| *Preconditions:* | The plant system gathers such information and makes them available. | |
| *Outcome:* | Status is retrieved and can be viewed by Enterprise IT department personnel. | |
| *Provisioning model:* | **Fully private 5G network** | **Network-as-a-Service** |
| *Involved Stakeholder(s):* | Enterprise IT department | Enterprise IT department, Service provider |

| | |
|---|---|
| *Action:* | **Monitor spectrum usage** |
| *Rationale / Objective:* | Enterprise IT department personnel want to know the utilization of spectrum. |
| *Preconditions:* | The 5G System gathers such information and makes them available. |
| *Outcome:* | The utilization is retrieved and can be viewed by Enterprise IT department personnel |
| *Provisioning model:* | **Fully private 5G network and Network-as-a-Service** |
| *Involved Stakeholder(s):* | Enterprise IT department<br>Service provider |

| | | |
|---|---|---|
| *Action:* | **Monitor networking capabilities, guaranteed performance and supported services.** | |
| *Rationale / Objective:* | The user or Enterprise IT department personnel want to know the network QoS/services status of the 5G network. | |
| *Preconditions:* | The 5G System gathers such information and makes them available. | |
| *Outcome:* | Status is retrieved and can be viewed by the user or Enterprise IT department personnel. | |
| *Provisioning model:* | **Fully private 5G network** | **Network-as-a-Service** |
| *Involved Stakeholder(s):* | User<br>Enterprise IT department | User<br>Enterprise IT department, Service provider |

| | | |
|---|---|---|
| *Action:* | **Verify that outage protection is activated** | |
| *Rationale / Objective:* | Enterprise IT department personnel want to know the outage protection activation status of plants. | |
| *Preconditions:* | The 5G system gathers such information and makes them available. | |
| *Outcome:* | Status is retrieved and can be viewed by Enterprise IT department personnel. | |
| *Provisioning model:* | **Fully private 5G network** | **Network-as-a-Service** |
| *Involved Stakeholder(s):* | Enterprise IT department | Enterprise IT department, Service provider |

| | | |
|---|---|---|
| *Action:* | **Verify that failover and redundancy concepts are ready** | |
| *Rationale / Objective:* | Enterprise IT department personnel want to know the failover/ redundancy concepts activation status of the 5G system. | |
| *Preconditions:* | The 5G System gathers such information and makes them available. | |
| *Outcome:* | Status is retrieved and can be viewed by Enterprise IT department personnel. | |
| *Provisioning model:* | **Fully private 5G network** | **Network-as-a-Service** |
| *Involved Stakeholder(s):* | Enterprise IT department | Enterprise IT department, Service provider |

| | |
|---|---|
| *Action:* | **Retrieve factory asset location information** |
| *Rationale / Objective:* | The user wants to know the location of a specific factory asset. |
| *Preconditions:* | The 5G System is able to localize a factory asset. |
| *Outcome:* | The user retrieves and viewes location information of a specific factory asset. |
| *Provisioning model:* | **Fully private 5G network and Network-as-a-Service** |
| *Involved Stakeholder(s):* | User (factory personnel) |

### 2.3.9 Fault Management

| *Action:* | **Fault management** | |
|---|---|---|
| *Rationale / Objective:* | The operator wants to detect and troubleshoot the faults that cause disruptions in network services | |
| *Preconditions:* | Network elements have monitoring and diagnostic tools for detecting various types of fault situations. Each fault is represented as an alarm which is sent to the network management system. | |
| *Outcome:* | The operator analyzes and troubleshoots the faults in network elements. | |
| *Provisioning model:* | **Fully private 5G network** | **Network-as-a-Service** |
| *Involved Stakeholder(s):* | Enterprise IT department | Service provider |

| *Action:* | **Retrieve communication error statistics** | |
|---|---|---|
| *Rationale / Objective:* | The user wants to know details about communication errors, such as the locations of handover failures. | |
| *Preconditions:* | The 5G System gathers such information and makes them available. | |
| *Outcome:* | The user retrieves, views and understands details about communication errors without having specific knowledge about rather complex communication mechanisms. | |
| *Provisioning model:* | **Fully private 5G network** | **Network-as-a-Service** |
| *Involved Stakeholder(s):* | User (factory personnel), Enterprise IT department | User (factory personnel), Service provider |

| *Action:* | **Verify status of UE (connected, registered)** | |
|---|---|---|
| *Rationale / Objective:* | Identify faults in the access links | |
| *Preconditions:* | Status of UE is available through the network management system | |
| *Outcome:* | Status is confirmed → no action<br>Status is not confirmed → troubleshooting and recovery actions are triggered | |
| *Provisioning model:* | **Fully private 5G network** | **Network-as-a-Service** |
| *Involved Stakeholder(s):* | Enterprise IT department | Service provider,<br>Enterprise IT department |

