5G DEPLOYMENT FOR SMART INDUSTRY USAGE

CALL: BREITBAND AUSTRIA 2030: GIGAAPP
THEME: DIGITIZATION & BROADBAND
PROJECT TYPE: COOPERATIVE R&D PROJECT
PROJECT START: 1 MAY 2023
PROJECT DURATION: 18 MONTHS

D4.1 DESIGN GUIDELINE ON 5G CAMPUS NETWORK DEPLOYMENT, COMMISSIONING, AND INTEGRATION WITH INDUSTRIAL USE CASES

5GEARING project is funded under the research and technology development of gigabit applications as part of lighthouse projects Breitband Austria 2030: GigaApp financed by the Austrian Federal Ministry of Finance and by the Austrian Research Promotion Agency (FFG) under the grant agreement n. FO999899772. Breitband Austria 2030: GigaApp was initiated by the Austrian Federal Ministry of Agriculture, Regions, and Tourism.

Document Information	
Project acronym:	5Gearing
Project number:	FO999899772
Deliverable number:	D4.1
Deliverable full title:	Design guideline on 5G campus network deployment, commissioning, and integration with industrial use cases
Deliverable short title:	Design guideline on 5G campus network deployment
Submission date:	31.7.2024
Status:	[Final]
Lead Author(s):	Damir Hamidovic (SAL)
Co-author(s):	Armin Hadziaganovic (SAL) Raheeb Muzaffar (SAL) Alexander Heinz (Cancom) Markus Dietinger (Cancom) Dalibor Mitrovic (Cancom)

Table of Contents

Executive Summary

Industry 4.0 leverages the digitization of industrial processes to enhance productivity, efficiency, and security in manufacturing. The advancements in 5G technology facilitate mobility and support time-sensitive communications, enabling innovative industrial applications. Critical sectors, including industrial automation, healthcare, and automotive, demand reliable, low-latency wireless communication. The 3^{rd} Generation Partnership Project (3GPP) offers significant opportunities for industrial IoT and smart manufacturing through 5G campus networks, which cater to specific organizations' communication needs within defined geographic areas, such as a factory floor. These networks impose stringent timing and reliability requirements for wireless interfaces to ensure seamless integration with wired networks. Non-public network deployments, whether isolated or integrated into public networks, provide benefits such as cost, robustness, availability, security, and scalability. The choice of deployment depends on specific needs, with isolated deployments offering superior control and security. Additionally, effective RF planning is crucial, especially in indoor environments, to achieve the required coverage and performance while considering spectrum availability, environmental factors, and budget constraints. Simulation tools are typically used for RF planning to optimize coverage, minimize interference, and ensure performance metrics such as throughput are met.

1 Introduction

Industry 4.0 promises on digitization of industrial processes that can significantly improve the productivity, efficiency, and security of the manufacturing industry. The 5G/6G technology enhances flexibility through mobility and support for time-sensitive communication, thereby enabling new innovative industrial use cases. Many applications from industrial automation to health care, automotive, etc., require reliable low-latency communication preferably with wireless connectivity. In that regard, the 3^{rd} generation Partnership Project (3GPP) promises novel opportunities for various industrial Internet-of-Things (IoT) and smart manufacturing use cases that have stringent communication requirements. More specifically, 3GPP specifications include a 5G campus (non-public) network that is meant to provide service to a specific organization over the geographic scope of a campus area, e.g., an indoor factory floor. However, this brings in stringent timing and reliability requirements for wireless interfaces, driven by the need for seamless integration with wired networks.

Deployment of non-public networks (isolated deployment) may be more suitable compared to other options for applications that require precision control or near real-time communication. A non-public network integrated into a public network requires lower deployment and maintenance costs compared to a completely isolated deployment. Nonetheless, an isolated deployment is superior in terms of robustness, availability, security, data privacy, and network scalability as the resources and components can be controlled locally, which is often a requirement in industrial deployments. There are various deployment options of a 5G System (5GS) from the isolated deployment, through a cloud-native non-public network (the 5G core is in the cloud), shared-access network (shared RAN between private and public network), shared access and control plane, to the deployment fully hosted by the public network operator [2, 3].

Besides the deployment option, a typical challenge especially for indoor environments is RF planning, to have the required coverage and performance with an optimal number of remote radio unit (RRU)s, type of RRUs, and cell-frequency planning. Typically, the available spectrum, environment, and budget/deployment costs are limiting parameters. Depending on those parameters and the required Key Performance Indicators (KPIs), the optimal deployment option is chosen. RF planning is usually performed using simulation tools, where the coverage, interference and performance parameters such as throughput can be simulated. An example of RF planning is presented in [2].

1.1 Objective of the report

The objective of this report is to describe the procedure of a 5G campus network planning and deployment. The goal is to provide options for optimization in the phase of planning and deployment based on the required performance and available resources. Further, the steps of the 5GS deployment, testing, and commissioning will be provided in an example of a private industrial Standalone (SA) 5G testbed scenario. Another objective is to provide guidelines on testing, commissioning, and integration of the overall system including the end-devices and applications with the deployed 5GS.

1.2 Structure of the document

Besides the Introduction, the document contains two main sections. Section 3 is about the deployment and setup of the 5GS itself, while Section 4 is about the commissioning, testing, and integration of the overall industrial setup with the 5GS. Section 4 concludes the document by summarizing the analyzed guidelines, procedures, and observations.

2 Deployment, setup, and commissioning of the 5G campus networks in industrial environments

2.1 5G core

5G core implementations are fully virtualized and do not require specific, dedicated hardware for their deployment. Instead, it can run on hardware with a generic OS, such as Linux or Windows. Depending on the implementation, there are various possible 5G core software deployment options. Virtualization environments aim to provide isolation or protection of resources such as computation, memory, and storage between different applications. As typical virtual environments, we consider virtual machines and containers.

