5G-ACIA White Paper

5G QoS for Industrial Automation

5G Alliance for Connected Industries and Automation

Table of Contents

1 Executive Summary

This white paper provides an overview of how 5G QoS can support the implementation of industrial applications. As 5G systems become integrated in factories, it's becoming increasingly important for key players involved in developing and operating Industrial IoT applications to understand the 5G QoS model and how applications can interact with the 5G network. This will help them customize and configure its capabilities to meet their particular requirements.

The paper is structured as follows:

- Chapter 3 describes how the 5G network applies QoS to connections. It also introduces basic terminology that nonspecialists need in order to understand how the described features of the 5G system work.
- Chapter 4 describes the relevant external interfaces of the 5G system and the steps that an IIoT application can perform to harness its functionality. Examples include requesting a specific QoS for a connection, requesting notification of QoS changes, and monitoring the QoS of a connection. The focus is on interfaces between user equipment (UE) and the 5G network and the interfaces that are available for network exposure using the 5G exposure function (5G-EF). It also presents several examples of IIoT applications that use the described functionality.

About 5G-ACIA

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

2 Introduction

Distributed industrial applications rely on the quality of service (QoS) of the underlying communications system, which must meet the relevant requirements in each case. Some industrial use cases pose highly demanding communication requirements and are therefore quite sensitive to any changes in QoS. 5G supports comprehensive mechanisms for defining, implementing, controlling, policing, and monitoring QoS. These include both dynamic QoS management for packet-level differentiation of traffic within a single connection and management of a 5G network's overall performance.

This white paper addresses industrial automation professionals who wish to take advantage of 5G QoS features in their applications. Its main purpose is to provide an easy-to-read technical guide on 5G QoS that frees users from having to study the details of 3GPP standards. It describes the functionality of 5G QoS from an end-user perspective and explains the terminology used in connection with configuring and using it. It also outlines the steps that an application can perform to request a certain QoS from the 5G network and monitor the actual QoS, illustrating these with real-world ex-

amples from industry. This functionality has been specified in response to requirements introduced by verticals.

Going beyond the basic functionality of the 5G QoS model, this paper also addresses related aspects such as:

- Features that support QoS-adaptive applications, in other words that are capable of adapting to some extent when the QoS changes
- How network slicing affects QoS, including possible impacts of network slice selection and how to choose a network slice
- Features related to QoS monitoring
- QoS aspects of TSN
- QoS aspects in connection with different NPN deployment options
- The 5G-EF functionality relevant to QoS that is available at the En reference point (see reference [1])
- Operating 5G QoS in the interface between the UE and the 5G network

QoS in 5G networks is a very broad topic and continually evolving along with the 5G specifications. To establish a common baseline, this white paper only addresses functionality that was agreed during the normative work phase for 3GPP Release 16. It doesn't cover requested factory automation features that aren't yet available in Release 16, which include but aren't limited to the following:

- QoS for multicast
- End-to-end (QoS) communication services for UE-UE communication
- QoS monitoring of parameters other than packet latency for device connections (UE-UPF)
- QoS for any connections besides those between UEs and the UPF
- Operation of 5G QoS via a 5G device's exposure function, specifically the Ed reference point (see [1] for details)

In order to focus on what is currently considered to be the most important functionality for IIoT applications, the following topics have been excluded from the discussion (despite being covered by 3GPP Release 16):

- QoS analytics
- Detailed aspects of QoS related to handover between cells

It is probable that these topics, as well as other aspects of QoS, will evolve significantly in subsequent 3GPP releases.

The following aspects have also been excluded, although they have some relevance to the goals of this white paper:

- How to convert the characteristic parameters of a communication service (see section C.2.2 of [8]) into 5G-internal parameters
- UE interfaces to the OS and applications

3 Introduction to 5G QoS Functionality

This chapter presents the basic concepts and functionality of the 5G QoS model. It describes the included functions for enabling applications to adapt to changes in QoS; the relationships among 5G QoS, 5G network slicing, and TSN; QoS monitoring functionality; and QoS aspects of various non-public network deployments.