| *Action:* | **React to a status change of a (critical) end device** | |
|---|---|---|
| *Rationale / Objective:* | Detect anomalies in the end devices | |
| *Preconditions:* | The system can check status of end devices | |
| *Outcome:* | Factory personnel confirms the status | |
| *Provisioning model:* | **Fully private 5G network** | **Network-as-a-Service** |
| *Involved Stakeholder(s):* | User (factory personnel), Enterprise IT department | User (factory personnel), Service provider<br>Enterprise IT department |

| *Action:* | **Acknowledge alarm upon occurrence of user-defined event related to the 3GPP / networking / virtualization environment domain** | |
|---|---|---|
| *Rationale / Objective:* | Detect anomalies in the network elements and/or UEs / network links / devices and apparatuses | |
| *Preconditions:* | The system identifies events related to 3GPP signaling / links failures and other connectivity problems / events related to the virtual resources (computing, storage and network) | |
| *Outcome:* | Factory personnel analyzes the notification | |
| *Provisioning model:* | **Fully private 5G network** | **Network-as-a-Service** |
| *Involved Stakeholder(s):* | Enterprise IT department | Service provider<br>Enterprise IT department |

| *Action:* | **Retrieve alarm log file** | |
|---|---|---|
| *Rationale / Objective:* | Analysis of root causes and troubleshooting | |
| *Preconditions:* | The system records events through appropriate logging facilities | |
| *Outcome:* | Factory personnel analyzes the logs | |
| *Provisioning model:* | **Fully private 5G network** | **Network-as-a-Service** |
| *Involved Stakeholder(s):* | Enterprise IT department | Service provider<br>Enterprise IT department |

# 3 Architecture Options for Private 5G Networks

When moving from traditional PLMN to private 5G network deployments models, ownership and governance of the different dimensions described in Sec. 2.2 are shared across multiple stakeholders as opposed to a single MNO. These dimensions, along with the different stakeholders involved, span a large space of possible architecture and deployment options. The choice of architecture will depend on the enterprises' specific functional and organizational requirements.

This section presents four architecture options that are suited for private network deployments. For each option, the involved stakeholders for all dimensions listed in Sec. 2.2 are provided, distinguishing between:

- *Owning Stakeholder*, that is, the legal proprietor of the element (e.g. physical infrastructure, licenses);
- *Governing Stakeholder*, that is, the stakeholder responsible for management and operation of the element in question.

For the purpose of the following discussion, the stakeholders considered are the following:

1. *MNO/MVNO*, that is, mobile network specific *Service Provider* as per Sec. 2.1.4;
2. *Enterprise*, grouping the *Owner of Premises*, *Enterprise IT Management Team* and End Users as per Sec. 2.1.1, 2.1.2 and 2.1.3;
3. *Service Provider*, that is, any party other than the M(V)NO or the Enterprise.

Moreover, the possible deployment locations of hardware and software components are provided in order of increasing distance from the network edge

1. *Edge Cloud*, that is, infrastructure on enterprise premises, either inside the factory or plant or on nearby enterprise premises;
2. *Enterprise Datacenter / Cloud*, that is, a datacenter infrastructure owned and governed by the enterprise, possible located off-site;
3. *Central Cloud, that is,* a (partially) public cloud infrastructure owned and governed by either or both an MNO or third party service provider.

While the presented options may be altered with respect to certain dimensions, each of them serves as representative to a broader class of architectures.

In general, the private network can be divided into two categories:

1. Private networks are deployed as the isolated and standalone network;
2. Private networks are deployed in conjunction with the public network.

The first category is comprised of one configuration which is described in section 3.1.

The second is comprised of three options according to the interaction and infrastructure sharing with the public network and they are described in section 3.2 to 3.4. In these scenarios, the network is a combination of public and private networks. The public network refers to the MNO's network that offers services to general public, whereas the private network refers to the non-public network (NPN) that provides services to the organization.

## 3.1 Fully Private Infrastructure

### 3.1.1 Architecture Description

When it comes to building Industry 4.0 and dedicated services for enterprises, the capability to have a highly available mobile network that works also in isolation from the rest of the national network and can prioritize voice, video, data and IoT services is a key requirement.

The fully private LTE/5G model is the most appropriate solution for this context, as it preserves the privacy of the data generated and consumed in the enterprise. The solution also integrates the intranet and cloud services which are specific to the enterprise, purchased over the years or self-developed such as VoIP services, location services, logistic information, high resolution camera, etc. Optional services that might be installed as well are IMS for VoLTE, PTT/MCX, eMBMS for LTE multicast / broadcast, location based services and NB-IoT.