First, there is an option of ’bare metal’ deployment, where all the 5G components are deployed directly on one or more host machines, without additional virtualization. This deployment option is suitable for scenarios where not a lot of other edge computing applications are running on the same host machines, and this deployment option provides the best performance since there are no additional abstraction levels on the software side. The downside of this type of deployment is dependency on the network configuration of the host machine and no separation of the network or computation resources between 5G core components and other applications. This deployment is suitable for testing, and for commercial deployments where either dedicated hardware can be used for the 5G deployment, or where the existing network configuration allows it. The advantage is that there is no need for substantial license costs for the virtualization. On the other hand, the deployment option is not flexible and might not be possible to use in every existing network configuration.

The second deployment solution, available in some implementations of the 5G core, is the option where network namespaces are used for the virtual separation of the network configuration of the 5G system and the rest of the network configuration on the host(s). However, in this solution, the 5G network components are also running directly on the host(s).

The next deployment solution is using virtual machines and/or Docker-container. In this case, the 5G core components are not running directly on the host machine(s), but in a virtualized environment, i.e., on virtual machine(s). This solution is suitable if we want to separate completely the 5G core applications from the rest of the applications on host(s). This solution is very scalable and easy to replicate on multiple hardware setups. Moreover, it is possible to reserve dedicated hardware resources for those virtual machines.

Kubernetes is an open-source platform that can automate the deployment, scaling, and management of containerized applications such as those running in Docker containers. Kubernetes can be used for orchestrating containers, running applications and making the deployment scalable, and ensuring high availability and reliability and independence from a single host machine. Kubernetes is widely used for containerized workload management in cloud environments, on-premises, and hybrid setups. If the 5G core is running in the Kubernetes, under the containerized environments, the deployment is detached from a specific hardware, but the components can run in a network of hardware devices. This solution provides high reliability and independence of a single host. In this case, each 5G component is running in Kubernetes and can be backed up, and restarted automatically on the same or different hardware, in case a component fails to function. Deployments in virtualized environments are suitable for commercial setups, but they can also be very practical in testing environments, especially if the 5G core is running on the host machine(s) where many other applications are running, due to the complete separation of the network configuration and option for reserved hardware resources for the 5G core applications.

Druid Software core

The 5G core, deployed in the SAL 5G testbed in LIT Factory at JKU campus is a Raemis™ platform from Druid Software Ltd. The Raemis™ platform is built on a Representational State Transfer (REST)-based and service-oriented architecture.

The platform provides a management GUI for the installation and maintenance of a private 5G network. REST API enables the integration of external applications to enhance the 5G network. It supports NSA and SA network deployment options.
The Raemis™ platform for SA 5G deployment consists of the 5G core components: Access and Mobility management Function (AMF), Session Management Function (SMF), Unified Data Management (UDM), Policy control function (PCF) and Short Message Service Function (SMSF) and the user plane component User Plane Function (UPF). The implemented interfaces are N1 (UE-AMF), N2 (AMF-gNB), N3 (gNB-UPF), N4 (SMF-UPF), N6 (UPF-IMS/external network).
The most important features of the Raemis™ 5G platform, according to the Druid documentation, are:

- Slicing - separation of multiple networks operating on the same set of virtualized infrastructure. It ensures a specified Quality of Service (QoS) and security level for a user or a group by virtual separation of traffic from each slice using VLANs where each slice has its own UPF. The slicing relies on a RAN slicing implementation in gNBs, where the implementation of the QoS service on the air interface is implemented.

- Mobile Edge Computing - a concept of implementing parts of communication handling at the edge of the network, closer to the radio interface. Two models are supported: pure MEC data plane offload and the distributed core model.

- RAN management - possibility to configure the radio base station equipment independent of their vendors. The configuration is done using NETCONF/YANG as a management framework.

- Integration of LTE coverage - support for roaming of 5G SA subscribers out to external LTE networks.

- 5G SA Roaming - enables roaming between 5G SA networks.

- Integration of 5G SA coverage with legacy LTE core - allowing usage of 5G features on certain areas, e.g., campus, with extended LTE coverage on a larger area, e.g., outside of campus.

- Real-time communication Services - support for voice and video calling, such as voice over NR (VoNR). Raemis™ platform includes the IP multimedia Subsystem (IMS) component implementation.

The procedure of deploying, configuring, and running the Druid Software 5G core is visually presented in Fig. 1.