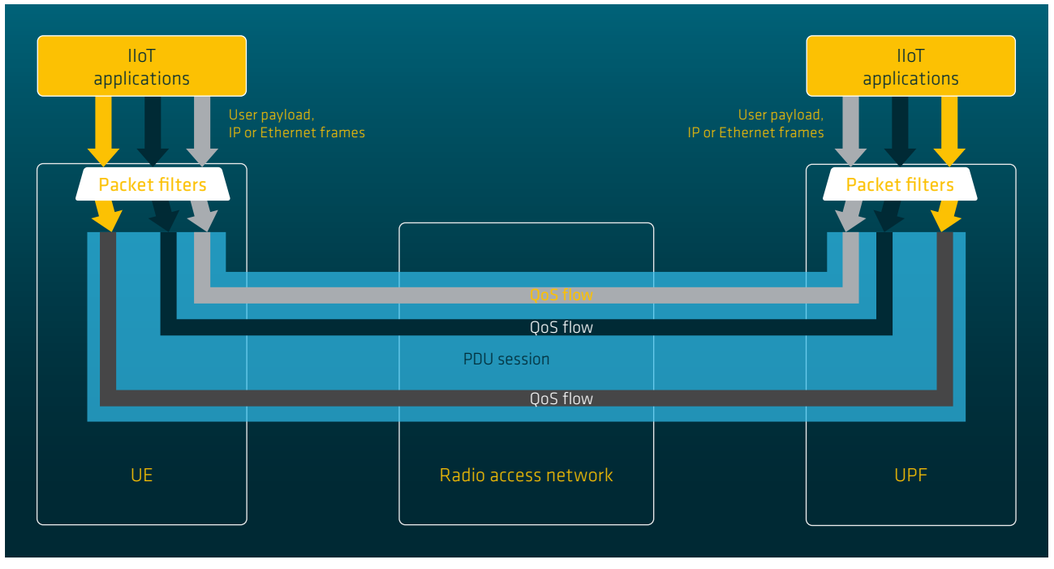
3.1 The QoS Model: Overview, Basic Concepts, and Functionality

Figure 1 below provides a high-level functional view of the QoS model of a 5G system. In a 5G system, the concept of QoS is always applied to a specific connection. A connection in this sense is a QoS flow within a PDU session. A device can have multiple connections in one or more PDU sessions, depending on how the packet filters are set. A PDU session is a logical connection within the 5G system that carries IP packets or Ethernet frames between a user equipment (UE) and user plane function (UPF) as shown in figure 1. In the 5G system, a QoS flow is defined as the smallest granularity for differentiating traffic in terms of scheduling, queue management, rate shaping, etc. They are characterized by a set of QoS attributes that are in turn divided into QoS characteristics and QoS parameters. All of these are explained in greater detail in the following sections.

An IIoT application can select values for QoS attributes as required for each connection (see section 4.1 for details). Once a connection has been successfully established, the 5G system is responsible for providing the required QoS. Whether or not it can do so depends on the UE subscription options, implemented and deployed 5G system capabilities, and network conditions (radio and system load). These are also discussed in greater detail.

It is important to note that different connections can have the same or different QoS attributes. Section 4.1 describes how an application can modify a QoS flow's attributes.

Figure 1: A high-level 5G QoS model



Source: 5G-ACIA

How PDU sessions and QoS flows are set up, configured, and supervised in the 5G system is invisible to the IIoT application. It doesn't matter whether the IIoT application connects to the 5G system via a UE or a data network.

IIoT applications don't need to manage and keep track of PDU sessions and QoS flows. For downlink data (from UPF to UE), the UPF identifies the PDU session by the destination MAC address or the IP address of the traffic. The QoS flow is implicitly identified by packet filters containing sets of application data parameters. Both the UPF and the UE use packet filters to map traffic onto corresponding QoS flows. This lets the packet filters map all QoS traffic in both directions: from UE to UPF and vice versa.

A packet filter applies one or more application data parameters to identify traffic in a given QoS flow. The possible parameters include the direction of traffic (uplink or downlink) and for IP PDU sessions the source or destination IP address or IPv6 prefix, source and destination port numbers, protocol identifier, and type of service or traffic class. For Ethernet PDU sessions they include the source and destination MAC address, priority code point (PCP), Ethernet type, and other parameters as described in section 5.7.6.2 of reference [3].

