



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

D2.2: GUIDELINES ON 5G CAMPUS NETWORK DEPLOYMENT, CONFIGURATION, RADIO PLACEMENT, AND FREQUENCY PLANNING



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:	D2.2
Deliverable full title:	Guidelines on 5G campus network deployment, configuration, radio placement, and frequency planning
Deliverable short title:	5G deployment guidelines
Submission date:	15.04.2024
Status:	Final
Lead Author(s):	Raheeb Muzaffar (SAL)
Co-author(s):	Mahin Ahmed (SAL)
	Damir Hamidovic (SAL)
	Clemens Gamsjaeger (Magna)
	Alexander Heinz (Cancom)
	Markus Dietinger (Cancom)
	Fjolla Ademaj-Berisha (SAL)
	Markus Raab (Liwest)

Table of Contents

1	Executive Summary	3
2	Introduction	4
2.1	Objective of the report	5
2.2	Structure of the document	6
3	What are campus networks?	6
3.1	Architecture	6
3.2	Benefits of campus networks	8
4	Campus network deployment options	8
4.1	Isolated deployment	9
4.2	Public network integrated NPN	10
4.2.1	Shared access network	11
4.2.2	Shared access network and control plane	11
4.2.3	Hosted by the public network operator	11
4.3	Security and privacy	12
4.3.1	Isolated deployment	13
4.3.2	Public network integrated NPN	13
4.3.3	Network slicing	14
4.4	Comparison and trade-off	14
4.5	Features and capabilities	18
4.5.1	Network slicing	18
4.5.2	5G QoS Support	19
4.6	5G support for industrial networks	20
4.6.1	Time-sensitive networking	20
4.6.2	Deterministic Networking	22
4.6.3	5G - OPC UA	23
4.6.4	Edge computing	25
5	5G network configuration	28
5.1	5G CORE	30
5.1.1	Fraunhofer 5G core	31
5.1.2	QoS parameters	32
5.2	Radio access network	33
5.3	User equipment options and features	34
5.3.1	Devices with User Interface	34
5.3.2	Mobile Routers	35
5.3.3	Radio Modem Module	35

6	Radio placement	36
6.1	Summary of requirements	36
6.2	Simulation results	36
6.2.1	General considerations on antenna placement, cells and sectors	36
6.2.2	Reference Signal Received Power (RSRP)	39
6.2.3	Signal to Interference plus Noise Ratio (SINR)	39
6.2.4	Downlink Throughput	39
6.3	Discussion on the simulation results	40
6.3.1	Interference	40
6.3.2	Available spectrum	40
6.3.3	Base Station architecture	41
6.3.4	Improved coding techniques	41
7	Spectrum for campus networks	41
7.1	Unlicensed spectrum	41
7.2	Licensed spectrum	42
7.2.1	Frequency planning in Austria	42
7.3	Shared spectrum	42
7.4	Millimeter wave spectrum	43
8	Conclusions	43

1 Executive Summary

The digital transformation of Industry 4.0 is driven by the automation of manufacturing processes. In this context, communication plays a vital role and the emergence of 5G wireless technology brings the promise of connectivity scenarios like the industrial internet of things and industrial cyber-physical systems. However, there are still several aspects to consider on how to employ 5G in practical industrial environments such that the highly demanding communication requirements of the use cases can be fulfilled. This report aims to review the essential enabling technologies of 5G with the primary focus on studying 5G non-public network variants, the potential of network slicing, multi-access edge computing infrastructure, and 5G integration with deterministic communication technologies including time-sensitive networking, deterministic networking, and open platform communications unified architecture. An evaluation of different 5G network deployment options with relevant example use cases is carried out. A critical analysis of available results suggests that these technologies can effectively facilitate ubiquitous wireless industrial communication, despite the stringent needs of industrial applications, including support of different quality of service levels and security requirements. Furthermore, network configuration options on CORE, RAN, and UE are discussed. The report also presents simulation results considering radio placement strategies to understand the capacity and limitations of the 5G system. Lastly, the report discusses frequency spectrum opportunities for campus networks.

2 Introduction

The digital transformation of the industrial processes together with the advent of Industry 5.0 emphasizing sustainability, resilience, and a human-centric approach is expected to bring a radical change to the manufacturing industry. A growing trend of providing connectivity both within companies' production systems and along the value chain is visible. This includes connectivity between and among goods, enabling communication capabilities during production and after-sales. This trend is closely related to the ever-increasing volume of data being collected and processed across different levels of industrial systems. Another noticeable trend is the shift in the industrial [information technology \(IT\)](#) systems hard- and software infrastructure, moving away from the traditional rigid server-based framework to cloud-based solutions. This transition allows for greater flexibility in terms of underlying computer systems, software tool hosting, and software framework scalability. It encompasses a range of options, from a local cloud near the shop floor to a company-owned [IT](#) cloud or a remotely hosted software-as-a-service solution. Proper communication systems play a crucial role in supporting these trends. Particularly, ubiquitous connectivity is required. Current shop floor networks, often referred to as [operational technology \(OT\)](#), have traditionally relied on wired connections for real-time performance and reliability. However, these networks are necessarily limited in spatial extension, number of devices, and flexibility. Wireless communications could offer increased flexibility and support for mobile devices, but their adoption has been limited due to concerns about latency and reliability. To reduce the heterogeneity of [OT](#) networks and to support the Industry 4.0 trends, [5th generation \(5G\)](#) mobile networks are a much-debated option [70]. Although the true impact of [5G](#) was still uncertain in 2018 [15], its visibility and perception within the industry has increased significantly in recent years. Several interest groups such as the [5G alliance for connected industries and automation](#) ([5G-ACIA](#)) and alliance for internet of things innovation [alliance for internet of things innovation \(AIOTI\)](#), have been founded to explore the potential of the technology. In the context of industrial automation, [5G](#) aims to provide support for diverse communication requirements of [OT](#) applications. To achieve this, so-called verticals have been defined that represent systems of end-user entities belonging to a particular application domain. These verticals utilize the end-to-end communication services offered by the underlying [5G](#) network, which are tailored to meet the specific user requirements of the application area. For industrial automation, the factories of the future vertical [5] define requirements such as guaranteed latencies below 5 ms, reliability, and device densities of up to 100 devices/m² as the key performance targets. These tar-

gets are notably ambitious compared to current mobile communication standards, but if realized, they would serve as a solid foundation for meeting the industrial automation requirements. It must be highlighted that an analysis of different 5G deployment opportunities for the industrial domains is one of the main concerns. It requires a careful evaluation that not only is limited to the technical aspects but also its feasibility and effectiveness for the application at hand. Indeed, industrial needs are so peculiar that efforts have been made in the recent past to overcome the usual, auction-based, approach for frequency assignment in favor of dedicated allocation (as already done in Germany), promoting companies to embrace private 5G networks. In particular, different deployment opportunities lead to different results regarding the fulfillment of industrial communication needs, service customization, and integration with legacy and already-in-place (wireless and wired) networks.

This deliverable report provides a survey of the current state of play in the development of 5G with a particular view on its applicability in industrial automation. 5G offers the necessary flexibility to cater to a wide range of Industry 4.0 applications. This includes the ability to adapt and configure the system in various ways such as the configuration of network slices with varying quality of service (QoS). Additionally, 5G supports multiple deployment options to provide the best possible applicability of the system. The 5G campus network and its variants is a recent development in cellular systems that allow more flexibility for industrial networks and are comprehensively discussed in this report.

2.1 Objective of the report

This report provides a comprehensive study on 5G deployment models including the cloud-native approaches. It suggests example use cases that align with each category. A qualitative analysis of these deployment models considering factors such as cost, network customization and adaptability, data ownership, reliability, availability, deterministic communication support, security, privacy, and data monitoring is also presented. Additionally, the focus is placed on the main enablers, such as network slicing, multi-access edge computing (MEC), time-sensitive networking (TSN), open platform communications unified architecture (OPC UA), and QoS provisioning. These enablers are discussed in accordance with the state-of-the-art design trends according to 3rd generation partnership project (3GPP) release-16, 17, and 18 that support I4.0 use cases and their stringent communication requirements. The report also reviews 5G security concepts aligned with the 5G private networks and analyzes real-world 5G deployments for I4.0 use cases. Lastly, the report also provides key insights on core, radio access network (RAN), and user equipment (UE) configurations as well as considerations on radio placement and

spectrum options for campus networks. The objective of this report is to understand the state of play of 5G, supporting technologies, and their integration with 5G for industrial systems.

2.2 Structure of the document

The deliverable report is structured as follows: Chapter III gives an overview of the 5G campus networks and basic 5G architecture. Chapter IV presents various 5G network deployment choices and evaluates these options against multiple attributes. It also describes features and capabilities to support network quality of service and provides an overview of 5G support for industrial networks through integration with TSN, Deterministic Networking (DetNet), and OPC UA. Moreover, edge computing facility to support factories of the future is also discussed. Chapter V discusses 5G network configuration insights from the CORE, RAN, and UE perspective. Chapter VI presents radio cell placement configuration in a factory environment and corresponding simulation results on interference and throughput. Lastly, chapter VII discusses spectrum options for campus networks. Finally, chapter VII concludes the report.

3 What are campus networks?

Campus networks are small, local networks dedicated to a set geographical area. They can provide coverage from a few hundred square meters indoors to a few square kilometers outdoors. In contrast to a public mobile network, usage of a campus network is restricted to people or devices affiliated with the campus area and therefore, can quickly be adapted to changing connectivity needs. Moreover, they can also be connected to public networks. 5G campus networks help mobile operators and enterprises to further improve their network security, flexibility, and reliability for their respective applications.

3.1 Architecture

5G was first introduced in 3GPP release-15. To allow early access to the new technology, the 5G new radio (NR) interface was deployed in conjunction with the existing long term evolution (LTE) core and radio access network. Such a network architecture was termed as non standalone (NSA) architecture. The NSA solution enabled the use of 5G NR without the need for a complete network replacement to support higher data rates compared to LTE. Later, the 5G standalone (SA) architecture was introduced to enable the NR to connect to the 5G core network. The 5G SA

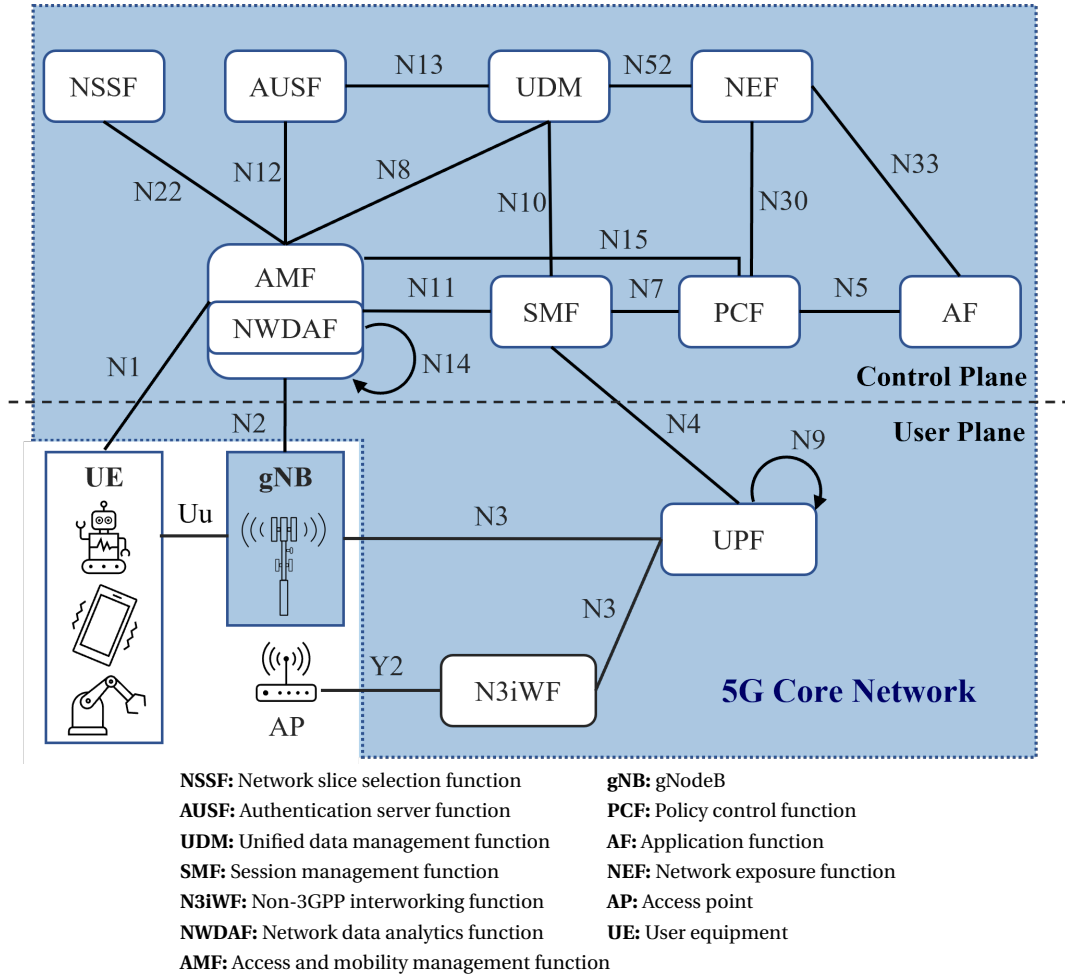


Figure 1: 5G standalone reference point system architecture [1]. The numbers N# denote point-point interfaces between network elements. Y2 is an interface to untrusted non-3GPP access and Uu is a wireless interface to the UEs.

core architecture allows virtualization that introduces new ways to develop, deploy, and manage its services.

The 5G SA architecture is depicted in Fig. 1, where the core network functionalities are separated into the control and user plane functions allowing capacity scaling and flexibility in the deployment topology. The control plane carries communication signaling and control traffic required for network access and resource allocation to the UE, whereas the user plane carries the data traffic. The access network includes the UE and the gNodeB (gNB).

The control plane comprises functions such as the access and mobility management function (AMF), session management function (SMF), and policy control function (PCF), while the user plane function (UPF) belongs to the user plane. The UPF is responsible for packet routing and forwarding, enforcing QoS policies, and facilitating efficient and secure communication between different network elements. The AMF handles connection and mobility management tasks including access

authentication and authorization of the **UE** and manages handovers between the **gNBs**. The 5G system architecture contains reference points between the network elements labeled by numbers N# in Fig. 1. The N1 interface is used for transmitting non-radio signaling between the **UE** and the **AMF** to handle messages related to connection and mobility but forwards session management information to the **SMF**. The **SMF** performs the session management functions such as allocation of IP addresses to UEs, selection and control of **UPF** for traffic routing, and signaling of **QoS** and policy information to **RAN** via the **AMF**. The N2 interface supports control plane signaling between the access network (**gNB**) and the core network for **UE** context and **protocol data unit (PDU)** session/resource management procedures. The **PCF** provides policy rules to **SMF** that include **QoS** policy and charging control, network slicing, as well as roaming and mobility management. The **network slice selection function (NSSF)** role is to provide network slice information to **AMF** that will serve a particular **UE**. More details on the 5G functions can be found in 3GPP specifications [1].

3.2 Benefits of campus networks

The 5G core architecture relies on a **service based architecture (SBA)** framework that exposes the functionality of the core elements to each other. Thus diverse application scenarios can be serviced using core deployment flexibility and configuration options. Because the application requirements may vary, a different setup of the 5G network may provide preferable services. As an example, in an industrial or manufacturing environment, deployment of a **non public network (NPN)** (isolated deployment) may be more suitable compared to other options for applications that require precision control or near real-time communication. A **public network integrated NPN (PNI-NPN)** requires lower deployment and maintenance costs compared to an isolated deployment. Nonetheless, an isolated deployment has advantages in terms of robustness, availability, security, data privacy, and network scalability as the resources and components can be controlled locally.