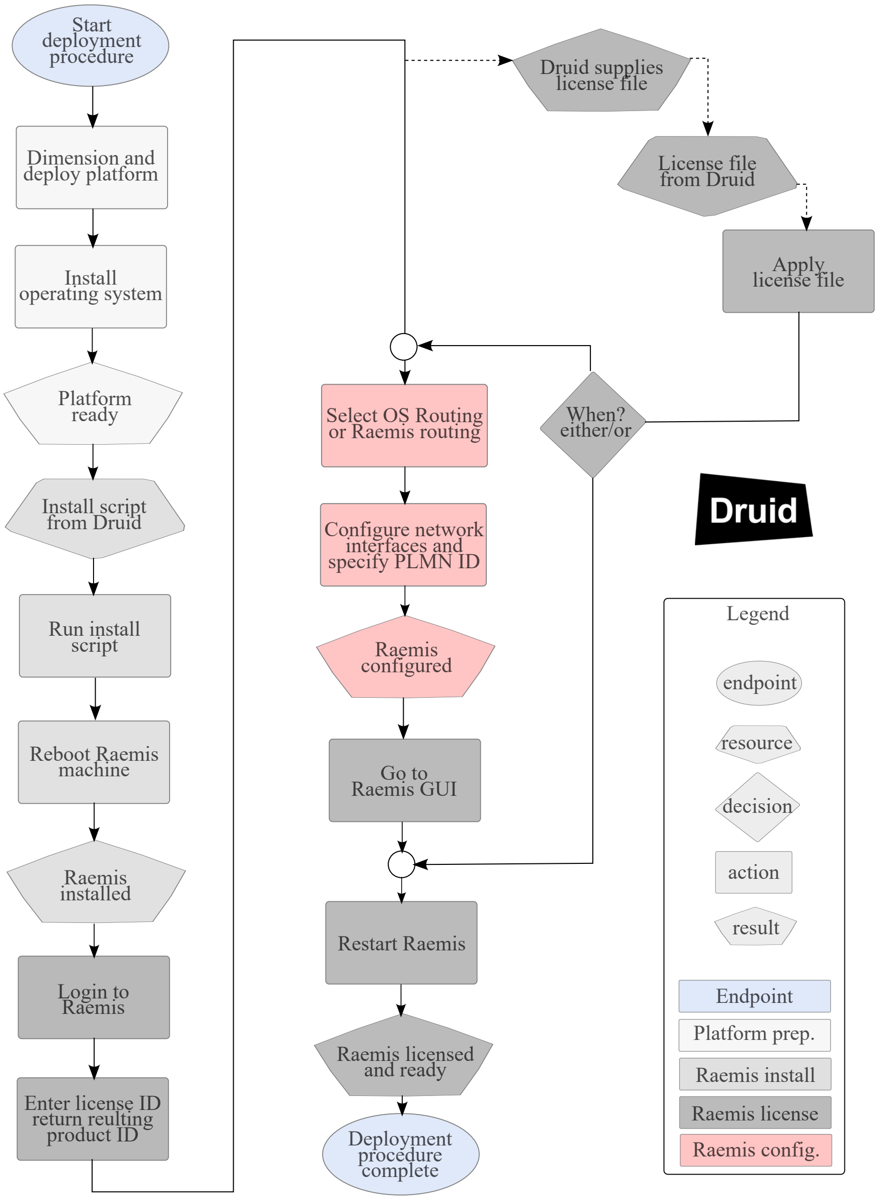


Figure 1: The installation procedure of the Druid Software 5G core [source: Druid].

2.2 Radio access network

The Radio Access Network (RAN) is part of 5GS which in general consists of a network of geographically distributed gNodeBs (gNBs). Each gNB consists of (i) a BaseBand Unit (BBU), which provides a set of computer-intensive signal processing functions that make wireless communication possible, and (ii) a radio part, including antennas, which converts digital information into signals that can be transmitted over-the-air and ensures that the transmitted signals are in the proper frequency bands with the right power levels. One gNB can consist of a BBU and one or multiple, geographically distributed radio units, also called Access Points (APs). The RAN part of 5GS makes on one hand wireless connectivity to User Equipments

(UEs), and on the other hand connectivity to the 5G core, i.e., to AMF component for control-plane and to UPF component for user-plane traffic.
When connecting the RAN to the 5G core network, the first step is the proper network configuration to ensure the connectivity between the BBUs and the 5G components, AMF and UPF, for control- and user-plane connectivity with the RAN, respectively. Besides network configuration, it is important to properly set the parameters such as peer and host IP addresses of the Control Plane (CP) and User Plane (UP) of the RAN and 5G core part.
After ensuring the basic connectivity between the RAN and the 5G core, several other important parameters need to be supported, set up, and aligned properly among the RAN, 5G core, and also UEs. Some of the parameters related to the RAN part are:

- frequency band (set up in RAN, supported by UEs),
- central frequency (set up in RAN, supported by UEs),
- division duplex configuration, i.e., Time Division Duplex (TDD) or Frequency Division Duplex (FDD) (set up in RAN, supported by UEs),
- Bandwidth (BW) (set up in RAN, supported by UEs),
- frame and slot configuration (in case of TDD) (set up in RAN, supported by UEs),
- Mobile Network Code (MNC) (set up in RAN, sim cards, and 5G core-UDM database),
- Mobile Country Code (MCC) (set up in RAN, sim cards, and 5G core-UDM database),
- Sub-Carrier Spacing (SCS) (set up in RAN, supported by UEs),
- 5G QoS Identifier (5QI) (set up in RAN, 5G core, and supported by UEs),
- slicing parameters (set up in RAN, 5G core and supported by UEs),
- Data Network Name (DNN) name (set up in 5G core and UEs),
- and other parameters depending on the configuration requirements.

The 5G RAN at SAL premises installed in the LIT Factory consists of a BBU 5900, RHUB 5963e and 3 pRRUs 5973 from Huawei.

2.3 5GS in LIT Factory

In Fig. 2 the 5GS integrated into an IP/Ethernet network in an industrial 5G testbed is shown.