A packet filter can include any combination of application data parameters (including a range of values if applicable). For example, a packet filter that includes port no. 80 matches all HTTP traffic, and a packet filter with the destination IP address 10.10.10.10 matches all traffic heading to that address. It should be pointed out that packet filters are only associated with a single PDU session; for example, a packet filter with port 80 associated with PDU session A won't be applied to traffic of PDU session B for the same UE.

A QoS-enabled connection can also link two UEs in the same 5G network. In such a case, application data is transmitted from one UE to another UE via the network. Each application data packet traverses the entire 5G network twice. In this case, the IIoT application has to request two separate connections as well as values for the QoS attributes of each connection.

From an IIoT application's perspective, the 5G system has separate reference interfaces for ingress and egress (i. e. inbound and outbound) application data. In figure 2, the reference interface to the UE is shown on the left and that to the UPF on the right. It should be stressed that the 5G QoS model doesn't include aspects related to non-3GPP communications. Any connected data network with layer 2 or 3 capabilities must therefore be configured and engineered to ensure overall QoS from the application's perspective. This is illustrated in figure 2, in which a 5G system's QoS functionality includes all nodes between the communication service interface (CSI) reference points but not the entire logical link between two IIoT applications. The 5G-ACIA white paper "Performance Testing of 5G Systems for Industrial Automation" (reference [35]) goes into greater depth on this.

From a protocol stack perspective, the 5G system applies QoS attributes to the connection between the two CSI reference points shown in figure 2, namely between radio protocol layers 2 and 3 and UPF levels 2 and 3.

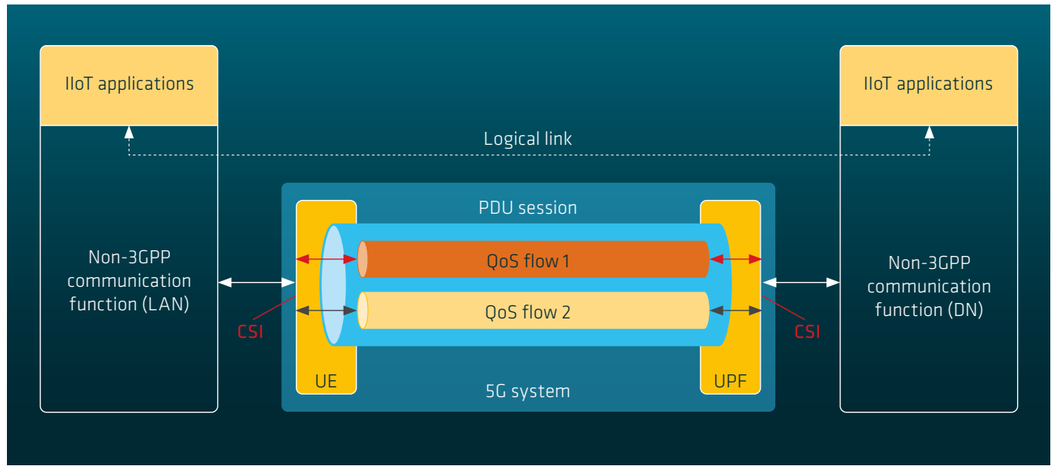
As already mentioned, the 5G system's internal mechanisms for QoS management are invisible to the IIoT applications. Some key concepts and parameters are described below. Application data are scheduled in a QoS flow that is defined by a QoS profile. This profile consists of a set of parameters including those listed below. Please refer to section 5.7.2 of reference [3] for additional details and an extensive list.

- **5G QoS identifier (5QI):** An integer that identifies a set of values for the QoS characteristics explained later in this chapter.
- **Allocation and retention priority (ARP):** This parameter indicates a QoS flow's relative importance or priority. It can have a value between one and 15, with one corresponding to the highest priority. The 5G network uses it to decide how a QoS flow should be served when resources are limited. When resources are limited, the network can also use the assigned value to decide which existing QoS flow to preempt to free up resources.
- **Reflective QoS attribute (RQA):** This optional parameter only applies to QoS flows without a guaranteed bit rate. Simplifying somewhat, it specifies that the same QoS applied to downlink traffic should also apply to uplink traffic.
- **Guaranteed flow bit rate (GFBR):** The bit rate that the network can be expected to provide for a QoS flow over the averaging window (described below).
- **Maximum flow bit rate (MFBR):** In QoS flows with a guaranteed bit rate, this parameter defines the maximum value that the actual rate can have.
- **Notification control:** In QoS flows with a guaranteed bit rate, this parameter specifies whether or not the radio access network (RAN) should be notified if the GFBR can no longer or once again be ensured during the lifetime of a QoS flow. It may only be used if the application is able to adapt to a change in the QoS as described in section 3.2 below.
- **Maximum packet loss rate:** In QoS flows with a guaranteed bit rate that are used to carry voice media, this parameter indicates the maximum tolerable percentage of lost packets in the uplink and downlink directions.