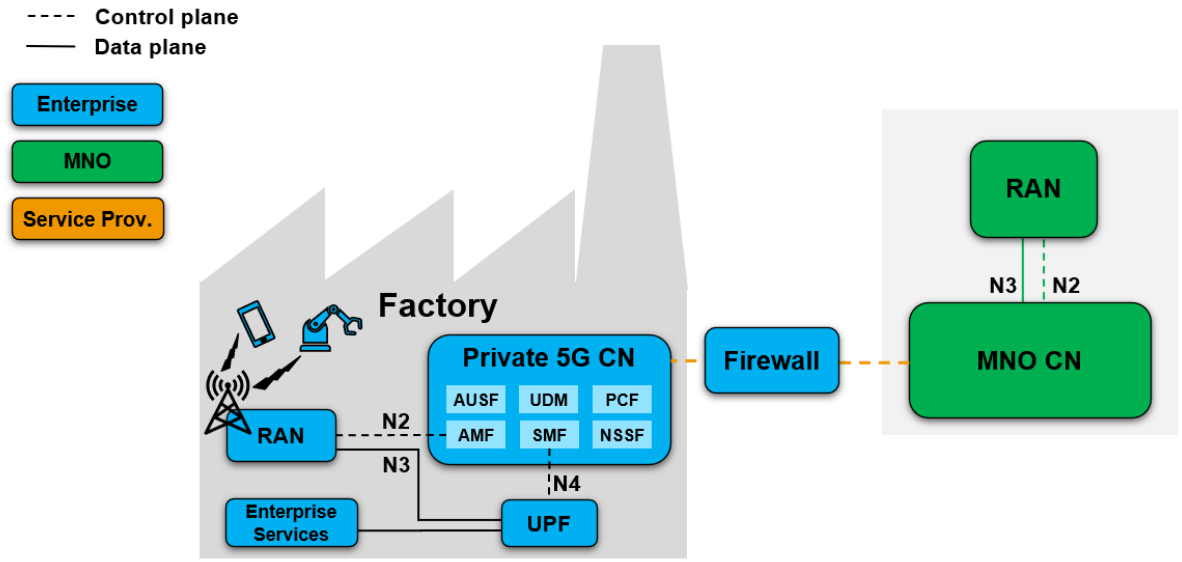


*Figure 2: Fully private model. The private CN may optionally connect to a public MNO's CN, as the NPN operator can conclude roaming agreements with one or more public network operators.*

As shown in Figure 2, a fully private ownership expects that the enterprise owns almost every dimension, that is, spectrum, RAN, MEC, CN, and applications. The only excluded dimensions are the OAM system and the transport network, which may be owned by a service provider or an operator. Generally, in case of large enterprises, this model provides for a dedicated enterprise IT management staff to manage the private network. For an enterprise deployment, the CN is integrated into the enterprise network with the enterprise IT management team responsible to assign appropriate IP addresses to the SGi interface, i.e. mobile devices. This setup allows the IT team to enforce the same policy (firewall, NAT, traffic separation, etc.) for fixed and mobile enterprise users.

A summary of owning, governance, and location of the various dimensions for the fully private model is provided in the following table ('M', 'E', and 'SP' denote the MNO/MVNO, the enterprise, and the service provider, respectively):

| Dimension | Owning stakeholder | Governing stakeholder | Location |
|---|---|---|---|
| Core - Subscriber data management (UDM) | E | E/SP | Edge cloud |
| Core - Authentication (AUSF) | E | E/SP | Edge cloud |

| Dimension | Owning stakeholder | Governing stakeholder | Location |
|---|---|---|---|
| Core - Session Management (SMF) | E | E/SP | Edge cloud |
| Core - Control Plane (AMF) | E | E/SP | Edge cloud |
| Core - User Plane (UPF) | E | E/SP | Edge cloud |
| OAM System | E/SP | E | Edge cloud |
| Transport Network | M/SP | M/SP | - |
| MEC platform | E | E/SP | Edge cloud |
| Applications | E | E/SP | Edge cloud |
| RAN | E | E/SP | - |
| Spectrum | E | E/SP | - |
| SIM | E | E/SP | - |

### 3.1.2 Stakeholder Impact

With all ownership dimensions under control of the enterprise, the Fully Private Infrastructure model offers the highest degree of flexibility in adapting the 5G system to the enterprises specific requirements. Especially pertaining to enterprise-specific security regulations, this model has a high likelihood of fulfilling the associated requirements since all data conveyed via the 5G system, including user, control and O&M traffic is fully controlled by the enterprise. If chosen to design the system accordingly, no traffic leaves the corporate IT network, thus exposing no potential vulnerabilities to external malicious actors.