4 Campus network deployment options

In the following, we present various 5G network deployment options and their characteristics as presented in fig. 2. Note that for each deployment option, the control and user plane separation is depicted in fig. 1 with its functionality details. The advantage of the 5G **SA** architecture also lies in the flexibility of the deployment option. Moreover, in each deployment option, the possibility to include **MEC** facility is open. The 5G **MEC** configuration is further discussed in Section 4.6.4.

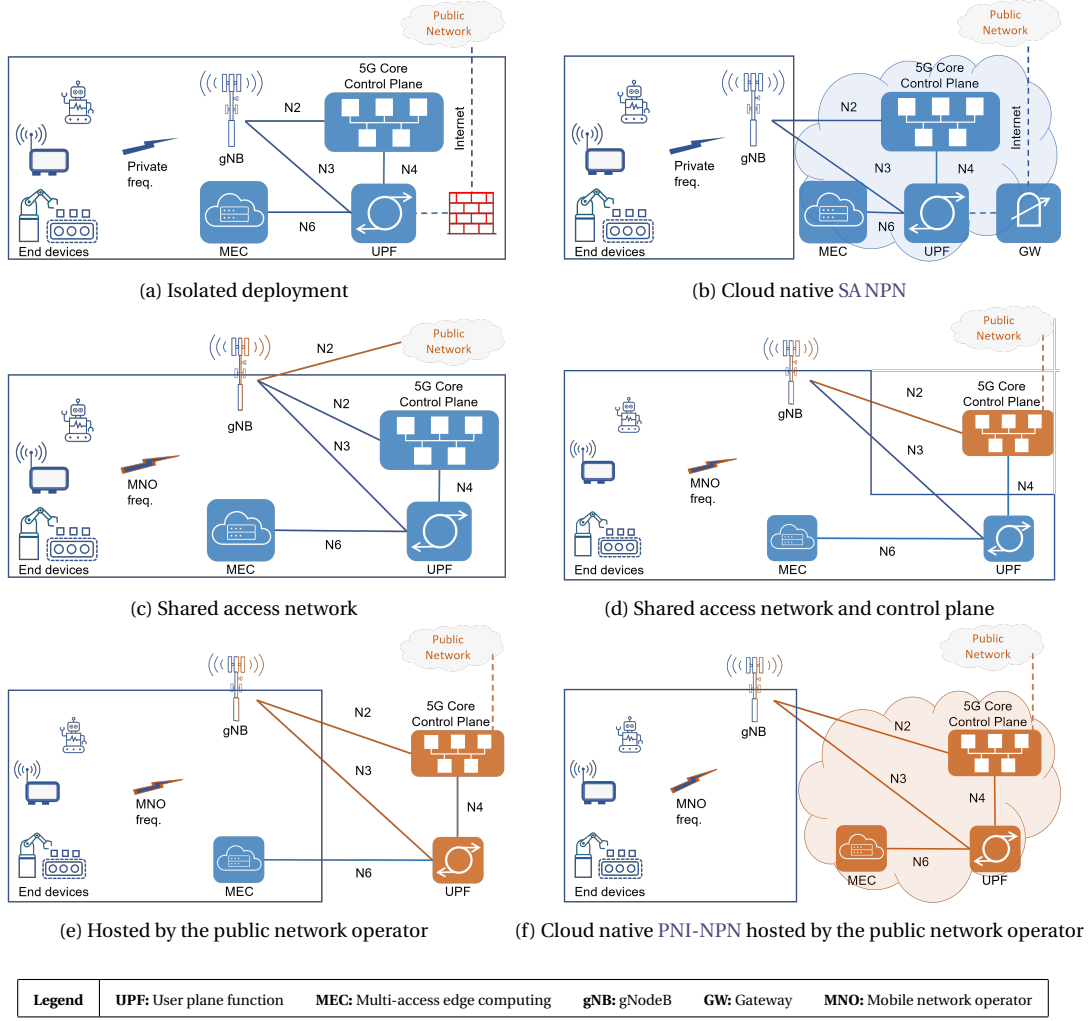


Figure 2: 5G non public network deployment options adapted from [2, 47]. A detailed 5G system component architecture is presented in Fig. 1. The network components and interfaces for campus network deployment are shown in blue whereby the public network components and interfaces are shown in orange.

4.1 Isolated deployment

An isolated deployment - also denoted with aliases such as private network and campus network - is formally known as **NPN** according to the 3GPP specifications [1]. A **NPN** could either be a **SANPN** or **PNI-NPN**. **PNI-NPN** versions are further discussed in section 4.2.

A **SANPN** is a private deployment of a 5G system (5GS) including the RAN and the core network elements where access to the network infrastructure is exclusive to authorized devices (fig. 2 a). An **SANPN** is identified by a combination of **public land mobile network (PLMN)** ID and **network identifier (NID)**. One advantage of such a deployment is data security due to its physical separation from the public

network. Also due to the proximity of the application server, minimal network delays between the devices are experienced, allowing better support for **ultra-reliable low latency communication (uRLLC)** service. However, such a network deployment does not support roaming between other **SA NPNs**. Similarly, interactions such as handovers between **SA NPNs**, **PNI-NPNs**, and **PLMNs** are not supported [1]. The end devices, though, can still have a dual subscription to access services from a **PLMN** [2]. Additionally, a connection between the **SA NPNs** and **PLMN** can optionally be set up via a firewall.

The **SA NPN** enhancements for neutral host deployment are further provided in release-17 where a **UE** subscribed to a **PLMN** or another **SA NPN** can be configured in access mode to operate with a given **SA NPN**. The support of neutral hosts is provided by the **SA NPN** by broadcasting an indication that the registration attempts from **UEs** that are not explicitly configured with the current **SA NPN** are allowed. Furthermore, a **UE** may have multiple **SA NPN** subscriptions but the order in which the **UE** should attempt for registration with a **SA NPN** is undefined and implementation dependent. Moreover, emergency services are supported in **SA NPN** access mode.

A **SA NPN** remains exclusive to an organization such as an industrial site (e.g., a warehouse or a production plant) enabling dedicated coverage, network control, and customized service availability [7]. The number of **base stations (BSs)** can also be scaled according to the capacity and coverage requirements. Moreover, connectivity with **MEC** system for computing and storage purposes can also be provisioned [25]. An **SA NPN** can be deployed in various ways, including a cloud-native approach where the control plane, user plane, and edge computation services are hosted in the cloud (fig. 2 b). Such a deployment option is appropriate for small enterprises offering reduced capital and operational costs. Although it is valid for both multi-site and single-site scenarios, it is more suitable for connecting an enterprise having multiple locations. However, it may not be suitable for enterprises requiring high data privacy, as enterprise traffic leaves the premises in a cloud-native approach.

4.2 Public network integrated NPN

The **PNI-NPN** deployment options combine parts of the public cellular network to locally installed elements of a private network. In a **PNI-NPN**, a **closed access group (CAG)** may optionally be created to allow network access to authorized **UEs**. This helps in avoiding overload of network resources by restricting network access to authorized **UEs** only (3GPP TS 22.261). A **CAG** cell identified by a **CAG ID** is unique within a **PLMN**. A **PLMN** is identified by a **PLMN ID**. A **CAG** cell may have one or multiple **CAG** identifiers per **PLMN** whereby a **UE** can gain access to a **CAG** cell if it

is configured with a list of allowed CAG identifiers.

In the following, we present PN-NPN deployment options that share public network resources.

4.2.1 Shared access network

One deployment option for a PN-NPN is to share the RAN deployed for a public network with the NPN core network as suggested in 3GPP TS 23.251 (fig. 2 c). In such a deployment, despite shared use of the RAN, all data flows of the NPN remain segregated within the perimeters of the premises, e.g., at an industrial site [7, 2]. This is because the UEs belonging to PN-NPN and those belonging to PLMN deliver data traffic to their respective UPFs. However, an agreement with a public network counterpart is required on RAN sharing. Despite shared use of the RAN, it is difficult to compromise the data security of the private network at the RAN level. Also, uRLLC can still be achieved due to low communication delay between the UEs, RAN, UPF, and MEC.

4.2.2 Shared access network and control plane

The shared access network and control plane PN-NPN deployment option share the RAN with a public network, while the control plane network functions are completely handled using the public infrastructure, e.g., of a mobile network operator (MNO) [7, 2, 47] (fig. 2 d). However, a private and dedicated user plane along with the MEC can be part of the private network. The UPF and MEC are thus physically separated and placed in the private campus, while the 5G core functions are logically separated and shared. Due to this physical separation of the UPF and MEC, NPN traffic flows remain within the logical perimeters of the premises allowing uRLLC for industrial use cases. However, the NPN devices remain subscribers of the public network by definition. The segregation of the traffic from a public network and NPNs can be configured by means of defining network slices. Alternatively, the 3GPP defined access point name (APN) feature can be used to configure this deployment scenario [2]. An APN comprises a data network identifier and an operator identifier. The data network identifier specifies the gateway to connect while the operator identifier specifies the MNO with which the gateway is associated. An APN configuration for this scenario also allows identifying and separating NPN traffic from public network traffic.

4.2.3 Hosted by the public network operator

A NPN can also entirely be hosted by a public network operator [7, 2, 47] (fig. 2 e). In this scenario, NPN traffic no longer remains within the logical perimeters but is

routed towards the **PLMN** via the shared **RAN**. The separation of the traffic from **NPN** and public devices can be enforced through network slicing configured and defined by the **MNO**. Similar to the shared access network and control plane **PNI-NPN**, an **APN** can also be defined for this deployment option [2].

Another variant of this deployment could be a cloud-native approach where the enterprise customers share the **RAN** deployed for a public network, however, the control plane, user plane, and edge services can be deployed in a cloud separated from the traditional **MNO** premises (fig. 2 f). Such deployment would keep traffic segregation between public and non-public networks, although solutions based on **APN** or network slicing can be applied to support multiple private customers.

4.3 Security and privacy

Typical for mobile networks, 5G has its own security concept designed for standalone installations (3GPP TS 33.501), but when 5G is deployed in an **industry 4.0 (I4.0)** factory environment, it faces an environment characterized by existing legacy wired and wireless communication systems [70]. In these environments, 5G is not the only network but has to be integrated according to the deployment type and security requirements of the specific use case. In most cases, **I4.0** state-of-the-art security concepts follow a defense in depth approach that has been proposed almost two decades ago [67] and is elaborated in detail in the IEC 62443 standard entitled *Industrial communication networks - Network and system security*. IEC 62443 assigns network segments with similar security requirements to zones. The links between zones are called conduits that are implemented vertically and in specific cases horizontally. The vertical conduits interconnect **OT** with **IT** domains or different **security level (SL)** domains and zones. It is common to think of conduits as wired connections that are controlled by firewalls or similar devices. There are already threat models [33], tools, and concepts covering the security requirements in **OT** [20, 22, 21, 19] but integrating the specific properties of and requirements for wireless industrial communication is often difficult.

Wireless industrial networks already in use today are mostly used as local wireless substitutes or extensions of Fieldbus systems. Examples are WirelessHART, ZigBee, ISA100, BLE, and many more. Also, WiFi is used in the **OT** domain if higher coverage and bandwidth are needed. Technologies like LoRaWAN rolled out in industrial environments have low rates but high coverage and can be used for very basic communication tasks. Security for LoRaWAN in the context of IEC 62443 and industry applications is discussed in [48, 23, 62]. Generally, wireless industrial networks are far less popular compared to their wired counterparts due to limited reliability, and their usage is often restricted to niche applications.

5G is expected to overcome the limitations of existing industrial wireless solutions

by providing higher QoS, broader coverage, and structured deployment. However, from a security architecture standpoint, 5G introduces new challenges. Unlike existing wireless networks that are integrated into predominantly wired OT communication architectures, 5G provides a parallel communication infrastructure that does not naturally integrate with industrial communication architectures. Therefore, when integrating 5G into a security architecture like IEC 62443, specific considerations for the deployment scheme must be addressed first.

4.3.1 Isolated deployment

In SANPN, the 5GS including RAN and core network elements are implemented on-premise as introduced in fig. 2 a. This deployment option allows security zones to be seen as network slices [4]. However, when integrating existing industrial networks, this concept must be adapted to the integrated parts or vice versa. This is still an open topic, especially since the integration of the 5G security concept into an existing IT-OT environment is not solved yet. Building blocks such as UE authorization could be useful, also for TSN integration, building blocks are provided and controlled by the 5GS (see fig. 4) that belong to different SL zones.

4.3.2 Public network integrated NPN

The PNI-NPN deployment options combine parts of the public cellular network with locally installed elements of a private network. If only RAN and gNB are used in shared mode, the network slicing concept solves the multiple uses as all control and interfacing are done by in-house deployments (fig. 2 c), so it can be treated similar to an isolated one.

When the deployment is considered as in fig. 2 d and fig. 2 e, it allows benefits including inter-factory communication through the use of a PNI-NPN and secured network slicing supported by 5GS of the PLMN operator. However, if the 5G network is part of a critical industrial system, the operator of the industrial infrastructure must set up trust measures together with operators of the 5G network [4]. Within the IEC 62443 standard, it is possible to develop these measures and implement them in the factory. Traditional OT deployment assumes that all structures in a network or zone are part of a single trust zone. When the PLMN operator provides parts of the OT network infrastructure or services as 5G PNI-NPN deployment, the PLMN operator has to be a reliable entity, which the OT operator can trust for certification requirements. Therefore visibility and tracking capabilities are key requirements to establish trust and ensure compliance safety rules on both OT operator and PLMN operator sides.

4.3.3 Network slicing

Network slicing has the potential to enhance security within the context of the IEC 62443 standard in various ways. By configuring network slices, it becomes possible to create isolated slices for specific security zones as defined by IEC 62443. This opens up the opportunity to prevent unauthorized access or the spread of attacks across different security zones. Additionally, network slicing offers flexibility in deploying security network functions that are tailored to the requirements of individual secure zones and can adapt to evolving security threats. This flexibility allows for a higher level of responsiveness and effectiveness in implementing security measures. Moreover, network slicing provides the means to isolate and contain potentially malicious devices or network components that exhibit suspicious behavior. Hence, mitigating risks and ensuring a more secure environment.

For all variants of 5G deployments in a factory, it is required to fulfill QoS, security requirements, and their integration in existing infrastructure. This opens up new research topics which cannot be answered in this work. To improve and further evolve I4.0, the new possibilities with 5G are an opportunity to innovate.

4.4 Comparison and trade-off

Table 1: Evaluation of 5G network deployment options [47, 2, 58, 31].