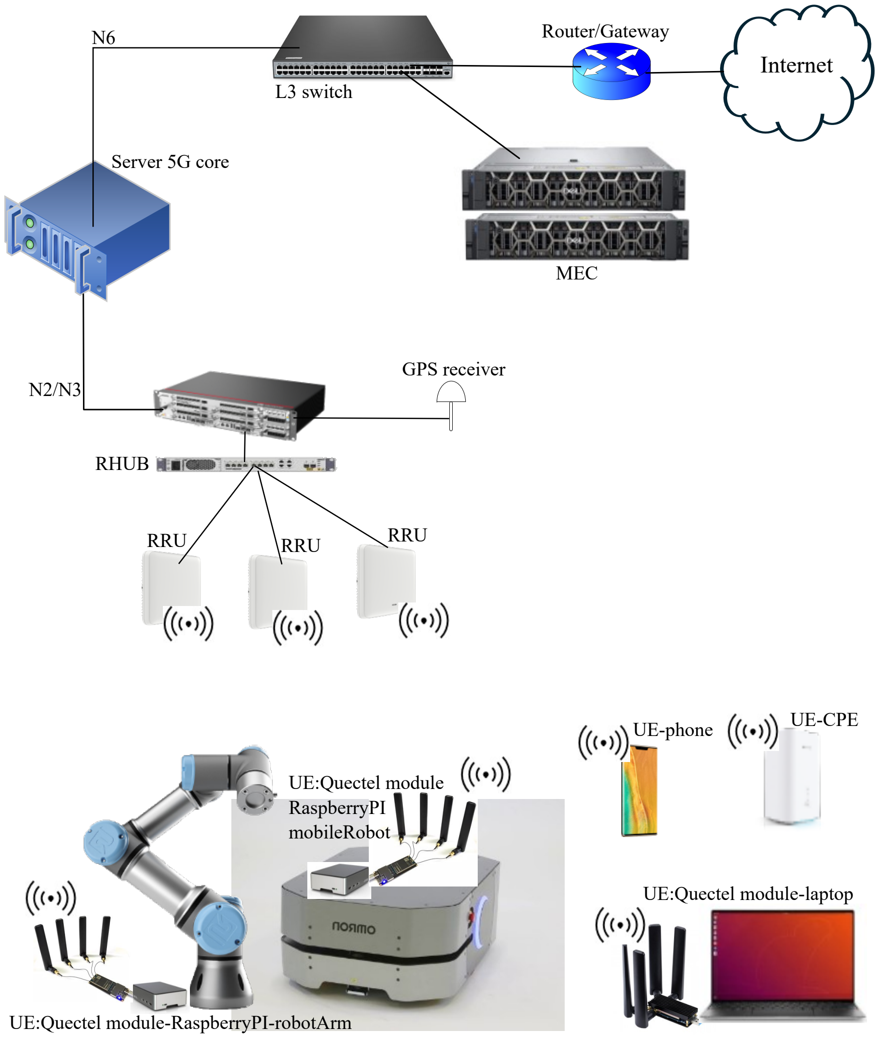


Figure 2: Integrated 5GS-IP/Ethernet network in an industrial testbed setup.

A typical procedure of a 5GS deployment can be summarized in several steps:

- The first step is the hardware network installation. This assumes the proper installation of the hardware components such as switches, routers, and operating system devices (servers) and proper cabling according to a defined setup/architecture, such as it is presented in Fig. 2. Regarding the physical setup, the important considerations are the hardware capabilities of the devices and the throughput requirements for the physical interfaces (e.g., 1G or 10G, copper or optical network interface).
- The second step is a proper network setup. This assumes network access and routing setup, remote access, firewalls and other security rules. In this stage,

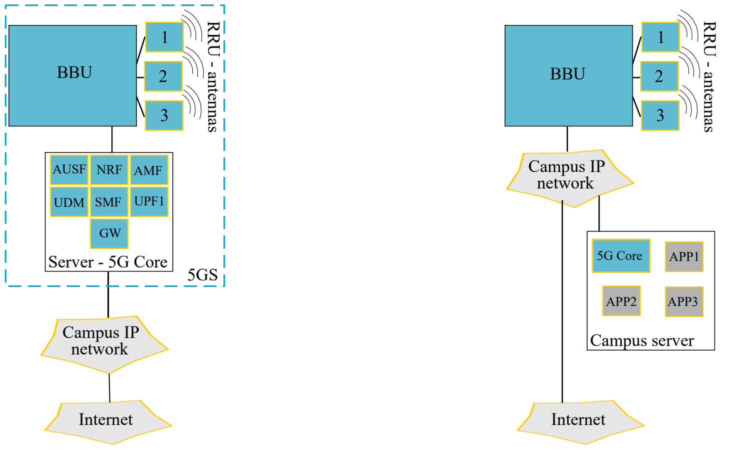
several tests should be made: connectivity and remote access, e.g., *ping* and network performance tests using tools such as *iperf*.

- After the verification of the hardware and network setup installation, the 5G core can be deployed, as explained in Section 2.1. After successful deployment, access to available interfaces of a running 5G core setup should be tested (e.g., using *ping*).
- The next step is the setup of the BBU of the 5G RAN. This assumes the proper network configuration (configuration of the physical interfaces and the 5G defined interfaces N2 and N3 which assumes host and peer IP addresses and port numbers). After this step, a registration of the gNB to the control plane of the 5G (N2 interface) should be checked from the RAN side or the 5G core side. The proper registration can be tested with packet trace tools, analyzing the NG Application Protocol (NGAP) packets over N2 interface. A successful NGAP session verifies that the control plane is properly setup in a gNB. It is important to align the 5G parameters between the gNB and the 5G core, as it is mentioned in Section 2.2.
- After the successful establishment of the control plane between the 5G core and the 5G RAN (N2 interface between the AMF and gNB), we can test the registration of a UE to the network. The verification of the successful registration to the network can be analyzed with a packet trace tool by analyzing the NGAP registration messages or in the GUI of the 5G core.
- The next step is the verification of the proper establishment of the user plane N3 interface between UPF and gNBs (5G RAN). It is used for establishing the GPRS Tunnelling Protocol - User data (GTP-U) tunnel on layer 3 of 5G protocol stack. The GTP-U tunnel is established during a Protocol data unit (PDU) session establishment between a UE and a DNN, over a UPF, which occurs after the UE registration procedure, mentioned in the previous step. The PDU session establishing procedure can be tracked and verified using a packet trace tool. From that trace of packets, the establishment of the GTP-U tunnel (user plane N3 interface between gNB and UPF) can also be verified. A PDU session supports one or more QoS flows and there is one-to-one mapping between a QoS flow and a QoS profile, i.e., packets belonging to the same QoS flow have the same 5QI. More about QoS will be described in 3.1. However, a proper setup of QoS flows can also be verified from the PDU session establishment procedure in a packet trace.
- After the successful establishment of the PDU session, we can perform End-to-End (E2E) connectivity (*ping*) and performance tests. The E2E here as-