However, of the deployment models discussed here, this model places the highest burden on the enterprise, which carries most responsibilities throughout all phases of deployment. Specific domain knowledge is required for planning and operation of the 5G system, which is likely to not exist within an enterprise. For example, radio planning and monitoring operational compliance with spectrum regulations are tasks quite distinct from those typically handled by enterprise IT departments.

Of course, the enterprise may choose to contract planning and/or operation with respect to any of the ownership dimensions to an external service provider.

Relating to the user stories for interaction with the 5G network of Sec. 2.3, the Fully Private Infrastructure model potentially enables the most direct interaction only involving the users and enterprise IT in all the identified categories without strictly requiring involvement of an intermediary, i.e. service provider or operator.

### 3.1.3 Cost Implications

In the Fully Private Infrastructure model, enterprises have to make a medium to large upfront investment for procuring the entire technical infrastructure of the 5G system. Additionally, one-time as well as recurring licensing and software maintenance fees for different components of the system are likely to apply.

Especially for very early SNPN deployments an uncertainty factor potentially driving the infrastructure investment cost is the novelty of the deployment model and thus lack a of clearly defined business and distribution models on the side of infrastructure vendors. Coming from a traditionally operator-centric business, the solutions initially offered to the market by vendors might not scale optimally to enterprises both in terms of technical features as well as their

pricing models. For example, a 5G core targeting the telecom carrier business may overfit the needs on the factory floor regarding, for example, capacity, i.e. number of connected devices.

Operational costs largely depend on the allocation of governance over the system dimensions. While transferring governance to an external service provider is likely to incur higher recurring cost as compared to an existing enterprise IT department, it alleviates the (initial) lack of expertise in mobile radio networks in enterprise IT. Thus, building the appropriate in-house know-how for 5G system operation additionally adds to higher initial costs.

Especially for larger enterprises, economies of scale apply with regard to operational costs. Through centralization of certain network functions, redundancies among multiple geographical locations or facilities may be reduced, thus resulting in reduced O&M workload. This is also likely to benefit the investment and recurring costs associated with typical infrastructure vendor pricing models.

## 3.2 MVNO Model

### 3.2.1 Architecture Description

In this scenario, the private and public network share part of the Radio Access Network (RAN), while other network elements remain separated. All user plane data related to the private network is terminated on the premises. The logical architecture is shown in the following Figure.

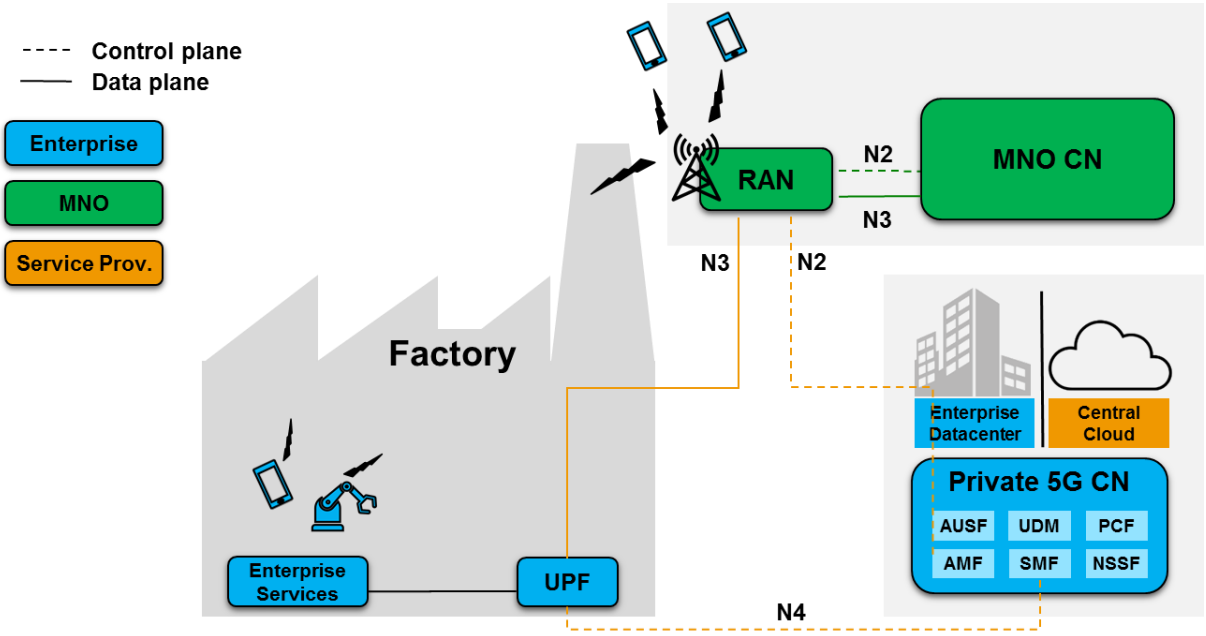


*Figure 1: MVNO Model*

The private 5G network comprises RAN, Core, OAM system, Transport Network, MEC platform, Applications, Spectrum and SIM and the MVNO model expects that the enterprise owns almost every dimension except the RAN and transport network. The enterprise deploys its own core network, MEC platform and applications, while the RAN is shared and connected to both the MNO and private core network. The radio network is accessible to both public and private users.