The following QoS characteristics are referenced by 5QI values (see section 5.7.3 of [3]):

- **Packet delay budget (PDB):** This parameter sets an upper limit on the amount of time by which a packet may be delayed while traveling between CSIs. If a packet is split up or combined with other packets while traveling within the 5G system, these operations affect on the packet delay budget. To avoid packet fragmentation between CSIs in the 5G system, the network can inform the UE of the size (in bytes) of the maximum transfer unit (MTU) when establishing a PDU session. This is done to limit the size of the packets sent by the UE to the network. See sections 5.6.10 and 5.7.4 and annex J of reference [3] for more information.
- **Resource type:** This setting determines whether or not network resources are permanently allocated for a guaranteed or unguaranteed bit rate (GBR or non-GBR). The bit rate required for delay-critical GBR QoS flows is also specified and permanently allocated. If a packet is delayed by more than its PDB, it is counted as lost.
- **Priority level:** This is a positive integer assigned to indicate a flow's priority in relation to other flows for scheduling resources. The lowest priority level value corresponds to the highest priority.

Figure 2: A user-to-network (UN) connection with links to non-3GPP data networks



Source: 5G-ACIA

- **Packet error ratio (PER):** This is the number of incorrectly received and lost packets divided by the total number of received packets.
- **Default maximum data burst volume:** This parameter is related to delay-critical GBR resources and specifies the largest data volume that can be sent without exceeding the packet delay budget.
- **Default averaging window:** This parameter has to do with GBR resources; it indicates the time allotted for calculating the guaranteed flow bit rate (GFBR) and maximum flow bit rate (MFBR) for a given traffic flow.

To sum up, the QoS attributes used to specify traffic in a particular QoS flow consist of a set of QoS characteristics, which is referenced by a 5QI value, and QoS parameters. Which parameters can be applied to a given QoS flow also depends on whether it is a GBR or non-GBR flow. For example, GFBR and MFBR can only apply to GBR-type QoS flows. A set of standardized 5QI values is defined for the services that are most commonly used in a given mobile network. This set can be extended by assigning nonstandard 5QI values, which lets service providers to apply alternative value sets to QoS characteristics. Table 1 shows example mappings between 5QI values and value sets for QoS characteristics.

Table 1: Examples of standardized 5QI-to-QoS mappings (excerpt from table 5.7.4-1 in [3]).

5QI value	Resource type	Default priority level	Packet delay budget	Packet error ratio	Default maximum data burst volume	Default averaging window	Example services
2	GBR	40	150 ms	10^{-3}	N/A	2000 ms	Conversational video (live streaming)
6	Non-GBR	60	300 ms	10^{-6}	N/A	N/A	Video (buffered streaming) TCP-based
…	…	…	…	…	…	…	…
82	Delay-critical GBR	19	10 ms	10^{-4}	255 bytes	2000 ms	Discrete automation
83	Delay-critical GBR	22	10 ms	10^{-4}	1354 bytes	2000 ms	Delay-critical GBR