sumes the connectivity between a UE and a UPF on the application level. The performance tests include throughput and latency tests. The throughput can be tested with *iperf*, which is a server-client-based tool, where we can test the Uplink (UL) and Downlink (DL) throughput and packet error rates for UDP and TCP streams. The one-way UL and DL and Round Trip Time (RTT) latency can be tested with Isochronous Round-Trip Tester (IRTT) or similar tools. For one-way latency measurements precise synchronization using Precision Time Protocol (PTP) between the end stations (server and client hosts) is a prerequisite.

3 Design guidelines on commissioning, integration, and overall system configuration

In the previous section, we focused on the setup and deployment of the 5GS itself. Here we will assume that the optimal 5GS has been deployed. First, we need to define the requirements of the overall system from the E2E perspective, where the 5GS is a part of the system. An example is the maximum one-way latency from an application on an end-station (a robot) to a control application on an edge computing platform, connected with the network side of the 5GS. Especially in industrial setups, it is often the case that there can be a high number of end stations where the applications are running and network devices, such as switches and routers. Depending on the scenario, the number of hops through the network can be from a single hop to several hundred hops, e.g., through switches, from one end station to another. This network can be a default Ethernet or the Time-Sensitive Networking (TSN) extension of it, in case of time-sensitive networking, high-reliability, or low-latency communication is a requirement for industrial processes. Therefore, the overall system with the integration of the 5GS into the external network of the industrial setup needs to be planned and the E2E performance of the overall system, and not only 5GS, needs to be tested accordingly. 3GPP specified the integration of the 5GS with the TSN for the support of E2E time-sensitive communication in Rel-16 [1]. This integration is described in detail in [3]. The greatest challenge in the integration of the 5GS with an external network, which is a wired network, is the inherently different behavior between the wireless and the wired channel in terms of Bit Error Rate (BER), packet loss, and channel variations, which translates to packet delay variation, reliability and capacity of the wireless interface. This leads to more complex planning of the available resources for the wireless interface, especially for mobile devices. The amount of resources required to guarantee specific communication requirements, such as reliability, latency, and throughput, can vary significantly, depending on the channel quality which is typically time-



(a) dedicated hardware for 5GS

(b) shared hardware for 5GS

Figure 3: 5G network configuration with a) dedicated and b) shared hardware

and spatial-variant. Therefore, it is important to define the worst-case communication scenarios to be able to plan the required amount of resources and to define the capacity of the network in each scenario. As aforementioned, in the planning phase, it is important to take into account the overall system, including 5GS and external networks in order to define the E2E capabilities.

3.1 Isolated vs. shared hardware setup for 5GS

Another important consideration regarding the integration of the 5GS into the IP/Ethernet network is the option for the physical integration of the 5GS with the external network(s). In general, there are two approaches: a completely isolated approach, where all the network devices and interfaces from 5GS are separated from the external network. In that case, there is only a gateway interface from the 5G core to the external network(s), while interfaces between the 5G core components and interfaces between the 5G core and RAN are physically isolated from the external network. This is a typical integration option for the 5GS, which guarantees the highest performance and security of the 5GS. However, in this option, all the hardware components, such as host machines, physical interfaces, and network devices (switches, routers) need to be dedicated to the 5GS only, which increases the investment costs and increases the number of hardware devices to be maintained. On the other side, a physical setup can be shared between the 5GS and the hardware and network devices on-premises. For example, a 5G core can be running in a virtualized environment on existing host machines if the host configuration and the 5G core deployment option allow it. In this case, the processing capabilities of the hardware need to be checked. The required resources need to be secured for the 5G core operations to not interfere with other applications. Similarly, depending on the network configuration on-premises, BBU from the 5G RAN part can be connected to the host machines where the 5G core runs over an existing Ethernet switch, a dedicated switch, or directly to host machines with deployed 5G core. In case the network interface between the 5G core and the RAN is shared with the same physical interface with other virtual interfaces non-related to 5GS, enough bandwidth in terms of throughput needs to be secured according to the 5GS requirements. Virtual interfaces sharing the same physical interface are usually separated by VLANs or similar means of network virtualization.

An example of an isolated deployment of the 5GS with dedicated hardware versus a physical setup with shared hardware components is shown in Fig. 3.