Depending on the scale of the enterprise, the OAM system and transport network may be owned by a service provider or MNO. The same goes for the governing stakeholders, each dimension or network element can be managed by the enterprise itself, the service provider or an operator.

A summary of owning, governance, and location of the various dimensions for the MVNO model is shown in the following table ('M', 'E', and 'SP' denote the MNO/MVNO, the enterprise, and the service provider, respectively):

| Dimension | Owning stakeholder | Governing stakeholder | Location |
|---|---|---|---|
| Core - Subscriber data management (UDM) | E | E/SP | Enterprise Datacenter / Central cloud |
| Core - Authentication (AUSF) | E | E/SP | Enterprise Datacenter / Central cloud |
| Core - Session Management (SMF) | E | E/SP | Enterprise Datacenter / Central cloud |
| Core - Control Plane (AMF) | E | E/SP | Enterprise Datacenter / Central cloud |
| Core - User Plane (UPF) | E | E/SP | Edge cloud |
| OAM System | E/SP | E/SP | Enterprise Datacenter / Central cloud |
| Transport Network | M/SP | M/SP | - |
| MEC platform | E | E/SP | Edge cloud |
| Applications | E | E/SP | Edge cloud |
| RAN | M | M | - |
| Spectrum | M | M | - |
| SIM | E | E/SP | - |

### 3.2.2 Stakeholder Impact

Since the enterprise deploys its own private core network, the degree of compliance is high in terms of subscriber management described in Section 2.3.1 and 2.3.2. Furthermore, third party APIs should be available in this shared RAN architecture which allows the enterprise to have full access to the operation and management functions. It can monitor the network status in order to troubleshoot the faults or even identify potential problems as early as possible. These are covered in Section 2.3.8 and 2.3.9.

RAN is shared and connected to both MNO and private core network in this model. This requires the governing stakeholder of RAN to consider the QoS requirements of both network. To this end, the enterprise has to reach the RAN sharing agreement with the MNO to ensure the enterprise service requirements are met in an end to end fashion. This may be achieved using efficient radio resource allocation mechanisms. In addition, cost sharing is considered in this agreement based on resource usage and billing strategies.

### 3.2.3 Cost Implications

In this approach, the MNO covers most of the cost of ownership and operation of the RAN, spectrum and even transport network. This helps to reduce the cost of deployment and might be beneficial to the enterprise in terms of economic feasibility. In the meantime, the enterprise is responsible for the rest of network segments and therefore it requires a dedicated enterprise IT management team or collaboration with network service provides.

In the fully private model described in Section 3.1, the enterprise purchases, owns and manages the private 5G network. The MVNO model is better suited for enterprises wishing to outsource day-to-day operations of the RAN which requires spectrum availability and technical

expertise to optimize hundreds of parameters in the radio network. In addition, the user plane data will stay in enterprise premises due to the self-managed core network.

## 3.3 Hybrid Model

### 3.3.1 Architecture Description

The hybrid model can be seen as a combination of the Fully Private and MVNO models. As shown in Figure 3, the enterprise hosts a local private RAN and MEC platform, which are connected to a private CN, also owned by the enterprise. However, radio access of enterprise's UEs can also take place by roaming through public MNO's RAN, which forwards control and management traffic reaches the private CN.

In the hybrid model, the CN may be split into a centralized Control Center (typically containing the 5G control-plane elements) which interacts with local RAN and devices through locally deployed Edge Nodes (containing user-plane elements (UPF) and the MEC platform) as shown in the diagram below. This platform allows the deployment and management of several distributed private networks, each anchored by an Edge Node. The Edge Node sits inside the enterprise firewall and keeps traffic and user data local to meet low latency, data security and edge compute requirements.