Attribute	Isolated deployment	Shared access network	Shared access network and control plane	Hosted by public network operator
Setup cost	High	Moderate	Low	Low
Infrastructure needed	Core (control/user plane), gNBs, UEs, MEC (optional)	Core (control/user plane), gNBs (MNO), UEs, MEC (optional)	Control plane/ gNB (MNO), user plane, UEs, MEC (optional)	Control/user plane/ gNB (MNO), UEs, MEC (optional)
Self customization	Full	High	Partial	None
Flexibility and adaptability	High	Moderate	Low	Very low
Edge Infrastructure	Dedicated and self-managed	Dedicated and self-managed	Managed by MNO, local storage (optional)	Managed by MNO
Data ownership	Isolated and exclusive	Isolated and exclusive	Exclusive	Exclusive
Reliability	Highest	High	As guaranteed by MNO	As guaranteed by MNO
Availability	Highest	High	As guaranteed by MNO	As guaranteed by MNO
Configurable for TSN integrated applications	Highly suitable	Suitable	Moderately suitable	Less suitable
Security and Privacy	Extremely high	High - dependent on security mechanisms at RAN	Medium - dependent on security mechanisms at RAN and control plane	Based on MNO defined mechanisms
Data monitoring access	Extremely high	High	Medium	Medium / low or as agreed with the MNO
Fast data offloading and computation	Extremely high	High	Medium	Medium / low
Suitable example use cases [27, 3]	Motion control, AGV [42, 56, 9], Augmented reality	Controller-to-controller communication, Closed loop control [57]	Mobile robots [61], Process monitoring	Massive wireless sensor networks, Plant asset management

A **PNI-NPN** may be a preferred option for many industrial enterprises since implementation and operation of an isolated deployment involves additional resources and efforts to manage the network [31]. In addition, an isolated deployment requires high setup costs, whereas a **PNI-NPN** hosted by a public network operator may require the least operational and capital costs. The costs for the needed infrastructure in terms of the core network control and user plane machines, **MEC** devices, **RAN** including the baseband unit and radio heads, and the **UEs** are to be considered. In case of an isolated deployment the infrastructure cost is to be borne by the enterprise itself whereby in case of a public network operator hosted setup, the infrastructure is provided by the **MNO**, and thereof the cost includes leasing/usage of the **MNO** services. Therefore, the costs for **MNOs** providing managed service in case of **PNI-NPN** or regular upgrades and licensing (software, frequency, etc.) in case of isolated deployments should be considered while selecting a deployment option. Although cost could be a decisive factor for 5G deployment in an industrial environment, an isolated deployment nevertheless allows complete control over the design and configuration of the network [2]. This not only enables exclusive data ownership, but also provides the highest level of reliability, availability, privacy, and data security guarantees. The features of different 5G network deployment scenarios are summarized in Table. 1.

Another consideration for 5G deployment may be based on applications that require low latency or time-sensitive deterministic communication. Such applications can be served best by an isolated deployment, specifically through a 5G **TSN** integrated deployment. Accordingly, an influencing factor is the location of **UPF** that enables the local functioning of time-critical applications along with the availability of multi-access computing resources which is usually desired for industrial applications [58, 47]. Moreover, the possibility to manage communication control signaling and tuning **QoS** parameters locally (through isolated deployment or shared RAN deployment) would be an added advantage in terms of availability and robustness. Communication control signaling means the exchange of information that enables **UE** access to the network, such as authentication, resource allocation, mobility, etc. **QoS** customization may be referred to as the flexibility to configure network parameters in a way that the requirements of the targeted use case can be satisfied. These requirements may vary and can be identified through parameters such as throughput, latency, jitter, and reliability. However, besides these performance parameters service availability, network scalability, privacy, and data security may also be considered for industrial scenarios. Therefore, with a greater degree of network isolation, higher performance, and network flexibility can be achieved.

From the **QoS** perspective, a network operator may also deploy a light-weight customer-

tailored core network with some core functions and UPF at industrial premises that may fulfill all QoS requirements of an application [53]. However, with respect to strict security requirements in OT trying to prevent unauthorized access to the plant infrastructure, an isolated deployment intuitively seems most suitable to meet security and privacy regulations [58, 47]. Nevertheless, the security measures enforced by the operators on RAN and the core network might also satisfy the needs of a particular use case. From a security viewpoint, the appropriate level of isolation can therefore be decided based on the application scenario and the guarantees from the network operator when considering PNI-NPN as the deployment option. The industrial automation trend towards digitization, resilience, and sustainability led to the incorporation of robotic platforms, flexible manufacturing designs, and the possibility of individualization of products. Customers may have different and diverse demands for a desired product. To meet these diverse demands, the units of the production line may need to be replaced to adapt to the design requirements of the product. In addition, to increase productivity robotic platforms can be used that not only provide mobility of objects but also assist humans in the manufacturing area. These trends have revamped the automation processes, however, require the support of reliable, dependable, and safe wireless communication systems. Some of these applications may also require a high amount of data off-loading, computation, and fast processing of results. In such scenarios, an isolated deployment can be an ideal wireless connectivity solution since the network QoS capabilities, computational resources, and infrastructural capacities can be customized and configured according to the application requirements. While 5G is not a replacement for all industrial communication technologies, it is a solution to provide mobile and wireless connectivity to support the digitization and automation of manufacturing processes. Therefore, the choice of the deployment option highly depends on the requirements of the manufacturing use case.

Considering the requirements from different industrial applications [27, 68, 3], use cases that fit best to the corresponding deployment option are presented as a guide in Table. 1. The motion control and augmented reality (AR) use cases are more suitable for an isolated deployment since motion control requires time-aware scheduling and strict deterministic cyclic communication (< 0.5 ms) while the AR use case requires quick feedback after processing complex tasks through the edge. The shared access network deployment option is suitable for controller-to-controller communication and closed loop control where the requirements in terms of reliability, latency, and determinism are less stringent compared to the motion control use case, and usually, no interaction with the public network is needed. The identified cyclic communication requirement for the controller-to-controller use case is 4-10 ms whereas for closed loop control is 10-100 ms [27]. The shared access network

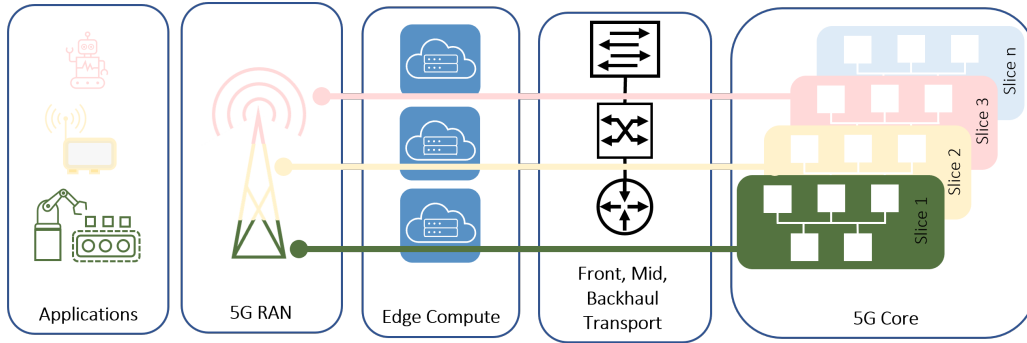


Figure 3: 5G end-to-end network slicing for diverse application requirements

and control plane deployment fits better for mobile robots (100 ms cycle time) and process monitoring (50 ms cycle time) use cases since it may require wide service area coverage and interconnection with the public network. Lastly, the public network operator-hosted option is suitable for massive wireless sensor networks and plant asset management that have relaxed requirements and may require interconnection with the public network.

In summary, even though an isolated deployment provides several advantages over other deployment options, the choice of deployment depends on the functional, performance, and operational requirements of the use case. Moreover, the deployment cost would be a decisive factor to consider.

4.5 Features and capabilities

4.5.1 Network slicing

Network slicing entails the programmable provisioning of virtualized networks. It provides high flexibility and modularity to the network functions by logically isolating the network to support diverse application requirements. Since the 5G system promises support for **enhanced mobile broadband (eMBB)**, **massive machine type communication (mMTC)**, and **uRLLC** service categories, network provisioning for applications with conflicting communication demands is required. Network slicing is an effective technique to provision the network according to the communication demands even for one service category such as **uRLLC**. Network slicing efficiently utilizes the network resources that also bring economic benefits [74]. **Software-defined networking (SDN)** and **network function virtualization (NFV)** are the key enabling technologies to realize network slicing [6]. **SDN** in 5G systems allows the physical separation between the control plane functions and the user plane function whereby **NFV** enables dynamic resource allocation and scalability of these functions to meet the service demands [46].

A network slice may span across multiple domains of the network including the

core network, transport network, distributed edge infrastructure, and the RAN [16] (fig. 3). The purpose of configuring a network slice is to provide customized functionalities needed to support the requirements of specific use cases. These requirements may also change and accordingly be managed and orchestrated. The 5G network functions specific to network slicing include NSSF, network slice specific authentication and authorization function (NSSAAF), and the recently introduced network slice access control function (NSACF) in release-17. The NSSF exposes its services to AMF or another NSSF (in case of roaming) by informing the appropriate AMF defined to serve the UE that is requesting registration to the network. The UE registration request message includes a list of network slice selection assistance informations (NSSAIs) it wants to use for connectivity. If the network supports the requested NSSAI, a PDU session is established for a particular single NSSAI (S-NSSAI). The NSSAAF performs S-NSSAI specific authentication and authorization for a given UE while the NSACF is responsible for performing admission control on the allowed number of UE to the S-NSSAI.

Network slicing is not limited to PLMN but can also be configured for SA NPN. In the context of digitization and connectivity for smart factories, network slicing enables high flexibility and better QoS support since multiple industrial applications can be serviced simultaneously. However, industrial use cases may have stringent communication demands such as highly accurate localization services for which optimized slice management and orchestration may be needed [71]. This optimization can potentially be achieved through incorporating artificial intelligence (AI)/machine learning (ML)-based approaches to network slicing for their intelligent management, configuration, and optimization [71, 69].

4.5.2 5G QoS Support

The wide variety of industrial applications defines diverse communication requirements that rely on the QoS provisioning of the underlying communication system. The 5GS defines extensive mechanisms to support and monitor QoS to fulfill the communication requirements for diverse applications. QoS in 5G can be differentiated by defining a QoS flow profile as a set of QoS parameters. A QoS flow represents the smallest granularity of QoS differentiation (fig. 4). The connection between a UE and the data network through the UPF is provisioned by establishing a PDU session. A PDU session may have one or more QoS flows. A QoS profile includes parameters such as the 5G QoS Identifier (5QI), the allocation and retention priority, the reflective QoS attribute, the guaranteed flow bit rate (GFBR), the maximum bit rate, the notification control, and the maximum packet loss rate. The 5QI is a value that identifies the set of QoS parameters [1].

The QoS flow between the UE and UPF can be characterized by 5QIs in terms of

resource type, priority level, packet delay budget, packet error rate, averaging window, and maximum data burst volume. The resource types can be **guaranteed bit rate (GBR)**, **non-GBR**, or **delay critical GBR** [1, 38]. Averaging window represents the duration over which the **GFBR** and **maximum flow bit rate (MFBR)** are calculated. **GFBR** is the guaranteed bit rate to be provided to a **QoS** flow, while **MFBR** limits the highest expected bit rate for the **QoS** flow over an averaging window.

QoS monitoring to assist **uRLLC** service can be applied for packet delay measurements. The monitoring of **uplink (UL)** and **downlink (DL)** packet delays between the **RAN** and **UPF** can be performed on the smallest granularities such as per **QoS** flow per **UE**.

4.6 5G support for industrial networks

The following sections present 5G integration with external networks to support deterministic communication needed for the operation of industrial networks.

4.6.1 Time-sensitive networking

Industrial applications not only desire reliable and low latency transmission but also deterministic communication with defined **QoS**. The IEEE 802.1 task group is working towards standardization of **TSN** to fulfill the requirements of industrial communication [34]. Although **TSN** standardization is focused on wired networks such as the local area network, 3GPP release-18 provides support for 5G integration with **TSN** along with enablers for time-sensitive communications and time synchronization [1, 30].

5G-**TSN** integration is supported for the fully centralized **TSN** configuration model (IEEE 802.1Qcc). The **5GS** integrates with the **TSN** domain as a **TSN** logical bridge without exposing its core and access network procedures (see fig. 4).

This integration is achieved through **TSN translator (TT)** functionalities that facilitate communication between the **TSN** domain and 5G system [10, 38, 35, 1]. These functionalities include the **network side TSN translator (NW-TT)** and the **device side TSN translator (DS-TT)**. On the control plane, the **TSN-application function (AF)** interacts with the **centralized network configuration (CNC)** for control and management procedures and to influence traffic routing in the user plane. On the user plane, **NW-TT**, located at the **UPF**, interacts with the **TSN** domain while the **DS-TT**, located at the **UE**, interacts with the end stations to enable wireless **TSN** for industrial devices.

To support time synchronization (IEEE 802.1AS), the 3GPP release-18 specifies the distribution of timing information via the 5G internal system clock (boundary clock solution) or the use of **TSN grandmaster (GM)** clock and time-stamping mechanism

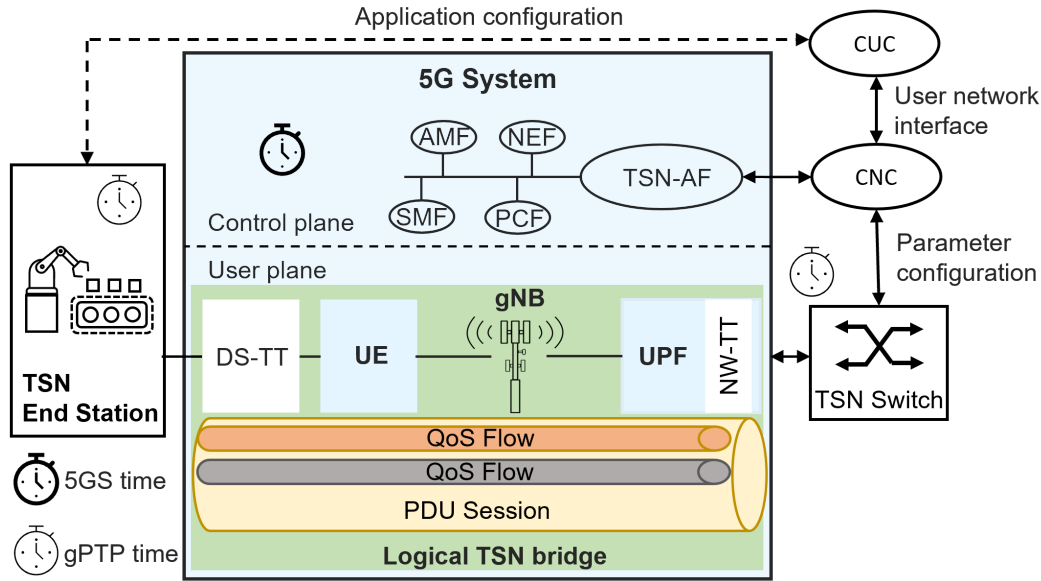


Figure 4: 5G system architecture as a logical TSN bridge [1].

through **generic precision time protocol (gPTP)** messages (transparent clock solution). The residence time (the duration that the **gPTP** packet spends within the **5GS**) is calculated and added to the correction field of the **TSN** synchronization packets. Additionally, to support timing resiliency to 5G applications sensitive to degradation in timing synchronization (examples include power grid and financial sector), release-18 (TS 22.261) provides mechanisms for 5G time resiliency. In this timing architecture, the 5G system acts as redundant or an alternative clock source to time-sensitive applications. 5G supports **TSN** traffic shaping and scheduling with a hold and forward mechanism and **TSC assistance information (TSCAI)**. **TSCAI** parameters obtained from the **TSN AF** via the **CNC** enable 5G **RAN** to schedule time-sensitive traffic. **Time-sensitive communication (TSC)** defines QoS flows using delay-critical **GBR** and **5QIs** [35]. The 5G multipath transmission supports ultra-reliability and enables **TSN frame replication and elimination for reliability (FRER)** at the cost of increased resource consumption [64]. Different approaches for redundant transmission paths include redundant **PDU** sessions over user planes, redundant user plane paths for dual RAN connectivity, redundant **UEs**, redundant transmission path between **RAN** and **UPF**, and intermediate **UPFs**. The **5GS** support for **per-stream filtering and policing (PSFP)** depends on implementation support from **TT** functions on both device and network sides. The **TSN AF** interfaces with the **CNC** to obtain **PSFP** information, extract relevant configuration parameters, and determine traffic pattern details. This information is forwarded to the **SMF** via **PCF** for configuring 5G QoS flows. 5G supports resource reservation as the **TSN AF** stores the binding between the **DS-TT** and **PDU** session. Port capabilities and delay information are shared with the **CNC** for traffic scheduling. The residence

time is the same for **UL** and **DL** but may vary among **UEs**. The **TSN AF** facilitates connectivity and coordination between 5G and TSN-enabled devices.