3.2 QoS in Ethernet/IP-5GS integrated network

3GPP TS 23.501 from [1], defines the 5G QoS model, which is based on QoS Flows. The QoS Flow is the finest granularity of QoS differentiation in a PDU Session. A QoS Flow ID (QFI) is the parameter used to identify a QoS Flow in the 5G System. The QFI may be dynamically assigned or may be equal to the 5QI. The 5QI is a scalar that is used as a reference to 5G QoS characteristics defined in [1] i.e. access node-specific parameters that control QoS forwarding treatment for the QoS Flow. Standardized 5QI values have one-to-one mapping to a standardized combination of 5G QoS characteristics as specified in Table 5.7.4-1 in [1]. In the 5G QoS model, there are both QoS Flows that require a guaranteed flow bit rate (GBR QoS Flows) and QoS Flows that do not require a guaranteed flow bit rate (Non-GBR QoS Flows). The same QFI within the same PDU session means the same traffic forwarding treatment (e.g., scheduling weights, admission thresholds, queue management thresholds, link layer protocol configuration, etc.) for the received user plane traffic. The 5G QoS characteristics for pre-configured 5QI values are pre-configured in the 5G RAN.

Besides 5QI, there are parameters such as Allocation and Retention Priority (ARP), Notification Control, Flow Bit Rate, Aggregate Bit Rate, and Maximum Packet Loss Rate [1].

ARP

The QoS parameter ARP contains information about the priority level, the pre-emption capability and the pre-emption vulnerability. This allows deciding whether a QoS Flow establishment/modification/handover may be accepted or needs to be rejected in the case of resource limitations (typically used for admission control of GBR traffic). It may also be used to decide which existing QoS Flow to pre-empt during resource limitations, i.e. which QoS Flow to release to free up resources.

The ARP priority level defines the relative importance of a QoS Flow. The range of the ARP priority level is 1 to 15 with 1 as the highest priority. The ARP pre-emption capability defines whether a QoS Flow may get resources that were already assigned to another QoS Flow with a lower priority. The ARP pre-emption vulnerability defines whether a QoS Flow may lose the resources assigned to it in order to admit a QoS Flow with higher priority. The ARP pre-emption capability and the ARP pre-emption vulnerability shall be either set to 'enabled' or 'disabled'.

Notification Control

The QoS Parameter Notification control indicates to the NG-RAN that notifications of "GFBR can no longer (or can again) be guaranteed" are requested when the NG-RAN determines that the Guaranteed Flow Bit Rate (GFBR), the Packet delay budget (PDB) or the Packet error rate (PER) of the QoS profile cannot be fulfilled (or can be fulfilled again) for a QoS Flow (during the lifetime of the QoS Flow) and that the QoS Flow should be kept while the NG-RAN is not fulfilling the requested QoS profile. Notification control may be used for a Guaranteed Bit Rate (GBR) QoS Flow if the application traffic is able to adapt to the change in the QoS (e.g. if the AF is capable of triggering rate adaptation).

Flow Bit Rate

For GBR QoS Flows only, there are additional QoS parameters, UL and DL GFBR and Maximum Flow Bit Rate (MFBR). The GFBR denotes the bit rate that is guaranteed to be provided by the network to the QoS Flow over the Averaging Time Window. The MFBR limits the bit rate to the highest bit rate that is expected by the QoS Flow (e.g. excess traffic may get discarded or delayed by a rate shaping or policing function at the UE, RAN, UPF). Bit rates above the GFBR value and up to the MFBR value may be provided with relative priority determined by the Priority Level of the QoS Flows. GFBR and MFBR are signaled to the RAN in the QoS Profile and signaled to the UE as QoS Flow level QoS parameter for each QoS Flow.

Aggregate Bit Rate

Each PDU Session of a UE is associated with the aggregate rate limit QoS parameter 'per Session Aggregate Maximum Bit Rate (AMBR)'. It is signaled to the appropriate UPF entity to the UE and to the RAN (to enable the calculation of the UE-AMBR). The Session-AMBR limits the aggregate bit rate that can be expected to be provided across all Non-GBR QoS Flows for a specific PDU Session. The Session-AMBR is measured over an AMBR averaging window which is a standardized value. The Session-AMBR is not applicable to GBR QoS Flows. Each UE is associated with the aggregate rate limit QoS parameter ’per UE Aggregate Maximum Bit Rate (UE-AMBR)’. The UE-AMBR limits the aggregate bit rate that can be expected to be provided across all Non-GBR QoS Flows of a UE. Each RAN shall set its UE-AMBR to the sum of the Session-AMBR of all PDU Sessions with active user plane to this RAN up to the value of the UE-AMBR received from AMF. The UE-AMBR is a parameter provided to the RAN by the AMF based on the value of the subscribed UE-AMBR retrieved from UDM or the dynamic serving network UE-AMBR retrieved from PCF (e.g., for roaming subscriber). The AMF provides the UE-AMBR provided by PCF to RAN if available. The UE-AMBR is measured over an AMBR averaging window which is a standardized value. The UE-AMBR is not applicable to GBR QoS Flows. Each group of PDU Sessions of the UE for the same slice (Single Network Slice Selection Assistance Information (S-NSSAI)) may be associated with the aggregate rate limit QoS parameter ’per UE per Slice-Maximum Bit Rate (MBR)’. The UE-Slice-MBR limits the aggregate bit rate that can be expected to be provided across all GBR and Non-GBR QoS Flows corresponding to PDU Sessions of the UE for the same slice (S-NSSAI) which have an active user plane. Each supporting NG-RAN shall set its UE-Slice-MBR to the sum of the Session-AMBR and MFBR for GBR QoS Flows of all PDU Sessions corresponding to the slice (S-NSSAI) with active user plane to this NG-RAN up to the value of the UE-Slice-MBR corresponding to the slice (S-NSSAI) received from AMF. The UE-Slice-MBR is measured over an AMBR averaging window which is a standardized value. The UE-Slice-MBR is an optional parameter provided to the NG-RAN by the AMF [1].