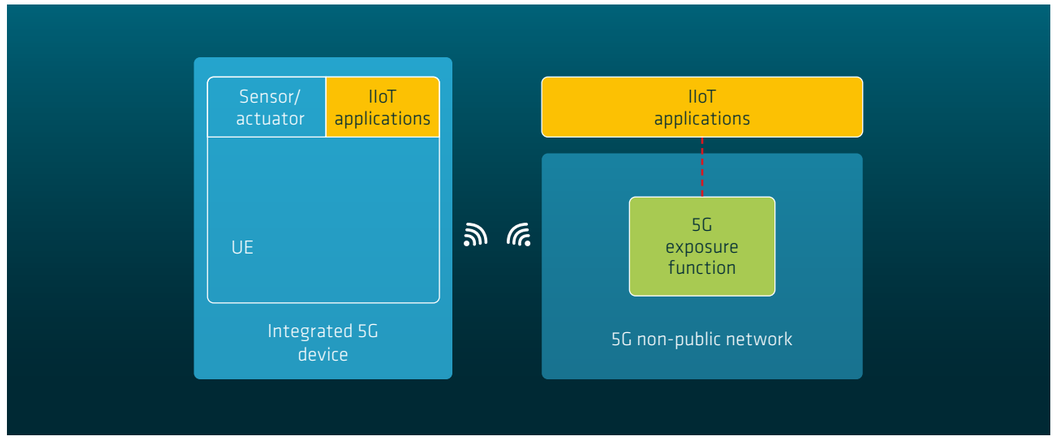
An IIoT application's QoS can be established in various ways:

1. Subscribed QoS profile
The simplest approach is to let the 5G system choose an UE's subscribed QoS profile. All profiles are stored in the 5G system. The application itself doesn't need to configure anything; the stored QoS profiles are automatically applied to every connection that the UE creates. Changing subscribed QoS profiles requires action on the part of the service provider (SP); section 4.1.2 of this white paper explains how this is done.

2. Application-detection-based QoS
The service provider can use application IDs for association with a preconfigured profile that includes a packet flow description (PFD). PFDs typically include application data protocol information such as the IIoT application's IP address and port number and parts of the application URL. If the UPF detects a data flow that matches the preconfigured packet filters, the 5G network automatically applies preconfigured QoS values to it. Like the subscription-based method, this method requires no action on the part of the application.

3. UE-controlled QoS
When an IIoT application connects to a UE, APIs in its 5G module specify a QoS level. The application therefore has complete flexibility for defining the profile and modifying the QoS profiles of previously established connections. This is described in section 4.1.3 of this white paper. When establishing or modifying a connection, the 5G network checks whether

Figure 3: Functional view of network exposure



Source: 5G-ACIA

the QoS profile requested by the IIoT application is allowed by the UE subscription profile, network configuration, and current network conditions. The APIs in the OS and chipsets of 5G modules have been standardized by 3GPP (see [33]), although chipsets may also support other APIs. This method is available when the IIoT application resides in the 5G device.

4. Network-exposure-controlled QoS
Similarly to UE-controlled QoS, the IIoT application can also flexibly choose QoS parameters as described in section 4.1.4 of this white paper and section 5.2.6 of reference [9]. This method has many advantages. Instead of directly interfacing with a variety of APIs from multiple 5G module vendors, the IIoT application only has to include a single 5G network API that controls all of the involved UEs. The IIoT application can also use this 5G network to monitor QoS after a device connection has been created and subsequently changed or severed. Figure 3 shows a simplified network exposure deployment in which the network API is implemented by the 5G network exposure function. The IIoT application can be implemented on a device's application processor or any other computing entity that has IP connectivity with the 5G network. For more detailed information on this, see section 3 of [1] and [2].

3.2 Support for QoS-Adaptive Applications

For QoS profiles that use 5QIs of the GBR (guaranteed bit rate) type, the 5G network also supports a mechanism that lets the application

- specify a prioritized list of alternative QoS profiles, in addition to the original QoS profile, that the network can select in case the original profile isn't supported and
- receive notifications both on the UE side and in the entity connected to the application function (AF) via the 5G exposure function (NEF) in case the network needs to switch to another QoS profile in response to changing network conditions.

This lets the application provide a set of alternative QoS levels for use by the network under different conditions, while also enabling the application to adapt to these. This is triggered by notifications sent by the network to the application. In this context, applications that are able to adapt to changes in the QoS are called "QoS-adaptive applications". Support for these is part of how 5G controls QoS, independently of how the application determines the required QoS (this was addressed in section 3.1).