Some recent works on the implementation and analysis of different aspects of a 5G-TSN integrated network are available. In particular, an analytical and experimental analysis of IEEE 802.1AS time synchronization over wireless media, in particular over **5GS** is also presented [66]. The authors analyze the factors that negatively impact the performance of time synchronization over wireless along with setup challenges. The performance of IEEE 802.1AS in a 5G testbed is evaluated for an industrial closed-loop control application to enable **TSN** over **5GS** [45]. The accuracy of time synchronization in a 5G-TSN integrated network and different over-the-air timing errors related to reference time indication are investigated in [63]. Apart from this, a proof-of-concept translation technique for TSN and 5GS traffic is demonstrated in the NeSTiNg simulator [60].

4.6.2 Deterministic Networking

The IETF **DetNet** is a network layer (layer 3) technology that provides deterministic communication support to **DetNet** flows. **DetNet** provides a low packet loss rate and an assured maximum end-to-end packet delivery latency. **DetNet** features are similar to IEEE 802.1 **TSN** which supports deterministic communication at layer 2. While **5G-TSN** integration was specified in 3GPP release-16 and release-17 where the **TSC** framework is defined, release-18 studied 5G support for **DetNet**.

5G integrates with **DetNet** as a logical **DetNet** transit router as presented in Fig. 5. Similar to 5G-TSN integration, the internal procedures of the **5G** core and **RAN** remain hidden from the **DetNet**. However, the **5G-DetNet** integration architecture does not require support for **DS-TT** or **NW-TT** functionality although they can co-exist with such functions. Nevertheless, to report information on the network side ports, the **NW-TT** control plane function is used.

The **time-sensitive communication time-sensitive function (TSCTSF)** provides the mapping between the **DetNet** controller and the **5G** core functions. **TSCTSF** is a 5G control plane function that controls the **DS-TT** and **NW-TT** for gPTP based time synchronization service to support **5G-TSN** integration. However, **TSCTSF** also provides support for **DetNet** 5G system mapping through **TSC** assistance container-related functionalities. The **TSCTSF** constructs the **TSC** assistance container based on information provided by the **DetNet** controller and sends it to the **PCF**. The **PCF** upon receiving **5GS** logical router information for the **PDU** session received from **SMF** provides information related to user-plane node ID, port number, IP address allocated to the **PDU** session, and MTU size to **TSCTSF**. The **TSCTSF** then creates an **AF** session with **PCF**. The **TSCTSF** may now subscribe to **NW-TT** for receiving user plane node management information changes for the **5GS** logical router. The

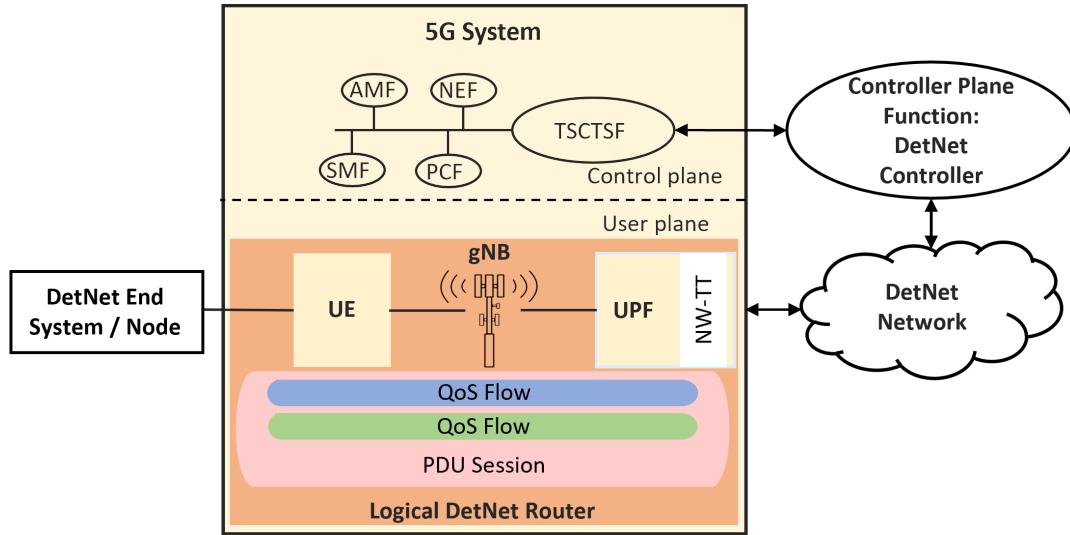


Figure 5: 5G system architecture as a logical [DetNet](#) router [1].

[TSCTSF](#) may also receive [DetNet](#) YANG configuration from a [DetNet](#) controller describing traffic characteristics and requirements. The [TSCTSF](#) can derive the requested [5GS](#) delay if the [DetNet](#) YANG configuration does not include [5GS](#)-specific [5GS](#)-node-max-latency or the end-to-end Max-latency. Similarly, the requested packet error rate can be derived by the [TSCTSF](#) if the [5GS](#)-node-max-loss or the end-to-end Max-loss is not specified in the [DetNet](#) YANG configuration.

The granularity of the [5GS](#) [DetNet](#) node is per [UPF](#) for each network instance. The [TSCTSF](#) stores the binding relationship between a device side port and a [PDU](#) session identified by the UE address. The [TSCTSF](#) also stores information about ports on the [UPF/NW-TT](#) side. To integrate with IETF [DetNet](#), it is assumed that the existing 3GPP routing mechanisms are re-used for [DetNet](#), the existing multicast capabilities can be applied, the integration is based on [DetNet](#) for IP whereas [DetNet](#) for MPLS is not supported, and IP-based [DetNet](#) traffic is carried in IP type [PDU](#) Sessions.

The integration of [DetNet](#) with 5G can enable new use cases and applications that require both high-speed wireless connectivity and deterministic network behavior, fostering innovation in areas such as industrial automation, autonomous vehicles, and real-time multimedia delivery.

4.6.3 5G - OPC UA

OPC UA (IEC 62541-1) is a popular standard in industrial automation, serving SCADA, manufacturing execution systems, and enterprise resource planning [36]. It replaces the open platform communications classic and includes a meta-model, transport protocol specification, and a server. [OPC UA](#) has domain-specific information models and supports client-server and PubSub communication models. Pub-

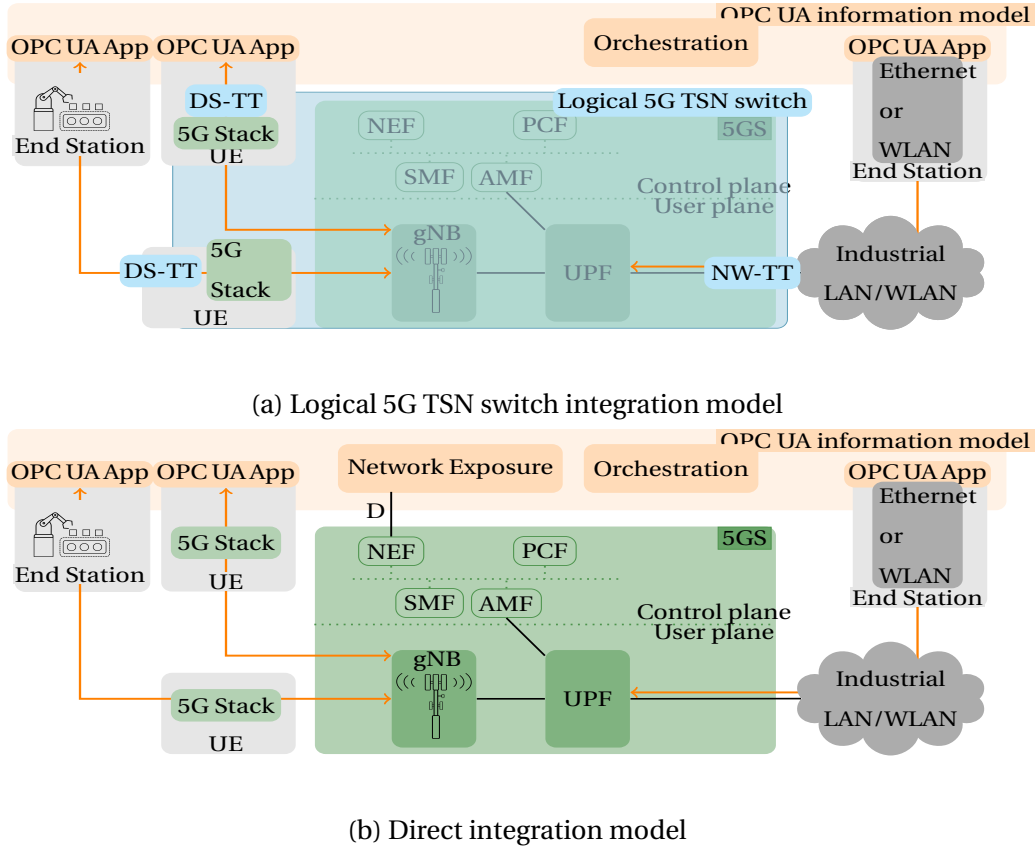


Figure 6: 5G-OPC UA integration models

Sub enables real-time capabilities, unlike the client-server model. OPC UA ensures vendor-neutral interoperability, offers mature information modeling, open standardization, and security features. It accommodates new technologies while maintaining backward compatibility (IEC 62541-1). Combining OPC UA and 5G provides a complete communication solution for industrial automation, considering that OPC UA operates on higher OSI model layers, while 5G operates on lower layers.

The integration of 5G with OPC UA offers several benefits for industrial systems. It leverages edge computing, mobility, and security features of 5G to enable faster communication, improved scalability, mobility, flexibility, and enhanced security to industrial systems, fostering advanced applications and internet-of-things (IoT) adoption. It enhances existing infrastructure without completely replacing current systems. Legacy systems can coexist with new 5G-enabled devices, allowing a gradual transition and future-proofing industrial communication networks.

For the 5G-OPC UA integration, two different options can be considered (Fig. 6): first, an integration of OPC UA with 5GS as a logical TSN bridge and second, a direct integration of OPC UA into 5G. The OPC UA application can reside on a UE, an end station connected to a UE, or a non-UE device connected via an external network

(Ethernet or WLAN).

The 3GPP release-16 describes mechanisms for the integration of TSN and its centralized configuration model with 5GS (details in section 4.6.1). Additionally, the integration of OPC UA publisher/subscriber (PubSub) with TSN has been discussed in the literature [13, 51].

The 5GS is integrated as a logical TSN bridge, and OPC UA could interact directly with TSN, as shown in fig. 6a. The connection with OPC UA application is made either via the DS-TT or the NW-TT. The 5GS could furthermore interact directly with the TSN CNC. The OPC UA applications could directly report their QoS requirements to the centralized user configuration (CUC) in the TSN network to set up Ethernet PDU sessions. In this way, the OPC UA applications would not have to deal with any 5G aspects of the network. While mechanisms for 5G-TSN integration are defined in 3GPP release-16 and also in the upcoming release-17, both OPC UA and TSN are being actively standardized and cannot be considered as fully developed standards. Hence, several open questions remain for the 5G-OPC UA integration. Currently, the IEEE/IEC 60802 industrial automation TSN profile and OPC UA extensions for field eXchange (OPC UA FX) working group are working towards filling gaps for the OPC UA TSN integration.

4.6.4 Edge computing

MEC is also an enabler to support uRLLC. Here, edge computing should not be confused with edge devices in the IoT that can perform computing and storage operations as a local service. In the context of 5G, MEC (also known as distributed edge computing) provides computing and storage resources close to the end-user allowing low-latency communication through local processing, real-time interaction, and high data exchange rates [32]. As an example, a high number of sensors and devices participating in an industrial process may generate a large amount of data. These sensors and devices may not have enough processing capabilities and require data offloading at an edge for computation and coordination. The edge computing devices not only deliver results quickly but also help in achieving low-latency local communication and avoid overloading public networks [65]. MEC can also be used for location awareness of mobile users by utilizing their signaling information. Similarly, it can be used for network optimization by utilizing knowledge of network conditions and contextual information [26]. The upcoming cyber-physical systems (CPS) applications including augmented reality and collaborative CPS among others will include edge computing in different forms (customized to the specific needs and limitations of the relevant domains), ranging from the device edge to the network edge [59].

The industrial CPSs will greatly benefit from the integration of MEC by offloading

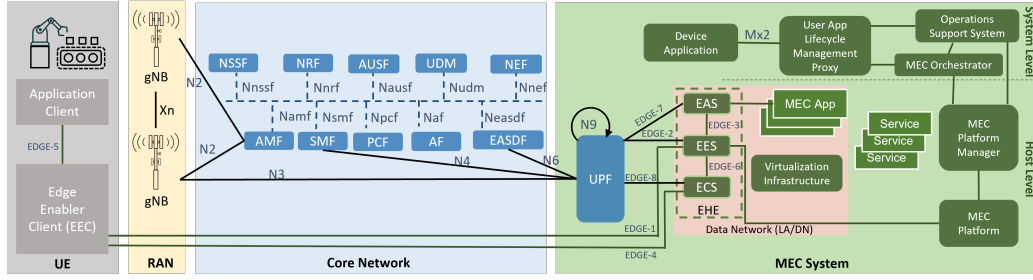


Figure 7: 5G MEC network deployment architecture. The figure is derived from the reference architectures specified in TS 23.558 and TS 23.548.

data from CPS devices to the edge for processing instead of sending it to remote clouds. It offers benefits including reduced latency for real-time responsiveness, optimized bandwidth usage by transmitting only relevant data, improved scalability through distributed computing, enhanced privacy and security by keeping sensitive data local, energy efficiency by minimizing data transmission, and offline operation when connectivity is limited. Overall, MEC enables efficient data processing, real-time decision-making, and enhanced system performance and reliability in CPS.

The European telecommunications standards institute (ETSI) industry specification group (ISG) has published a set of MEC specifications that focus on management and orchestration, application enablement, application programming interfaces (APIs), and UE API in ETSI GS MEC 003 [52]. Accordingly, MEC can be placed in or close to the network edge which runs applications using a virtualized infrastructure while the APIs facilitate in running these applications and ensure service continuity.

The 3GPP 5G system architecture also specifies support for MEC integration through the exposure of 5G core network information and capabilities to external consumers [1, 52] in TS 23.558 and TS 23.548, with security aspects presented in TS 33.558. The MEC can interact with the 5GS as an AF to gain support for one or a combination of 5G enablers. These enablers may include connectivity support to a local area data network, user plane (re)selection to influence the application traffic routing decisions, session and service continuity to provision application and device mobility, and interaction for QoS control and charging rules [1].