Maximum Packet Loss Rate

The Maximum Packet Loss Rate (UL, DL) indicates the maximum rate for lost packets of the QoS Flow that can be tolerated in the UL and DL direction. This is provided to the QoS Flow if it is compliant to the GFBR.
For each 5QI, there are defined performance characteristics such as resource type (GBR or non-GBR), Priority Level, PDB, PER, Maximum Data Burst Volume (MDBV) (for some GBR QCIs), Averaging Window (for GBR and Delay-critical GBR resource type only), and Maximum Data Burst Volume (for Delay-critical GBR resource type only).

Resource Type

The Resource Type determines if dedicated network resources related to a QoS Flow-level Guaranteed Flow Bit Rate (GFBR) value are permanently allocated (e.g., by an admission control function in a radio base station). GBR QoS Flows are therefore typically authorized "on demand" which requires dynamic policy and charging control. A GBR QoS Flow uses either the GBR resource type or the Delay-critical

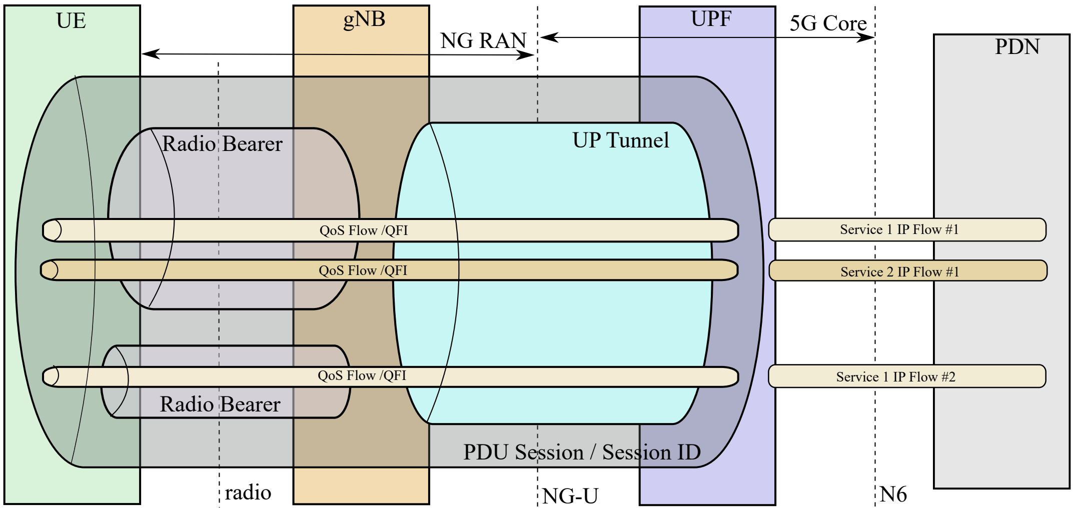


Figure 4: 5G QoS Flow diagram.

GBR resource type. The definition of PDB and PER are different for GBR and Delay-critical GBR resource types, and the MDBV parameter applies only to the Delay-critical GBR resource type. A Non-GBR QoS Flow may be pre-authorized through static policy and charging control. A Non-GBR QoS Flow uses only the Non-GBR resource type [1].

Priority Level

The Priority Level associated with 5G QoS characteristics indicates a priority in scheduling resources among QoS Flows. The lowest Priority Level value corresponds to the highest priority. The Priority Level shall be used to differentiate between QoS Flows of the same UE, and it shall also be used to differentiate between QoS Flows from different UEs. In the case of congestion, when all QoS requirements cannot be fulfilled for one or more QoS Flows, the Priority Level shall be used to select for which QoS Flows the QoS requirements are prioritized such that a QoS Flow with Priority Level value N is prioritized over QoS Flows with higher Priority Level values (i.e., N+1, N+2, etc.). In the case of no congestion, the Priority Level should be used to define the resource distribution between QoS Flows. In addition, the scheduler may prioritize QoS Flows based on other parameters (e.g., resource type, radio condition) to optimize application performance and network capacity. Every standardized 5QI is associated with a default value for the Priority. Priority Level may also be signaled together with a standardized 5QI to the RAN, and if it is received, it shall be used instead of the default value. Priority Level may also be signaled together with a pre-configured 5QI to the RAN, and if it is received, it shall be used instead of the pre-configured value [1].

Packet Delay Budget

The PDB defines an upper bound for the time that a packet may be delayed between the UE and the N6 termination point at the UPF. For a certain 5QI the value of the PDB is the same in UL and DL. In the case of 3GPP access, the PDB is used to support the configuration of scheduling and link layer functions (e.g., the setting of scheduling priority weights and Hybrid Automatic Repeat reQuest (HARQ) target operating points). For GBR QoS Flows using the Delay critical resource type, a packet delayed more than PDB is counted as lost if the data burst does not exceed the MDBV within the period of PDB and the QoS Flow is not exceeding the GFBR. For GBR QoS Flows with GBR resource type not exceeding GFBR, 98 percent of the packets shall not experience a delay exceeding the 5QI's PDB [1].

Packet Error Rate

PER defines an upper bound for the rate of PDUs (e.g., IP packets) that have been processed by the sender of a link layer protocol (e.g., Radio Link Control (RLC) layer in RAN of a 3GPP access) but that are not successfully delivered by the corresponding receiver to the upper layer (e.g., Ppacket data convergence protocol (PDCP) in RAN of a 3GPP access). Thus, the PER defines an upper bound for a rate of non-congestion related packet losses. The purpose of the PER is to allow for appropriate link layer protocol configurations (e.g., RLCand HARQ in RAN of a 3GPP access). For every 5QI the value of the PER is the same in UL and DL. For GBR QoS Flows with Delay-critical GBR resource type, a packet that is delayed more than PDB is counted as lost and included in the PER unless the data burst exceeds the MDBV within the period of PDB or the QoS Flow exceeds the GFBR [1].