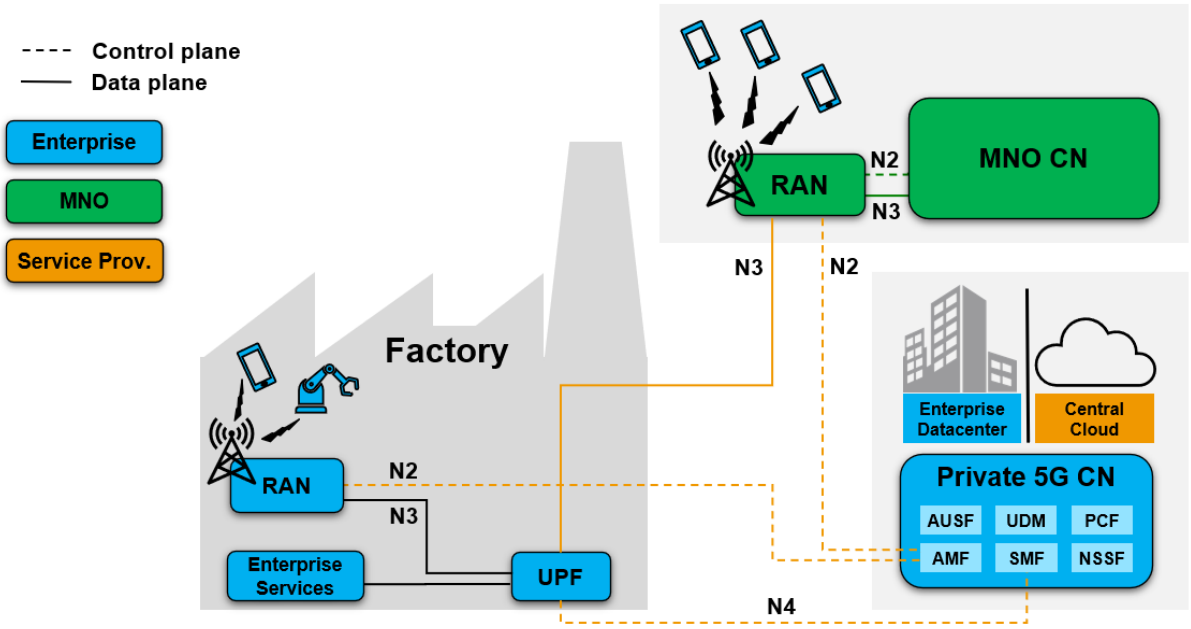


*Figure 3: Hybrid model. UEs can connect to the private CN by accessing from a private RAN or a public one. The enterprise's CN may be placed in a private datacenter or a central public cloud.*

The Edge Node can have a very small footprint to be deployed in every commercial building, factory (as shown in Figure 3), warehouse or enterprise or be deployed at an aggregation point for several private networks.

The hybrid model could be considered as part of a long-term transitional strategy: the enterprise can start in outsourcing with a simple MVNO model (see Sec. 3.2), in case an adequate enterprise IT management team may not be initially set. Once a favorable status is achieved, the enterprise can initiate a transition towards a fully private network (see Sec. 3.1), where all the network is owned by the enterprise.

A summary of owning, governance, and location of the various dimensions for the hybrid model is provided in the following table ('M', 'E', and 'SP' denote the MNO/MVNO, the enterprise, and the service provider, respectively):

| Dimension | Owning stakeholder | Governing stakeholder | Location |
|---|---|---|---|
| Core - Subscriber data management (UDM) | E | E/SP | Enterprise Datacenter / Central cloud |
| Core - Authentication (AUSF) | E | E/SP | Enterprise Datacenter / Central cloud |
| Core - Session Management (SMF) | E | E/SP | Enterprise Datacenter / Central cloud |
| Core - Control Plane (AMF) | E | E/SP | Enterprise Datacenter / Central cloud |
| Core - User Plane (UPF) | E | E/SP | Edge cloud |
| OAM System | E/SP | E/SP | Enterprise Datacenter / Central cloud |
| Transport Network | M/SP | M/SP | - |
| MEC platform | E | E/SP | Edge cloud |
| Applications | E | E/SP | Edge cloud |
| RAN | M/E | M/E/SP | - |
| Spectrum | M/E | M/E/SP | - |
| SIM | E | E/SP | - |

### 3.3.2 Stakeholder Impact

If SIMs are allowed to roam between the private RAN and the public RAN, the way of ordering and deploying them (see Sec. 2.3.1) should be agreed between the enterprise and the MNO. Furthermore, SIM authentication should be managed in order to enable seamless access between different owned RANs. Moreover, when configuring a private communication (see Sec. 2.3.6), the governing stakeholder may grant access for a specific group of UEs' SIMs across private and public RANs to preserve group isolation.

The power of the hybrid model lies in the *centralized* management system acting as a unique integration and control point for distributed Edge Nodes. This allows the governing stakeholder to have an active role in monitoring the connectivity status of Edge Nodes and devices, fault and performance analysis and services management (see Sec. 2.3.8). The Control Center allows the CSP, resellers and end-customers to deploy, manage, monitor and control the whole network (in the case of the CSP) or their relevant network modules (for system integrators and tenants). CSPs can also allocate SIMs through a waterfall procedure to resellers who can then further distribute and activate SIMs to end tenants.