The 5G SBA for network functions and services align with ETSI API framework for MEC enabling them to interact for their services reciprocally [25]. This is further illustrated in fig. 7 which presents the MEC architecture integrated with the 5GS as per the 3GPP specifications. The 5GS enables the use of edge hosting environment (EHE) in the data network (DN) beyond the UPF, which can be controlled by either the operator or third-party entities. The EHE holds the edge servers i.e., the edge enabler server (EES), the edge application server (EAS), and the edge con-

figuration server (ECS). The EES provides functionalities like interaction with the 5G core network for accessing the capabilities of network functions to support the EASs and edge enabler client (EEC). The EAS is the application server to which the MEC application connects to avail services and benefit from edge computing. The ECS provides supporting functions to the EEC for connecting to the EES. The edge servers connect with the 5G core network either directly via the PCF or indirectly via the network exposure function (NEF). On the 5G core network side, the edge application server discovery function (EASDF) registers with the network repository function (NRF) for EASDF discovery and selection. The EASDF has direct user plane connectivity with the UPF using the N6 interface. On the UE side, the EEC supports the application client by providing functionalities like detecting UE mobility, retrieving configuration information for the exchange of data, and discovery of EASs. The reference points Edge-1 to Edge-8 are used for the interaction between different entities in the MEC architecture.

Once an end device (UE) is registered with the 5GS and a PDU session is established, available MEC applications from the user application lifecycle management proxy using the Mx2 interface can be discovered. The procedures resulting from the requests generated by the UE API get routed via the operations support system towards the MEC system-level management. A UE can then send an application instantiation to the MEC host if the desired application package is enabled at the MEC orchestrator.

The deployment of MEC is a challenging task requiring the analysis of different operational, performance, and/or security aspects impacting the QoS of the IoT system. MEC deployment options for 5GS are presented in the ETSI white papers [25], [26], and [24]. A proof-of-concept demonstration of ETSI-complaint MEC deployment is presented in [12]. For the optimal performance of MEC, it is not only important to identify the edge gateway and the host devices but also to identify where each service needs to be deployed. Similarly, the deployment and management of networked resources are equally important to investigate. Correct deployment of MEC services and networked resources ensures flexibility, reduced processing burden on MEC servers, and optimized computation offloading. Different MEC service deployment frameworks are presented in [18, 44, 37]. The management and deployment of networked resources is a complex task given the distributed nature of the resources. Reinforcement learning and Lyapunov optimization techniques [49, 50, 55] are used for resource management in MEC to meet the QoS requirements. Further evaluations can help analyze and optimize the management of network resources. Different strategies and tools used in the literature for MEC practical implementations and its initiatives are discussed in [17] with regard to the ETSI MEC standard.

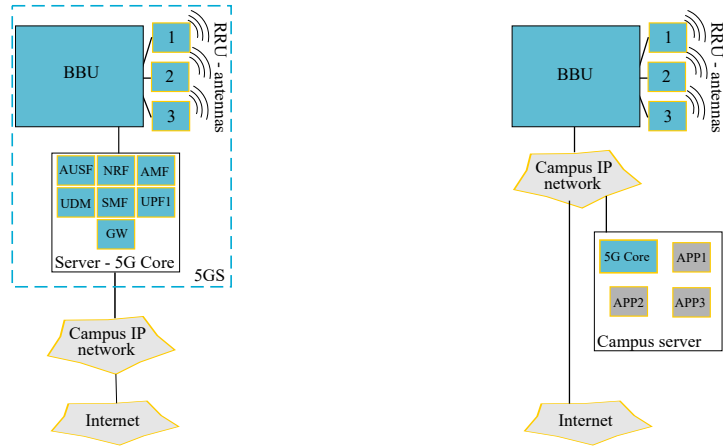
Machine learning algorithms can be deployed on the edge instead of the cloud to support applications like Tactile Internet, monitoring and maintenance, and anomaly detection [41, 72]. Such a capability is referred to as edge intelligence. The computationally heavy tasks like prediction, estimation, classification, and alike can be offloaded from the IoT devices to the edge server. The edge server being closer to the edge devices enables low end-to-end delay, reduced energy consumption, and high learning/inference accuracy [40, 73]. The concept of multi-service edge intelligence is also introduced recently to enable real-time control over wireless medium (i.e., 5GS) [8]. It requires a strong coupling of the wireless edge with edge computing and ML techniques aimed at ensuring reliability even in the presence of wireless inconsistencies. Similarly, **pervasive edge computing (PEC)** for 5GS and beyond systems has been discussed with a focus to achieve low latency for delay-intolerant applications [43]. PEC presents a highly relevant and crucial deployment approach for industrial communication networks, particularly given the emerging trend of incorporating local operations and flexible management in private industrial 5G networks.

5 5G network configuration

Campus networks with various deployment options including benefits and disadvantages of each are described in detail in Section 4. Some of the deployment options are (i) isolated deployment, (ii) cloud native SA NPN, (iii) shared access network, (iv) shared access network and control plane, (v) hosted by the public network operator, or (vi) cloud-native PNI-NPN hosted by the public network operator.

In this section, we focus on campus networks, more specifically, on indoor industrial scenarios, where security, flexibility, dependability, and performance are of utmost importance. Therefore, the isolated deployment option is the most suitable one for the campus networks in industrial scenarios where the communication has a time- and security-critical role. An additional benefit of the isolated deployment is that it provides the lowest dependency on external support, e.g., in terms of the time of a reaction in cases of failures or any backup requirements such as power supply for each device in the network, which can be fully controlled by the owner of the campus network. Similarly, regarding the RAN part, the most suitable option is a dedicated RAN, due to the possibility of optimization and radio planning for the best coverage and performance, required for a specific industrial setup. Shared RAN usually does not provide an optimal solution for a specific customer in terms of radio planning.

Depending on the network configuration requirements of an industrial setup on-



(a) dedicated hardware for 5GS

(b) shared hardware for 5GS

Figure 8: 5G network configuration with a) dedicated and b) shared hardware

premises, there can be variations in physical and software deployment options for the 5GS. The first variation is if all 5GS components need to run on dedicated hardware, separated from other network and computing devices or the same hardware components could be used for deployment of the 5G core components e.g., in virtualized environments such as dedicated virtual machines, separated network namespaces, Kubernetes, etc. Similarly, network devices, such as switches and routers can be dedicated, or shared with other industrial devices in the network.

In Fig. 8 are shown two network configuration options, typical for isolated 5G campus network deployments. The first network configuration option is where all the hardware components of 5GS are separated from the rest of the network. This option has the greatest potential for optimal performance, it is the easiest to troubleshoot and it is the most secure solution. However, it requires the most of hardware components, which slightly increases the investment budget. In this option, the **baseband unit (BBU)**, which is part of the **RAN** part of the 5GS, is directly connected to the server where all the components of the 5G core are running. The gateway to other networks is done via a router, which separates the 5GS network from the rest of the network, and it can be connected to a switch or a router of the network on-premises.

The second option, shown in Fig. 8b, is where the network devices and computing hardware, i.e., server machines, switches, and routers, are shared with the hardware resources, already available on-premises. In such configuration, the **BBU** can be connected directly to the switch, available already on-premises, and 5G core components can be running on a hardware (server) already available on-premises, which is potentially used for other applications as well. In this case, one can save on hardware investment, however, the hardware computing performance should be analyzed to ensure the required performance for 5GS.

In any network configuration option, basic network configuration settings, such as [virtual local area network \(VLAN\)](#), [network address translation \(NAT\)](#) rules, access list rules, and routing tables can be used for proper separation and translation of the 5GS traffic and the traffic from/to other networks on-premises.

5.1 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.

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-containers solution. 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.

A similar deployment option is the deployment with Kubernetes, where the 5G core components are running in virtualized environments, where in this case the deployment is detached from specific hardware, but the components can run in a net-

work 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, if a component is stopped. 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.

In the next subsection, an example of an open-source 5G core implementation is described in more detail.

5.1.1 Fraunhofer 5G core

The Fraunhofer FOKUS Open5GCore toolkit is a vendor-independent, open-source, practical implementation of the 3GPP 5G core network addressing the needs of 5G testbeds. It is a prototype of 3GPP Release 15 and 16 core network functionality, and it is suitable for R&D activities. Open5GCore interoperates with 5G NR BSs and UEs (more available on www.open5gcore.org).

Open5GCore main features are:

- Fundamental 5G core network functionality (AMF, SMF, authentication server function (AUSF), unified data management (UDM), NRF, UPF)
- Implementation of Service Based Architecture [HTTP/2 OpenAPI, REST]
- Integration with standard 5G NR using the 5G interfaces [N1, N2, N3], 5G non-access stratum (NAS) and new generation application protocol (NG-AP)
- Implementing control-user plane split with packet forwarding control protocol (PFCP) [N4]
- Advanced QoS and session management with traffic influence
- Network slice support
- Comprehensive non-3GPP access convergence
- Location Service Support
- Benchmarking Tools

Open5GCore runs on common hardware platforms and can be deployed on top of a large number of virtualization environments. The required hardware for a testbed setup highly depends on the expected capacity. Open5GCore scales from a Raspberry PI implementation to a complete rack of servers for deployment with a very high capacity.

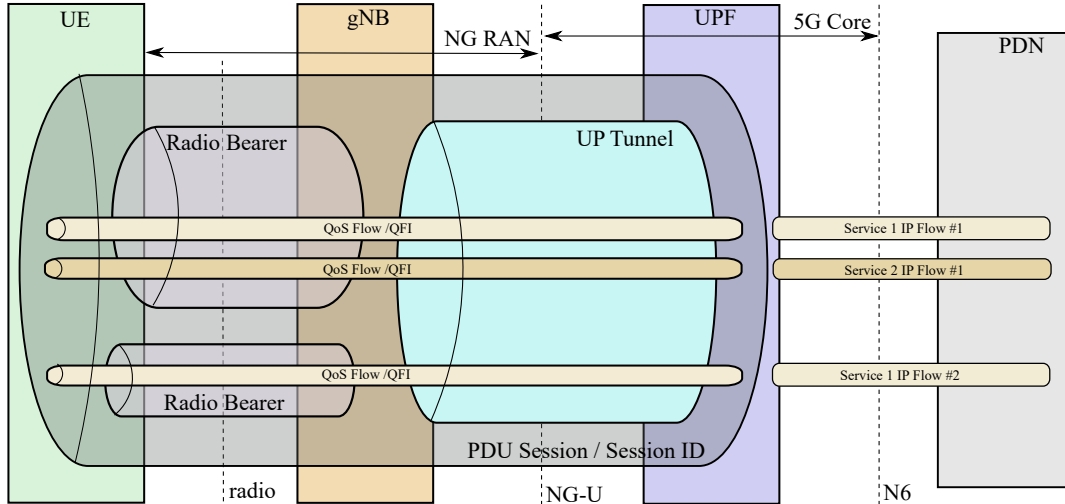


Figure 9: 5G QoS Flow diagram.

5.1.2 QoS parameters

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 the PDU Session. A QoS Flow ID (QFI) is the parameter used to identify a QoS Flow in the 5G System. 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, admission threshold) for the received user plane traffic. PDU Set QoS Parameters are determined by the PCF and provided by SMF to the new generation radio access network (NG-RAN) as part of the QoS profile. The flow diagram of the 5G QoS model is shown in Fig. 9. For each QoS Flow, the QoS profile shall include the QoS parameters:

- 5QI,
- allocation and retention priority (ARP),
- PDU set QoS parameters,
- reflective QoS attribute (RQA) (for non-GBR flow only),
- GFBR for UL and DL (for GBR flow only),
- MFBR for UL and DL (for GBR flow only),
- notification control (for GBR flow only),
- maximum packet loss rate for UL and DL (for GBR flow only).

Each QoS profile has a corresponding QFI which is not part of the QoS profile itself. The following options are supported to control QoS Flows:

1. The 5QI value may be used as the QFI value of the QoS Flow for Non-GBR QoS Flows when standardized 5QIs or pre-configured 5QIs are used, and when the 5QI is within the range of the QFI (i.e. a value less than 64).
 - (a) A default ARP shall be pre-configured in the RAN, or,
 - (b) the ARP and the QFI shall be sent to RAN at PDU Session Establishment or at PDU Session Modification and when NG-RAN is used every time the user plane of the PDU Session is activated,
2. For all other cases, a dynamically assigned QFI shall be used, where the 5QI value may be standardized, pre-configured, or dynamically assigned value. The QoS profile and the QFI of a QoS Flow shall be provided to the RAN at PDU Session Establishment/Modification and when NG-RAN is used every time the user plane of the PDU Session is activated.

A QoS rule contains the QFI of the associated QoS Flow, a Packet Filter Set, and a precedence value. A QoS rule, explicitly signaled, contains a QoS rule identifier which is unique within the PDU Session and is generated by SMF. There can be more than one QoS rule associated with the same QoS Flow (i.e., with the same QFI).

5.2 Radio access network

The RAN is part of 5GS which in general consists of a network of geographically distributed gNBs. Each gNB consists of (i) a 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 parts, called also access points (APs). The RAN part of 5GS makes on one hand wireless connectivity to 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),
- **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 many other parameters, if needed.

5.3 User equipment options and features

In 3GPP a User Equipment (UE) is a device connected to the Base Station over the air interface. We can distinguish between devices with User Interface like Smartphones or Tablets, Mobile Routers and Modems.

5.3.1 Devices with User Interface

The most common UE is a smartphone. A smartphone normally consists of a Multi-Mode/Mult-Band Modem supporting GSM, UMTS, LTE and 5G, a processor with User Interface and a SIM card. Typical smartphones have integrated antennas and Operating Systems like iOS and Android. Tablets are very similar to Smartphones, but in most cases do not support native voice services.

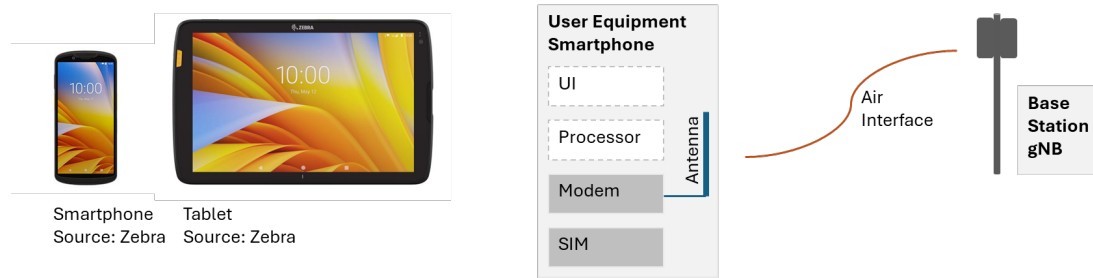


Figure 10: Smartphone or Tablet connected to Base Station

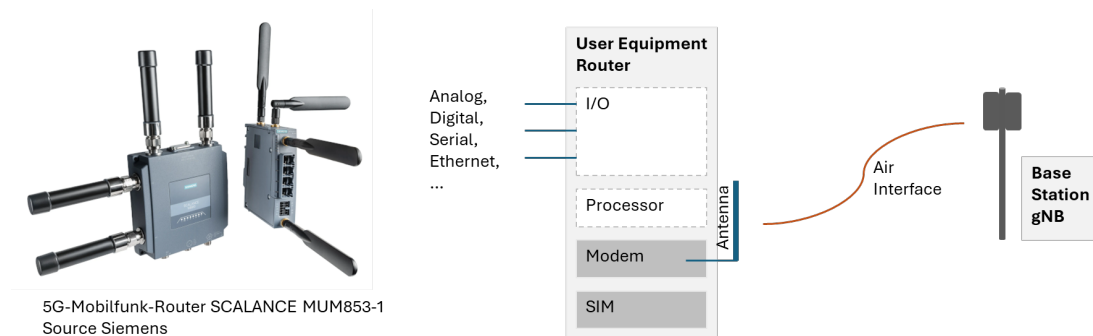


Figure 11: Mobile Router connected to Base Station

5.3.2 Mobile Routers

Mobile Routers are used for Industrial Machine-2-Machine type of Applications. They are equipped with different I/O ports and the processor typically supports protocol conversions and the ability to run (custom) applications. Such applications can be for instance small data applications to poll and convert measurement data on the edge of the network and forward to a central server or a firewall application. In many cases the devices are used stationary, but also mobile applications are possible. Antennas are typically external to improve radio performance and increase flexibility.