E2E QoS

Here it is important to mention that the mechanisms to provide the required QoS and differentiate applications/users/flows based on their requirements are defined within the 5GS. However, the traffic that goes through the 5GS from the UE to the UPF and vice versa passes through the IP/Ethernet network, which is beyond the scope of the 5GS. This means that the QoS mechanisms need to be translated from the 5GS to the IP/Ethernet network to keep the performance characteristics differentiated outside of 5GS. Otherwise, we have the QoS service only in a part of the communication system, and not on the E2E level. To have the E2E QoS for a service, the Backbone IP/Ethernet network needs to have implemented its QoS mechanisms that are translatable with the QoS mechanisms from the 5GS. Some of those mechanisms in the IP/Ethernet networks are:

- *IntServ* - uses the Resource Reservation Protocol (RSVP) to reserve the BW and resources for each QoS flow,
- *DiffServ* - marks packets into different classes and applies different policies based on their class,
- Multi-Protocol Label Switching (MPLS) uses labels to route packets along predefined paths and apply different QoS levels based on their label.

Regardless of the chosen method of QoS mechanisms implementation, all the network elements along a QoS flow need to support a QoS mechanism to have an E2E QoS service. Moreover, depending on the complexity of the Backbone network, different methods could be used in different parts of the network to provide E2E QoS service.

4 Conclusions

This deliverable provides an overview of the 5G campus networks. The deployment options of the 5GS were mentioned, and options for the 5G core software deployment were explained. The main contribution of the document is the provided guidelines on the 5GS deployment, testing, and commissioning procedures based on an example deployment of the industrial 5GS testbed setup, deployed within this project. In section 2 the 5G core deployment options were explained and an example deployment procedure and feature list of the Druid Software 5G core was provided. Moreover, the 5G RAN with the most important parameters, which need to be aligned with UEs on one side and the 5G core on the other side, were presented. The network setup, with the deployed 5GS in LIT Factory, was presented as a block diagram, and the guideline on the 5GS deployment was provided at the end of the section. In section 3, the overall system from the E2E perspective, including the 5GS and the external networks, with a focus on the E2E QoS, was analyzed. The 5G QoS working principle and the main parameters were presented and the importance of the E2E QoS in an integrated 5GS into an external network was explained. Moreover, the isolated and shared 5GS deployment options were compared.

Acronyms

3GPP 3^{rd} generation Partnership Project. 3

5GS 5G System. 3, 7

5QI 5G QoS Identifier. 8, 10, 13, 16, 17

AMBR Aggregate Maximum Bit Rate. 14

AMF Access and Mobility management Function. 6, 8, 15

AP Access Point. 7

ARP Allocation and Retention Priority. 13

BBU BaseBand Unit. 7, 8

BER Bit Error Rate. 11

BW Bandwidth. 8, 18

CP Control Plane. 8

DL Downlink. 11

DNN Data Network Name. 8, 10

E2E End-to-End. 10, 11

FDD Frequency Division Duplex. 8

GBR Guaranteed Bit Rate. 14

GFBR Guaranteed Flow Bit Rate. 14, 17

gNB gNodeB. 7

GTP-U GPRS Tunnelling Protocol - User data. 10

HARQ Hybrid Automatic Repeat reQuest. 17

IMS IP multimedia Subsystem. 6

IoT Internet-of-Things. 3

IRTT Isochronous Round-Trip Tester. 11

KPI Key Performance Indicator. 3

MBR Maximum Bit Rate. 15

MCC Mobile Country Code. 8

MDBV Maximum Data Burst Volume. 15–17

MFBR Maximum Flow Bit Rate. 14

MNC Mobile Network Code. 8

MPLS Multi-Protocol Label Switching. 18

NGAP NG Application Protocol. 10

PCF Policy control function. 6, 15

PDB Packet delay budget. 14–17

PDCP Ppacket data convergence protocol. 17

PDU Protocol data unit. 10, 13

PER Packet error rate. 14–17

PTP Precision Time Protocol. 11

QFI QoS Flow ID. 13

QoS Quality of Service. 6, 10, 13

RAN Radio Access Network. 7

REST Representational State Transfer. 5

RLC Radio Link Control. 17

RRU remote radio unit. 3, *Glossary:* RRU

RSVP Resource Reservation Protocol. 18

RTT Round Trip Time. 11

S-NSSAI Single Network Slice Selection Assistance Information. 15

SA Standalone. 4

SCS Sub-Carrier Spacing. 8

SMF Session Management Function. 6

SMSF Short Message Service Function. 6

TDD Time Division Duplex. 8

TSN Time-Sensitive Networking. 11

UDM Unified Data Management. 6, 15

UE User Equipment. 7, 8, 10

UL Uplink. 11

UP User Plane. 8

UPF User Plane Function. 6, 8, 10, 17

Glossary

RRU	Commonly referred to as a remote radio head (RRH), is a transceiver that can be found on wireless base stations.. 3

References

[1] 3GPP. *TS 23.501: Technical Specification Group Services and System Aspects, System architecture for the 5G System (5GS)*. Release-18, v18.0.0. 2022.

[2] 5GEARING. *Guidelines on 5G campus network deployment, configuration, radio placement, and frequency planning*. Release-18, v18.2.0. 2021.

[3] Mahin K. Atiq et al. “When IEEE 802.11 and 5G Meet Time-Sensitive Networking”. In: *IEEE Open Journal of the Industrial Electronics Society* 3 (2022), pp. 14–36. DOI: `10.1109/OJIES.2021.3135524`.