### 3.3.3 Cost Implications

This approach cuts through the cost and complexity associated with traditional EPC deployments and allows for low touch, low cost deployments with complete local off-load of traffic and customer data. It allows low-latency applications and compliance with traffic and data privacy rules and requirements. The key business benefit is that a CSP can deploy private networks using standard IT professionals rather than specialized telecoms engineers. It therefore allows rapid business roll-out at highly affordable price points.

## 3.4 MNO's Private Core Network

### 3.4.1 Architecture Description

The MNO's private network architectures is similar with MVNO but the core networks, transport, spectrum, and SIM cards are used by enterprise belong to the operator. This model can be used end-to-end Network slice technology, so that the core network and RAN resources can be separated to different enterprises.

For the Multi-Operator Core Network (MOCN) architecture, this is sharing the same RAN in one site, so the operators can share the same RAN and spectrum resource to reduce the hardware coast. For 5G Multi-Operator Core Network (5G MOCN) architecture, only the RAN is shared in 5G system. The UE, RAN and AMF, shall support operators' ability to use more than one PLMN ID. 5G MOCN also can support the NG-RAN sharing with or without multiple cell identity broadcast.

For the other architecture of Dedicated Core Networks (Decor), operators can deploy more than one core networks within only one PLMN for a different type of subscribers and UEs. Based on the"UE Usage Type" send from UE, the core network can identify which UE type belong to which Decor, and provide the isolated slice resource to serve the specific type of end devices.

#### *3.4.1.1 Edge Breakout Options*

##### 3.4.1.1.1 UPF

For the 5G system in 3GPP R16 standard, a newly module Intermediate-UPF (I-UPF) has been introduced in 5G core network architecture. The I-UPFs between the PDU session anchor UPF (PSA UPF) and the NG-RAN may be used to support the data flow local breakout, which uses the N3 tunnel connecting with NG-RAN node and via N6 interface connecting with public service at edge or local site.

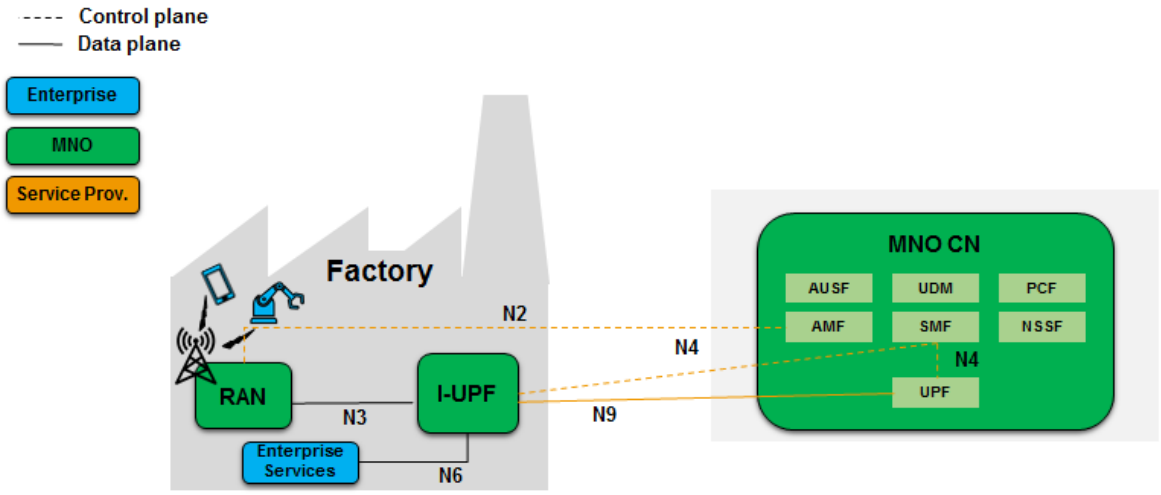


*Figure 4: MNO's Private Core Network architecture with I-UPF LBO*

In this architecture, the enterprise can have own data flow transport without back through the operator's data center in order to achieve the high efficiency and low latency.

#### 3.4.1.1.2 Bump-in-the-Wire

The bump-in-the-wire mode consists of dedicated RAN, on-premise MEC, and core network built by operator, as shown in Figure 5. The USIM cards also belong to the MNO. It is convenient to use the same USIM card between private and public network. The applications of enterprises are deployed on on-premise MEC. Because the RAN connected to MNO's core network, operator assist enterprises to deploy the MEC and connect to their internal applications. This architecture distinguishes internal and external areas of the enterprise through dedicated base stations.