5.3.3 Radio Modem Module

M.2 is a typical form factor for the packaging of a modem board. Interface is for instance PCIe or USB for data and a connector to interface with a SIM. The modems are controlled over AT commands and come with all electronic components for a mobile connection including the RF front end and support various bands from 700 up to 3,800 MHz and different signal waveforms (UMTS, LTE, 5G). In 5G they typically support Stand Alone as well as Non Stand Alone operation. These M.2 modules are often basis for the modem part in Mobile Routers.



Source: Quectel

5G RM530N-GL

Summary	Specifications	PCB
• Sub-6GHz & mmWave 5G module • Max. data rates of 4.0Gbps (DL) / 1.4Gbps (UL) • M.2 form factor • 8.7g • 30mm x 52mm x 2.3mm • Extended temperature range of -40°C to +85°C		

Figure 12: m.2 modem board

6 Radio placement

6.1 Summary of requirements

As described in D2.1, a reference manufacturing plant was defined (see fig. 13). A traffic profile was derived from the different required services. Based on that input, a Network Planning coverage map was established.

Summary of the requirements on building characteristics:

- Indoor manufacturing area with about 40.000 m²
- 6 m ceiling height
- Some columns (concrete), some concrete beams
- 2 light weight wall incl glass windows in the middle of the building

5G frequency parameters:

- Use of Band n78 / 3,5GHz
- Bandwidth: 80 MHz
- Framing: DL/UL framing structure: 8:2

6.2 Simulation results

Based on the given requirements, a network planning for the production hall was done.

6.2.1 General considerations on antenna placement, cells and sectors

Since the production hall is a relatively open and unobstructed scenario, using multi-sector antennas will bring strong interference. For such scenarios it is also

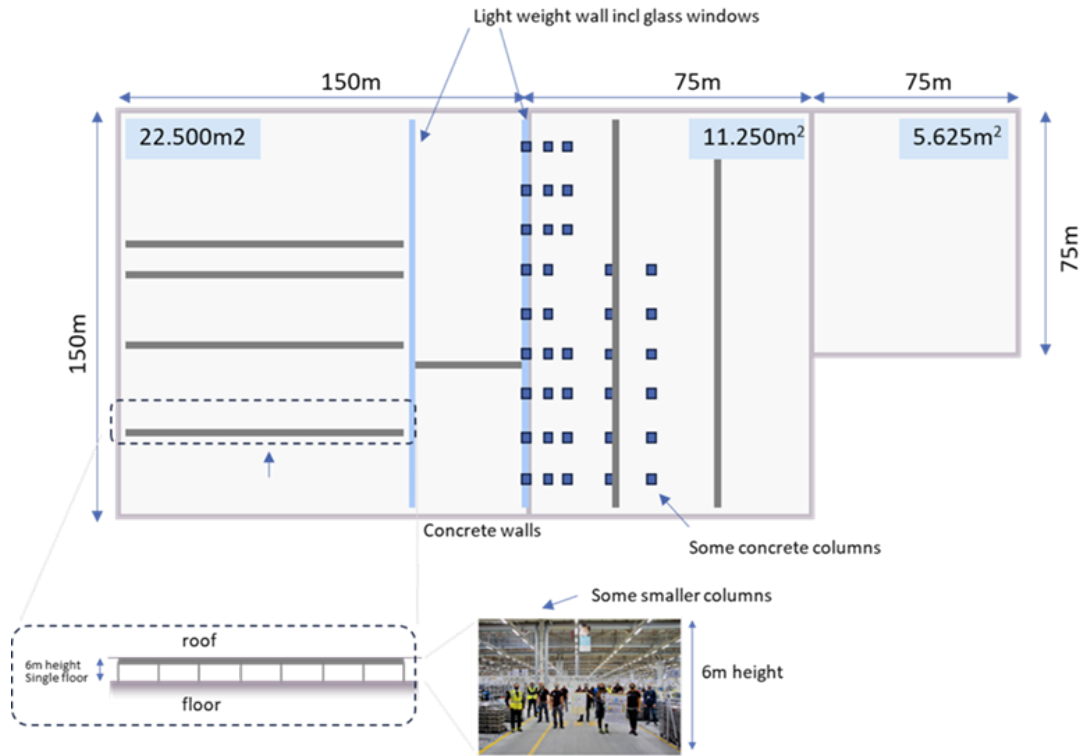


Figure 13: Reference factory layout

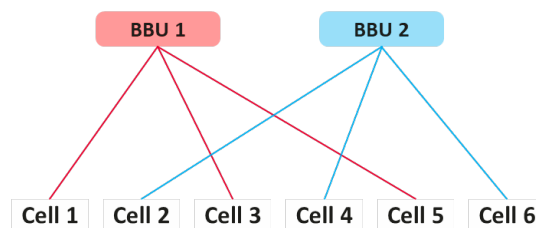


Figure 14: Redundant cell configuration

important to plan for coverage redundancy in the network. In order to control interference, inter-Frequency networking is planned.

In total 6 cells are planned for open scenario interference control and better UL throughput. In order to reach a better UL performance, Multi-pRRU with Distributed Massive MIMO are planned. The distance between pRRU is around 24m. In order to deploy a coverage redundancy network, 2 BBUs and a Cell to BBU cross connection is planned. A sketch of the network planing is given in fig. 14 and fig. 15. BBU 1 assigns the lower half of the spectrum, BBU 2 the upper half. pRRUs are distributed throughout the building and are mounted on the ceiling. Figure 16 shows an example how the antennas are mounted on the ceiling of the building. A Hub is used as connection between BBU and pRRU and distributes the signals over fiber optical cables. The radio network planning results in 58 pRRUs.

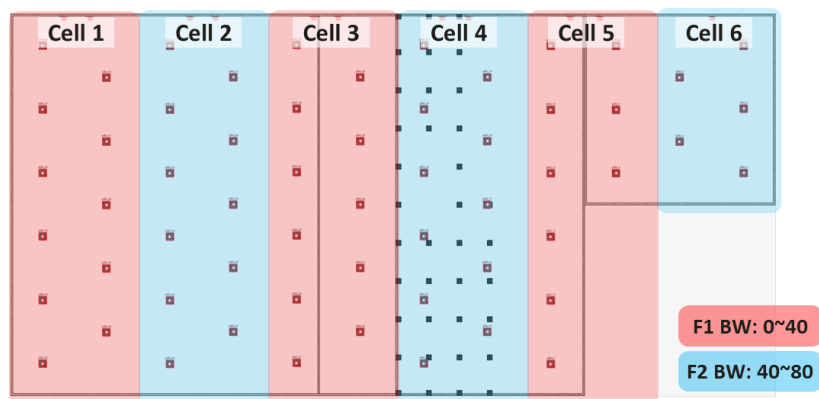


Figure 15: Distribution of Cell 1 to Cell 6

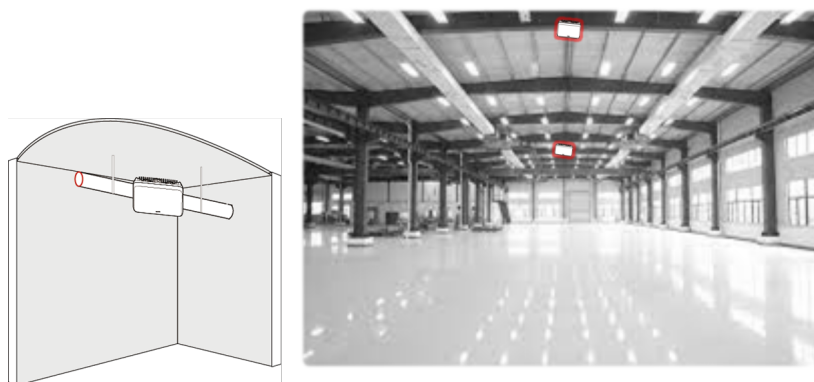


Figure 16: Example mounting of pRRU

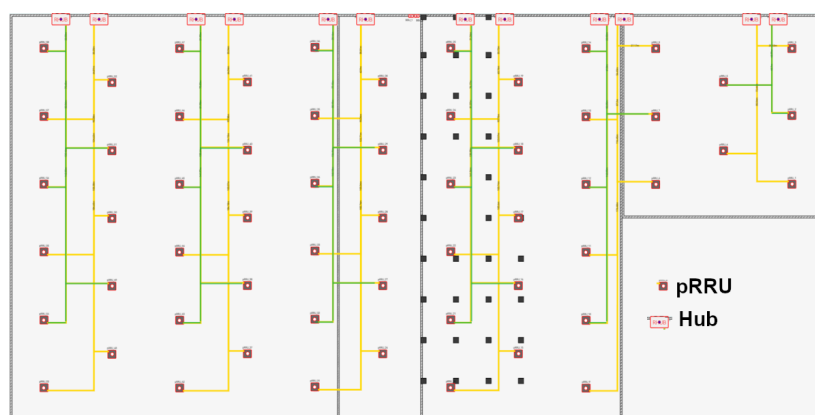


Figure 17: Placing and connecting the Hub

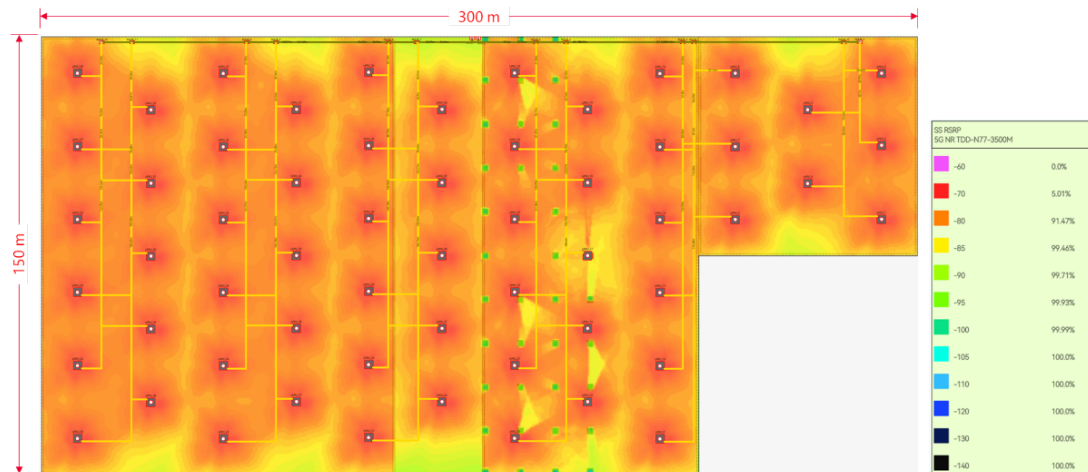


Figure 18: Simulation result: RSRP

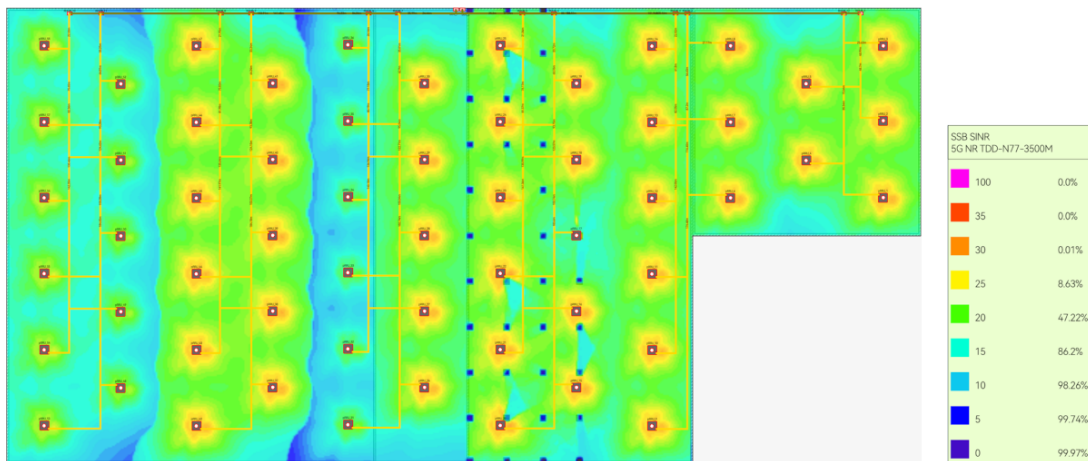


Figure 19: SINR

6.2.2 Reference Signal Received Power (RSRP)

Figure 18 shows the RSRP values for the given scenario. It can be seen that 100% of the coverage area has a RSRP of more than -105 dBm, which leads to a perfect coverage.

6.2.3 Signal to Interference plus Noise Ratio (SINR)

Figure 19 shows the SINR values. In 98.26% of the coverage area we observe an SINR better than 10dB. The left side of the production hall has no partition, therefore Cell1 and Cell3 interfere with each other.

6.2.4 Downlink Throughput

Figure 20 illustrates the achieved throughput in DL. As the bandwidth per BBU is limited to 40 MHz and to the level of interference, the theoretical maximum

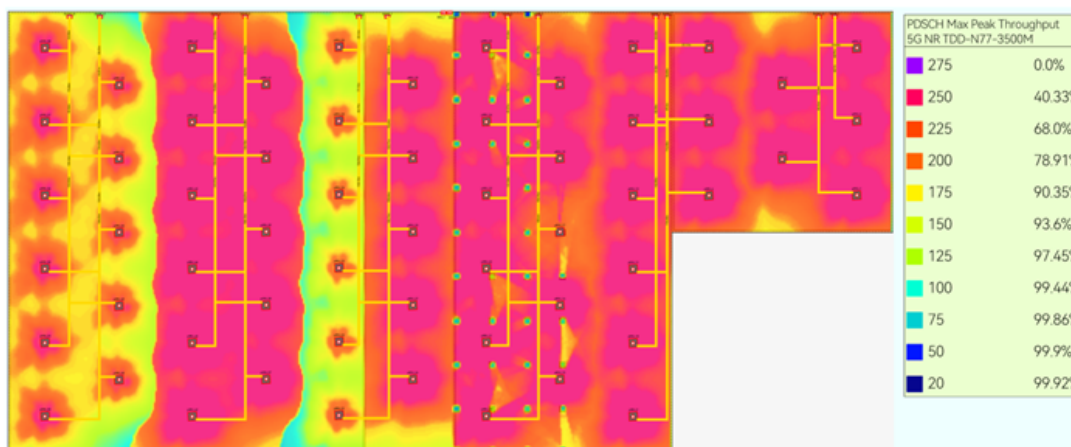


Figure 20: Downlink Throughput

throughput is around 250 Mbps per Cell, with a theoretical total throughput of production hall of 1.5 Gbps. Based on experience in open area multi-cells with interference scenario, the UL throughput will be around 100 Mbps per Cell, with a total throughput of 0.6 Gbps for the whole production hall.

6.3 Discussion on the simulation results

Based on spectrum and available technology, the simulation concluded with a total DL throughput of 1.5 Gbps for the whole system. In contrast to that, the summary of all requirements as given in Chapter 7 of Document 2.1 led to a capacity requirement of 14.757 Gbps, which is almost 10 times higher than the available throughput. Different approaches can be combined to overcome this limitation.

6.3.1 Interference

The simulation shows that interference is one of the limiting factors. To reduce interference between neighboring cells, the available spectrum is divided into two halves (40 MHz per cell). This on one hand reduces interference, but on the other hand reduces capacity. Alternative techniques to reduce interference could be the use of directional antennas.

6.3.2 Available spectrum

Simulations were done with a total available spectrum of 80 MHz. Increasing the RF bandwidth will increase the throughput of the system. The base stations used support a maximum of 200 MHz in Band n78 (3.5 GHz). Theoretical, if the whole 200 MHz could be used, the throughput would be around 3.75 Gbps. With Millimeter Wave using 5G channels in the range of 26 GHz, much more spectrum will be

available. In Austria it is planned to use a range of 600 MHz for campus networks. This would allow much higher throughput than required.

6.3.3 Base Station architecture

Simulations were done based on commercially available Base Station hardware. A more sophisticated base station architecture could also improve throughput. Improvements could be in terms of available MIMO Layer, sensitivity, output power or beam steering and massive MIMO.

6.3.4 Improved coding techniques

Video Codecs with lower bit-rates could be used to reduce the over-all load of the system.

7 Spectrum for campus networks

When deploying 5G networks for campus environments, organizations have different options for spectrum utilization, each offering unique advantages and considerations. These spectrum options include licensed spectrum and/or unlicensed spectrum. Each spectrum option presents distinct characteristics in terms of coverage, capacity, interference management, regulatory requirements, and cost implications, requiring careful evaluation to determine the most suitable approach for meeting the specific connectivity needs and use cases within the campus environment. By selecting the appropriate spectrum and deploying tailored infrastructure solutions, organizations can realize the full potential of 5G technology. These options include the licensed spectrum, unlicensed spectrum, shared licensed spectrum [58, 7], and [millimeter wave \(mm-wave\)](#) spectrum. On the other hand, 3GPP release-16 enables [NR](#) operation in unlicensed spectrum under the 5 GHz and 6 GHz bands. [uRLLC](#) configured grant enhancements in unlicensed spectrum are supported in release-17, while additional supporting features are also expected in release-18 [39, 29]. A shared licensed spectrum is the means of coordinated and dynamic access of the licensed spectrum subject to meeting a set of regulations. Examples of the shared licensed spectrum include the 3.7–3.8 GHz band in Germany and the 3.8–4.2 GHz band in the United Kingdom [7].

7.1 Unlicensed spectrum

Unlicensed spectrum offers a compelling option for deploying 5G campus networks, providing organizations with flexibility, cost-effectiveness, and rapid deployment capabilities. Unlicensed spectrum encompasses frequency bands such as 2.4 GHz

and 5 GHz, commonly utilized by Wi-Fi and other wireless technologies. Unlike licensed spectrum, unlicensed bands are open for public use without the need for regulatory licensing, significantly reducing upfront costs associated with spectrum acquisition. This makes unlicensed spectrum particularly attractive for organizations seeking to establish private 5G networks within their campus environments without reliance on external operators. However, unlicensed spectrum poses challenges related to interference from neighboring networks and devices, which can impact network performance. To address these challenges, advanced interference mitigation techniques and spectrum management tools are employed, allowing organizations to optimize the utilization of available spectrum resources [11, 28]. Despite these considerations, unlicensed spectrum offers unparalleled deployment flexibility and scalability, enabling organizations to rapidly deploy and expand 5G campus networks to support evolving connectivity needs and emerging use cases.

7.2 Licensed spectrum

Licensed spectrum presents a robust option for deploying 5G campus networks, offering operators exclusive access to specific frequency bands allocated by regulatory authorities or a [MNO](#). These bands typically include frequencies below 6 GHz, such as the C-Band (3.5 GHz) and mid-band spectrum, which strike a balance between coverage and capacity. Leveraging licensed spectrum ensures operators can prioritize traffic and enforce [QoS](#) measures, guaranteeing consistent performance levels for critical applications within the campus environment. While acquiring licenses for exclusive spectrum use involves significant costs and regulatory compliance requirements, it provides greater control over network resources and interference management. Additionally, licensed spectrum offers extensive coverage and penetration capabilities, making it suitable for providing seamless connectivity across large campus areas and indoor environments. Overall, licensed spectrum offers reliability, regulatory compliance, and QoS guarantees, making it a preferred choice for organizations prioritizing performance and stability in their 5G campus deployments.

7.2.1 Frequency planning in Austria

In deliverable D2.1, we provide details on the 5G spectrum situation in Austria in section 8.5 of deliverable D2.1.

7.3 Shared spectrum

Shared spectrum for 5G deployment in campus networks involves utilizing frequency bands that are shared among different entities or user categories, promoting effi-

cient spectrum utilization and coexistence among various wireless systems. In the context of 5G campus networks, shared spectrum offers several advantages. Firstly, it provides increased spectrum access beyond licensed and unlicensed bands, thereby enhancing capacity and network performance. Additionally, shared spectrum models employ [dynamic spectrum sharing \(DSS\)](#) technologies to dynamically allocate spectrum resources based on demand and availability, optimizing spectrum utilization while minimizing interference. Moreover, organizations can obtain [priority access licenses \(PALs\)](#) to secure exclusive spectrum use within defined geographic areas, ensuring interference protection for critical applications within the campus environment. Shared spectrum frameworks also establish clear rules and guidelines for spectrum sharing, facilitating fair access and interference avoidance among different user categories under regulatory oversight, typically provided by government agencies. By leveraging shared spectrum for 5G deployment in campus networks, organizations can capitalize on increased spectrum access, efficient spectrum utilization, and regulatory support, thus enabling enhanced connectivity, capacity, and performance to cater to diverse use cases and applications within the campus environment.

7.4 Millimeter wave spectrum

[Mm-wave](#) spectrum presents an interesting option for 5G campus networks, offering wide bandwidths and ultra-fast data rates that cater to the demands of high-capacity applications within dense environments. Frequencies above 24 GHz, including bands like 28 GHz and 39 GHz, are utilized in [mm-wave](#) deployments, providing multi-gigabit per second data speeds and low latency connectivity [54, 14]. This makes [mm-wave](#) spectrum ideal for delivering immersive experiences such as [AR](#), [virtual reality \(VR\)](#), and ultra-high-definition video streaming, enhancing productivity and innovation within campus environments. Despite its shorter propagation distances and susceptibility to blockage by obstacles like buildings and foliage, [mm-wave](#) spectrum is well-suited for localized deployments within campus areas, leveraging small cell infrastructure to provide seamless coverage and capacity where it's needed most. With careful planning and deployment, [mm-wave](#) spectrum enables organizations to harness the full potential of 5G technology, driving digital transformation and unlocking new opportunities for collaboration, research, and education within the campus ecosystem.

8 Conclusions

The concept of industrial automation based on 5G communication technology is being extensively studied and debated today. The promise of faster and more reli-

able wireless communication links provided by 5G holds the potential to increase the customization flexibility of industrial operations, enabling easier adaptation of the factory floor to changing communication demands. This report provides an overview of the available options and configuration choices for 5G deployment that can assist in designing a communication network for industrial CPS. Several 5G features and ongoing developments such as network slicing, MEC, 5G-TSN integration, 5G-DetNet integration, and 5G-OPC UA integration already allow communication support for diverse industrial applications. However, the assessment done in this report also acknowledges that the adoption of 5G as a communication system for industrial environments is not a straightforward task. While 5G supports digitization and automation of industrial networks and can provide communication services for several use cases, it is not a complete replacement for existing industrial communication networks.

The critical analysis conducted highlights that there are many open challenges that still require extensive research to provide effective solutions for industrial CPS. Of paramount importance is the need for validating low latency, determinism, and effective integration with technologies like TSN, DetNet, and OPC UA in real-world scenarios. Equally significant are ensuring security measures and achieving seamless integration between the original 5G specifications and widely accepted standards in the industrial domain. This latter aspect will require increased cross-domain standardization efforts. The evaluation of different 5G deployment options also highlights the limitations of the current state of 5G deployment in industrial practice. One of the essential factors is the lack of network automation and zero-touch management solutions which hinders easy deployment and configuration of the system. Nevertheless, despite the open challenges that still need to be addressed, this work shows that 5G in industrial automation has potential benefits in the long run.

Acronyms

3GPP	3 rd generation partnership project. 5
5G	5 th generation. 4–6, 22
5G-ACIA	5G alliance for connected industries and automation. 4
5GS	5G system. 9, 13, 19–29, 33
5QI	5G QoS Identifier. 19, 21, 32, 34
AF	application function. 20–22, 26
AI	artificial intelligence. 19
AIOTI	alliance for internet of things innovation. 4
AMF	access and mobility management function. 7, 8, 19, 31, 33
AP	access point. 33
API	application programming interface. 26, 27
APN	access point name. 11, 12
AR	augmented reality. 17, 43
ARP	allocation and retention priority. 32, 33
AUSF	authentication server function. 31
BBU	baseband unit. 29, 33
BS	base station. 10, 31
BW	bandwidth. 34
CAG	closed access group. 10, 11
CNC	centralized network configuration. 20, 21, 25
CP	control plane. 33
CPS	cyber-physical systems. 25, 26
CUC	centralized user configuration. 25

DetNet Deterministic Networking. [6](#), [22](#), [23](#)

DL downlink. [20](#), [22](#)

DN data network. [26](#)

DNN data network name. [34](#)

DS-TT device side TSN translator. [20–22](#), [25](#)

DSS dynamic spectrum sharing. [43](#)

EAS edge application server. [26](#), [27](#)

EASDF edge application server discovery function. [27](#)

ECS edge configuration server. [26](#), [27](#)

EEC edge enabler client. [27](#)

EES edge enabler server. [26](#), [27](#)

EHE edge hosting environment. [26](#)

eMBB enhanced mobile broadband. [18](#)

ETSI European telecommunications standards institute. [26](#), [27](#)

FDD frequency division duplex. [34](#)

FRER frame replication and elimination for reliability. [21](#)

GBR guaranteed bit rate. [20](#), [21](#), [32](#)

GFBR guaranteed flow bit rate. [19](#), [20](#), [32](#)

GM grandmaster. [20](#)

gNB gNodeB. [7](#), [8](#), [13](#), [15](#), [33](#)

gPTP generic precision time protocol. [21](#), [22](#)

I4.0 industry 4.0. [12](#), [14](#)

IoT internet-of-things. [24](#), [25](#), [27](#), [28](#)

ISG industry specification group. [26](#)

IT information technology. [4](#), [12](#), [13](#)

LTE long term evolution. [6](#)

MCC mobile country code. [34](#)

MEC multi-access edge computing. [5](#), [8](#), [10](#), [11](#), [15](#), [16](#), [25–27](#)

MFBR maximum flow bit rate. [20](#), [32](#)

ML machine learning. [19](#), [28](#)

mm-wave millimeter wave. [41](#), [43](#)

mMTC massive machine type communication. [18](#)

MNC mobile network code. [34](#)

MNO mobile network operator. [11](#), [12](#), [16](#), [42](#)

NAS non-access stratum. [31](#)

NAT network address translation. [30](#)

NEF network exposure function. [27](#)

NFV network function virtualization. [18](#)

NG-AP new generation application protocol. [31](#)

NG-RAN new generation radio access network. [32](#)

NID network identifier. [9](#)

NPN non public network. [8–13](#), [19](#), [28](#)

NR new radio. [6](#), [41](#)

NRF network repository function. [27](#), [31](#)

NSA non standalone. [6](#)

NSACF network slice access control function. [19](#)

NSSAAF network slice specific authentication and authorization function. [19](#)

NSSAI network slice selection assistance information. [19](#)

NSSF network slice selection function. [8](#), [19](#)

NW-TT network side TSN translator. [20](#), [22](#), [25](#)

OPC UA open platform communications unified architecture. 5, 6, 23–25

OT operational technology. 4, 12, 13, 17

PAL priority access license. 43

PCF policy control function. 7, 8, 21, 22, 27, 32

PDU protocol data unit. 8, 19, 21–23, 25, 27

PEC pervasive edge computing. 28

PFCP packet forwarding control protocol. 31

PLMN public land mobile network. 9–13, 19

PNI-NPN public network integrated NPN. 8–13, 16, 17, 28

PSFP per-stream filtering and policing. 21

PubSub publisher/subscriber. 25

QFI QoS Flow ID. 32, 33

QoS quality of service. 5, 7, 8, 13, 14, 16, 17, 19–21, 25–27, 31, 32, 42

RAN radio access network. 5, 6, 8, 9, 11–13, 16, 17, 19–22, 28, 29, 33

RQA reflective QoS attribute. 32

RRU remote radio unit. *Glossary: RRU*

S-NSSAI single NSSAI. 19

SA standalone. 6–10, 13, 19, 28

SBA service based architecture. 8, 26

SCS sub-carrier spacing. 34

SDN software-defined networking. 18

SL security level. 12, 13

SMF session management function. 7, 8, 21, 22, 31, 32

TDD time division duplex. 34

TSC time-sensitive communication. 21, 22

TSCAI TSC assistance information. [21](#)

TSCTSF time-sensitive communication time-sensitive function. [22](#), [23](#)

TSN time-sensitive networking. [5](#), [6](#), [13](#), [15](#), [16](#), [20–22](#), [24](#), [25](#)

TT TSN translator. [20](#), [21](#)

UDM unified data management. [31](#)

UE user equipment. [5–8](#), [10](#), [11](#), [13](#), [15](#), [16](#), [19–22](#), [26](#), [27](#), [31](#), [33](#), [34](#)

UL uplink. [20](#), [22](#)

UP user plane. [33](#)

UPF user plane function. [7](#), [8](#), [11](#), [16](#), [17](#), [19–21](#), [23](#), [26](#), [27](#), [31](#), [33](#)

uRLLC ultra-reliable low latency communication. [10](#), [11](#), [18](#), [20](#), [25](#), [41](#)

VLAN virtual local area network. [30](#)

VR virtual reality. [43](#)

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] 5G-ACIA. *5G Non-Public Networks for Industrial Scenarios*. Whitepaper, ZVEI â German Electrical and Electronic Manufacturersâ Association. 2019.
- [3] 5G-ACIA. *Key 5G Use Cases and Requirements*. Whitepaper, ZVEI â German Electrical and Electronic Manufacturersâ Association. 2020.
- [4] 5G-ACIA. *Security Aspects of 5G for Industrial Networks*. Whitepaper, ZVEI â German Electrical and Electronic Manufacturersâ Association. 2020.
- [5] 5G-PPP. *5G and the Factories of the Future*. Whitepaper, The 5G Infrastructure Public Private Partnership. 2015.
- [6] Ibrahim Afolabi et al. “Network slicing and softwarization: A survey on principles, enabling technologies, and solutions”. In: *IEEE Commun. Surveys Tuts.* 20.3 (2018), pp. 2429–2453.
- [7] Adnan Aijaz. “Private 5G: The Future of Industrial Wireless”. In: *IEEE Ind. Electron. Mag.* 14.4 (2020), pp. 136–145.
- [8] Adnan Aijaz, Nan Jiang, and Aftab Khan. “Toward Multi-Service Edge-Intelligence Paradigm: Temporal-Adaptive Prediction for Time-Critical Control over Wireless”. In: *IEEE Internet of Things Mag.* 6.1 (2023), pp. 96–101.
- [9] Junaid Ansari et al. “Performance of 5G Trials for Industrial Automation”. In: *MDPI Electronics* 11.3 (2022), p. 412.
- [10] 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.
- [11] Rojeena Bajracharya, Rakesh Shrestha, and Haejoon Jung. “Future Is Unlicensed: Private 5G Unlicensed Network for Connecting Industries of Future”. In: *Sensors* 20.10 (2020). ISSN: 1424-8220. DOI: [10 . 3390 / s20102774](https://doi.org/10.3390/s20102774). URL: <https://www.mdpi.com/1424-8220/20/10/2774>.
- [12] Davide Borsatti et al. “Enabling industrial IoT as a service with multi-access edge computing”. In: *IEEE Commun. Mag.* 59.8 (2021), pp. 21–27.
- [13] Dietmar Bruckner et al. “An introduction to OPC UA TSN for industrial communication systems”. In: *Proc. of the IEEE* 107.6 (2019), pp. 1121–1131.