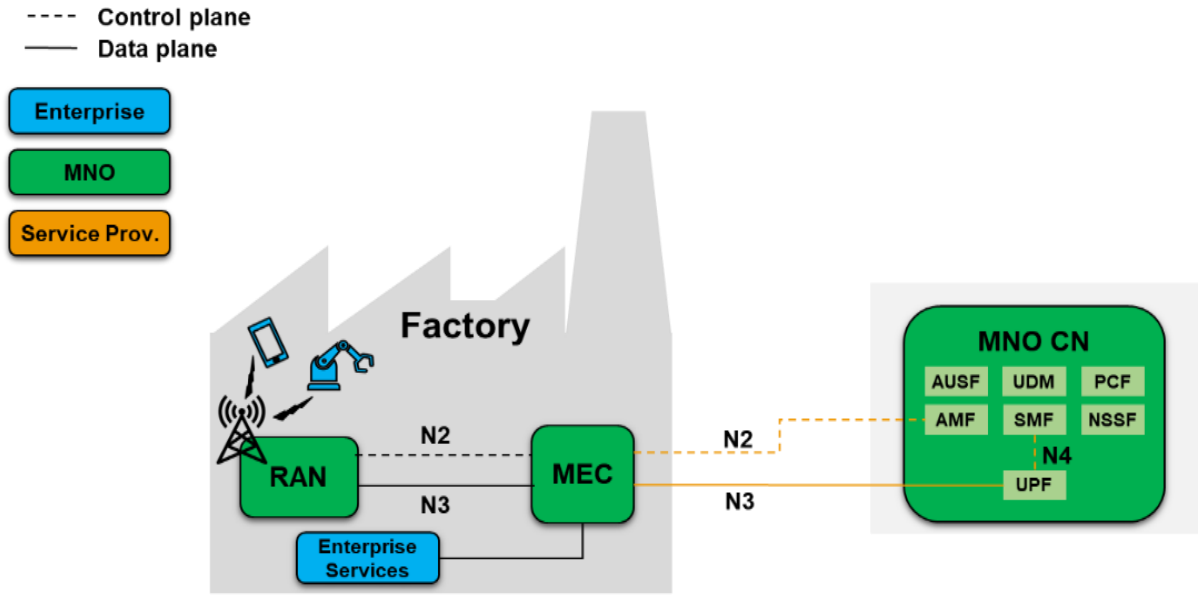


*Figure 5 MNO's Private Core Network architecture bump-in-the-wire edge breakout option*

A summary of owning, governance, and location of the various dimensions for the MNO's private core network model is provided in the following table ('M', 'E', and 'SP' denote the MNO/MVNO, the enterprise, and the service provider, respectively):

| Dimension | Owning stakeholder | Governing stakeholder | Location |
|---|---|---|---|
| Core - Subscriber data management (UDM) | M | M | Central cloud |
| Core - Authentication (AUSF) | M | M | Central cloud |
| Core - Session Management (SMF) | M | M | Central cloud |
| Core - Control Plane (AMF) | M | M | Central cloud |
| Core - User Plane (UPF) | M | M | Central cloud |
| OAM System | M/E/SP | M/E/SP | Central cloud / Edge cloud / Enterprise Datacenter |
| Transport Network | M | M | - |
| MEC platform | M | M | Edge cloud |

| Applications | E/SP | E/SP | Edge cloud |
|---|---|---|---|
| RAN | M | M | - |
| Spectrum | M | M | - |
| SIM | M | M | - |

### 3.4.2 Stakeholder Impact

For MNO's private core network model, the operator has lots of effort on this model because it provides most of the network components such as spectrum, RAN, core and transport network shown as Table 4. Enterprises basically only have to prepare their own applications and the service requirements demanded by use cases in enterprise's intra network.

For this division of responsibilities, the enterprise and operators may have to discuss the information shared mechanism across enterprise and operators for the network OAM system like section 2.3.4 mentioned. Also, the enterprise and operators have to pay attention to clarify the authority of monitoring systems (see sec 2.3.8) and provide the fault management functions (see Sec 2.3.9), then discuss what specifications operators would plan to build in enterprises for supporting those services.

Additionally, the end user in both MOCN and eDECOR architecture options has no control on the network, just SIM management and IP assignment.

### 3.4.3 Cost Implications

This model can significantly reduce the cost of construction and maintenance no matter if you use UPF or Bump-in-the-Wire edge break out option. Enterprises only need to pay the main dedicated base stations and UPF or MEC expenses. For spectrum, transport network, and core network, they can only pay fewer fees for these items. Because MNO already built the commercial 5G network for general consumers, enterprises can share these resources. The maintenance cost also can be reduced. The enterprises mainly focus on the continuous operation of edge computing systems and applications. The operators can maintain the other parts, so enterprises only need to pay a part of the maintenance cost for RAN, core network and transparent network, instead of investing all human resources and time by themselves.