- [14] Sherif Adeshina Busari et al. “5G Millimeter-Wave Mobile Broadband: Performance and Challenges”. In: *IEEE Communications Magazine* 56.6 (2018), pp. 137–143. DOI: [10.1109/MCOM.2018.1700878](https://doi.org/10.1109/MCOM.2018.1700878).
- [15] Richard Candell et al. “Industrial Wireless Systems Guidelines: Practical Considerations and Deployment Life Cycle”. In: *IEEE Ind. Electron. Mag.* 12.4 (2018), pp. 6–17.
- [16] Mohammed Chahbar et al. “A comprehensive survey on the E2E 5G network slicing model”. In: *IEEE Trans. on Network and Service Management* 18.1 (2020), pp. 49–62.
- [17] Pedro Cruz, Nadjib Achir, and Aline Carneiro Viana. “On the edge of the deployment: A survey on multi-access edge computing”. In: *ACM Computing Surveys* 55.5 (2022), pp. 1–34.
- [18] Mengmeng Cui, Yiming Fei, and Yin Liu. “A survey on secure deployment of mobile services in edge computing”. In: *Secur. and Commun. Netw.* 2021 (2021).
- [19] Jan deMeer et al. “The 5th GI/ACM Workshop 2020 Scope and Draft Programme on Standardization of Secure and Safe Smart Manufacturing Systems with respect to IEC 62443 IACS”. In: *INFORMATIK 2020*. Ed. by Ralf H. Reussner, Anne Koziolk, and Robert Heinrich. Gesellschaft für Informatik, Bonn, 2021, pp. 283–287. DOI: [10.18420/inf2020_26](https://doi.org/10.18420/inf2020_26).
- [20] David Dolezilek, Dennis Gammel, and William Fernandes. “Cybersecurity based on IEC 62351 and IEC 62443 for IEC 61850 systems”. In: *Proc. Int. Conf. on Develop. in Power Syst. Protection (DPSP)*. 2020.
- [21] Marco Ehrlich et al. “Automated Processing of Security Requirements and Controls for a common Industrie 4.0 Use Case”. In: *Proc. IEEE Int. Conf. on Networked Syst. (NetSys)*. 2019.
- [22] Marco Ehrlich et al. “Secure and Flexible Deployment of Industrial Applications inside Cloud-Based Environments”. In: *Proc. IEEE Int. Conf. on Emerg. Technol. and Factory Automat. (ETFA)*. 2019.
- [23] Mohamed Eldefrawy et al. “Formal security analysis of LoRaWAN”. In: *Computer Networks* 148 (2019), pp. 328–339.
- [24] ETSI Whitepaper No. 24. *MEC deployments in 4G and evolution towards 5G*. 2018.
- [25] ETSI Whitepaper No. 28. *MEC in 5G networks*. 2018.
- [26] ETSI Whitepaper No. 36. *Harmonizing standards for edge computing - A synergized architecture leveraging ETSI ISG MEC and 3GPP specifications*. 2020.

- [27] S. Gangakhedkar et al. “Use cases, requirements and challenges of 5G communication for industrial automation”. In: *Proc. IEEE Int. conf. on Commun. Workshops (ICC Wkshps)*. 2018.
- [28] Majid Gerami and Bikramjit Singh. “Configured Grant for Ultra-Reliable and Low-Latency Communications: Standardization and Beyond”. In: *IEEE Communications Standards Magazine* 6.4 (2022), pp. 40–47. DOI: [10.1109/MCOMSTD.0001.2000076](https://doi.org/10.1109/MCOMSTD.0001.2000076).
- [29] Majid Gerami and Bikramjit Singh. “Configured grant for ultra-reliable and low-latency communications: Standardization and beyond”. In: *arXiv preprint arXiv:2210.08940* (2022).
- [30] Amitabha Ghosh et al. “5G evolution: A view on 5G cellular technology beyond 3GPP release 15”. In: *IEEE Access* 7 (2019), pp. 127639–127651.
- [31] GSMA. *5G IoT Private & Dedicated Networks for Industry 4.0*. Whitepaper, Global System for Mobile Communications Association. 2020.
- [32] N. Hassan, K-L. A. Yau, and C. Wu. “Edge computing in 5G: A review”. In: *IEEE Access* 7 (2019), pp. 127276–127289.
- [33] Siegfried Hollerer, Wolfgang Kastner, and Thilo Sauter. “Towards a Threat Modeling Approach Addressing Security and Safety in OT Environments”. In: *Proc. IEEE Int. Conf. on Factory Commun. Syst. (WFCS)*. 2021.
- [34] *Time-sensitive networking (TSN) task group*. 2020. URL: <https://1.ieee802.org/tsn/>.
- [35] *Integration of 5G with Time-Sensitive Networking for Industrial Communications*. Whitepaper, ZVEI - German Electrical and Electronic Manufacturers' Association. 2020.
- [36] Juergen Jasperneite, Thilo Sauter, and Martin Wollschlaeger. “Why We Need Automation Models: Handling Complexity in Industry 4.0 and the Internet of Things”. In: *IEEE Ind. Electron. Mag.* 14.1 (2020), pp. 29–40. DOI: [10.1109/mie.2019.2947119](https://doi.org/10.1109/mie.2019.2947119).
- [37] Adlen Ksentini and Pantelis A Frangoudis. “On extending ETSI MEC to support LoRa for efficient IoT application deployment at the edge”. In: *IEEE Commun. Standards Mag.* 4.2 (2020), pp. 57–63.
- [38] Ana Larrañaga et al. “Analysis of 5G-TSN Integration to Support Industry 4.0”. In: *Proc. IEEE Int. Conf. on Emerg. Technol. and Factory Automat. (ETFA)*. 2020.
- [39] T-K. Le, U. Salim, and F. Kaltenberger. “An Overview of Physical Layer Design for Ultra-Reliable Low-Latency Communications in 3GPP Releases 15, 16, and 17”. In: *IEEE Access* 9 (2021), pp. 433–444.

- [40] Yaqiong Liu et al. “Toward edge intelligence: Multiaccess edge computing for 5G and internet of things”. In: *IEEE Internet of Things J.* 7.8 (2020), pp. 6722–6747.
- [41] Mattia Merluzzi, Paolo Di Lorenzo, and Sergio Barbarossa. “Wireless edge machine learning: Resource allocation and trade-offs”. In: *IEEE Access* 9 (2021), pp. 45377–45398.
- [42] Winnie Nakimuli et al. “Deployment and evaluation of an industry 4.0 use case over 5G”. In: *IEEE Commun. Mag.* 59.7 (2021), pp. 14–20.
- [43] Arun Narayanan et al. “Key Advances in Pervasive Edge Computing for Industrial Internet of Things in 5G and Beyond”. In: *IEEE Access* 8 (2020), pp. 206734–206754. DOI: [10.1109/ACCESS.2020.3037717](https://doi.org/10.1109/ACCESS.2020.3037717).
- [44] Tien-Dung Nguyen, Eui-Nam Huh, and Minh Jo. “Decentralized and revised content-centric networking-based service deployment and discovery platform in mobile edge computing for IoT devices”. In: *IEEE Internet of Things J.* 6.3 (2018), pp. 4162–4175.
- [45] Kota Nikhileswar et al. “Time-Sensitive Networking Over 5G for Industrial Control Systems”. In: *Proc. IEEE Int. Conf. on Emerg. Technol. and Factory Automat. (ETFA)*. 2022, pp. 6–9.
- [46] Jose Ordonez-Lucena et al. “Network slicing for 5G with SDN/NFV: Concepts, architectures, and challenges”. In: *IEEE Commun. Mag.* 55.5 (2017), pp. 80–87.
- [47] Jose Ordonez-Lucena et al. “The use of 5G Non-Public Networks to support Industry 4.0 scenarios”. In: *Proc. IEEE Conf. on Standards for Commun. and Netw. (CSCN)*. 2019.
- [48] Stefan Parkvall et al. “5G NR Release 16: Start of the 5G Evolution”. In: *IEEE Commun. Standards Mag.* 4.4 (2020), pp. 56–63.
- [49] Haixia Peng and Xuemin Shen. “Multi-Agent Reinforcement Learning Based Resource Management in MEC- and UAV-Assisted Vehicular Networks”. In: *IEEE J. on Sel. Areas in Commun.* 39.1 (2021), pp. 131–141. DOI: [10.1109/JSAC.2020.3036962](https://doi.org/10.1109/JSAC.2020.3036962).
- [50] Haixia Peng and Xuemin Sherman Shen. “DDPG-based Resource Management for MEC/UAV-Assisted Vehicular Networks”. In: *Proc. of IEEE Veh. Technol. Conf. (VTC2020-Fall)*. 2020.
- [51] Julius Pfrommer et al. “Open source OPC UA PubSub over TSN for realtime industrial communication”. In: *Proc. IEEE Int. Conf. on Emerg. Technol. and Factory Automat. (ETFA)*. Vol. 1. IEEE. 2018, pp. 1087–1090.

- [52] Quoc-Viet Pham et al. “A survey of multi-access edge computing in 5G and beyond: Fundamentals, technology integration, and state-of-the-art”. In: *IEEE Access* 8 (2020), pp. 116974–117017.
- [53] Jonathan Prados-Garzon et al. “5G Non-Public Networks: Standardization, Architectures and Challenges”. In: *IEEE Access* 9 (2021), pp. 153893–153908.
- [54] Theodore S. Rappaport et al. “Millimeter Wave Mobile Communications for 5G Cellular: It Will Work!” In: *IEEE Access* 1 (2013), pp. 335–349. DOI: [10.1109/ACCESS.2013.2260813](https://doi.org/10.1109/ACCESS.2013.2260813).
- [55] Ju Ren et al. “Joint Channel Allocation and Resource Management for Stochastic Computation Offloading in MEC”. In: *IEEE Trans. on Veh. Technol.* 69.8 (2020), pp. 8900–8913. DOI: [10.1109/TVT.2020.2997685](https://doi.org/10.1109/TVT.2020.2997685).
- [56] Justus Rischke et al. “5G Campus Networks: A First Measurement Study”. In: *IEEE Access* 9 (2021), pp. 121786–121803.
- [57] Ignacio Rodriguez et al. “An experimental framework for 5G wireless system integration into industry 4.0 applications”. In: *MDPI Energies* 14.15 (2021), p. 4444.
- [58] Ahmad Rostami. “Private 5G Networks for Vertical Industries: Deployment and Operation Models”. In: *Proc. IEEE 5G World Forum (5GWF)*. 2019.
- [59] José Manuel Gaspar Sánchez et al. “Edge computing for cyber-physical systems: A systematic mapping study emphasizing trustworthiness”. In: *ACM Trans. on Cyber-Physical Syst. (TCPS)* 6.3 (2022), pp. 1–28.
- [60] Zenepe Satka et al. “Developing a Translation Technique for Converged TSN-5G Communication”. In: *Proc. IEEE Int. Conf. on Factory Commun. Syst. (WFCS)*. IEEE. 2022, pp. 1–8.
- [61] Stefan Senk et al. “5G NSA and SA Campus Network Testbeds for Evaluating Industrial Automation”. In: *Proc. European Wireless (EW)*. 2021.
- [62] Hafiz Husnain Raza Sherazi et al. “Energy-Efficient LoRaWAN for Industry 4.0 Applications”. In: *IEEE Trans. Ind. Informat.* 17.2 (2021), pp. 891–902.
- [63] Haochuan Shi, Adnan Aijaz, and Nan Jiang. “Evaluating the Performance of Over-the-Air Time Synchronization for 5G and TSN Integration”. In: *Proc. IEEE Int. Black Sea Conf. on Commun. and Netwo. (BlackSeaCom)*. 2021, pp. 1–6. DOI: [10.1109/BlackSeaCom52164.2021.9527833](https://doi.org/10.1109/BlackSeaCom52164.2021.9527833).
- [64] Tobias Striffler, Nicola Michailow, and Michael Bahr. “Time-Sensitive Networking in 5th Generation Cellular Networks - Current State and Open Topics”. In: *Proc. IEEE 5G World Forum (5GWF)*. 2019.

- [65] T. Taleb et al. “On multi-access edge computing: A survey of the emerging 5G network edge cloud architecture and orchestration”. In: *IEEE Commun. Surveys Tuts.* 19.3 (2017), pp. 1657–1681.
- [66] Minh-Thuyen Thi et al. “IEEE 802.1 TSN Time Synchronization over Wi-Fi and 5G Mobile Networks”. In: *Proc. of IEEE Veh. Technol. Conf. (VTC2022-Fall)*. 2022, pp. 1–7.
- [67] A. Treytl, T. Sauter, and C. Schwaiger. “Security measures in automation systems—a practice-oriented approach”. In: *Proc. IEEE Int. Conf. on Emerg. Technol. and Factory Automat. (ETFA)*. 2005.
- [68] Rath Vannithamby and Anthony Soong. *5G Verticals: Customizing Applications, Technologies and Deployment Techniques*. John Wiley & Sons, 2020.
- [69] Shalitha Wijethilaka and Madhusanka Liyanage. “Survey on network slicing for Internet of Things realization in 5G networks”. In: *IEEE Commun. Surveys Tuts.* 23.2 (2021), pp. 957–994.
- [70] M. Wollschlaeger, T. Sauter, and J. Jasperneite. “The Future of Industrial Communication: Automation Networks in the Era of the Internet of Things and Industry 4.0”. In: *IEEE Ind. Electron. Mag.* 11.1 (2017), pp. 17–27. DOI: [10 . 1109/MIE.2017.2649104](https://doi.org/10.1109/MIE.2017.2649104).
- [71] Yulei Wu et al. “A survey of intelligent network slicing management for industrial IoT: Integrated approaches for smart transportation, smart energy, and smart factory”. In: *IEEE Commun. Surveys Tuts.* 24.2 (2022), pp. 1175–1211.
- [72] Ijaz Yahmad et al. “The Challenges of Artificial Intelligence in Wireless Networks for the Internet of Things: Exploring Opportunities for Growth”. In: *IEEE Ind. Electron. Mag.* 15.1 (2021), pp. 16–29. DOI: [10 . 1109/MIE.2020 . 2979272](https://doi.org/10.1109/MIE.2020.2979272).
- [73] Rong Yu and Peichun Li. “Toward resource-efficient federated learning in mobile edge computing”. In: *IEEE Network* 35.1 (2021), pp. 148–155.
- [74] Shunliang Zhang. “An overview of network slicing for 5G”. In: *IEEE Wireless Commun.* 26.3 (2019), pp. 111–117.