Section 4.2 describes how a QoS-adaptive application can use alternative QoS profiles to adjust its operating mode to suit the QoS profile that the network is currently applying. When the network switches from one QoS profile to another, it notifies the application if it has been requested to do so. Notifications are requested by setting a parameter called "notification control" in the QoS profile. These notifications can be received by the UE, which forwards them to the part of the application residing in it, and/or by the AF (application function) via the NEF. A UE can be automatically notified every time the network changes its QoS profile, eliminating the need to specifically request this every time, while the AF must ask to be notified. The AF can also instruct the network to stop sending these notifications to the UE. Section 4.2 explains the details of these notification mechanisms. They are only available for QoS flows with a guaranteed bit rate.

To illustrate use of the functionality described here, consider a handover between two cells. If the network is unable to meet certain stringent QoS requirements (i. e. characteristics or parameters specified by a QoS profile), it must downgrade to another QoS profile with more relaxed values for those characteristics or parameters.

For more information on this mechanism, see section 5.7.1.2a of [3] and section 4.4.9 of [19].

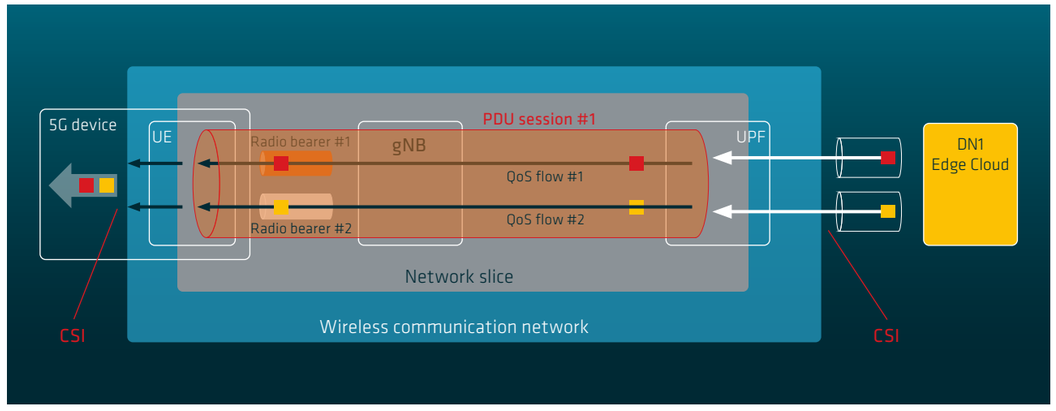
3.3 QoS and Network Slicing

Unlike earlier networks, which were designed as monolithic blocks, the 5G system supports "network slicing". This network architecture enables multiplexing of independent virtualized logical networks (called "network slices") on the same physical infrastructure. Each network slice is an isolated end-to-end network tailored to meet the requirements of a particular application. A service provider can make slices available for use by different enterprises or different entities of the same enterprise. By default, a 5G network comprises a single network slice that is equipped with all 5G system functions and defined QoS characteristics. From a QoS perspective, there is no need to apply network slicing. This section describes the main QoS principles that apply in the 5G system in case a service provider decides to take advantage of network slicing.

A network slice is a logical network with certain defined capabilities and characteristics. For example, one network slice could be tailored to provide services requested by smartphones while another is deployed for IoT services that support TSN or URLLC features. Every network slice is basically able to support all possible services, however, so it's up to the operator to decide whether or not to integrate slicing capabilities into a network.

In the following, some example scenarios are described in which devices connect to different data networks via a multiplexed 5G network with a defined number of slices, PDU sessions, QoS flows, radio bearers, and slice-specific QoS. According to 3GPP specifications, a particular PDU session belongs to exactly one specific network slice. If a UE needs to connect to more than one network at the same time, it has to establish at least one PDU session for each slice (see section 4.1.2 for details on how PDU sessions are established). A network slice can in turn support multiple PDU sessions for each UE, and conversely a UE can support up to 16 concurrent PDU sessions. If enough resources are allocated to a network slice, it can support all of a network's active PDU sessions.

Figure 4: A UE accessing a network slice with one PDU session



Source: 5G-ACIA

By way of example, figure 4 shows a UE accessing a single network slice connected to a data network that supports Edge Cloud-based services. The UE has established a PDU session with multiple QoS flows, which may be required to support various QoS profiles for different traffic flows. The QoS flows shown are mapped to different radio bearers, but it's also possible to map multiple QoS flows to the same radio bearer.

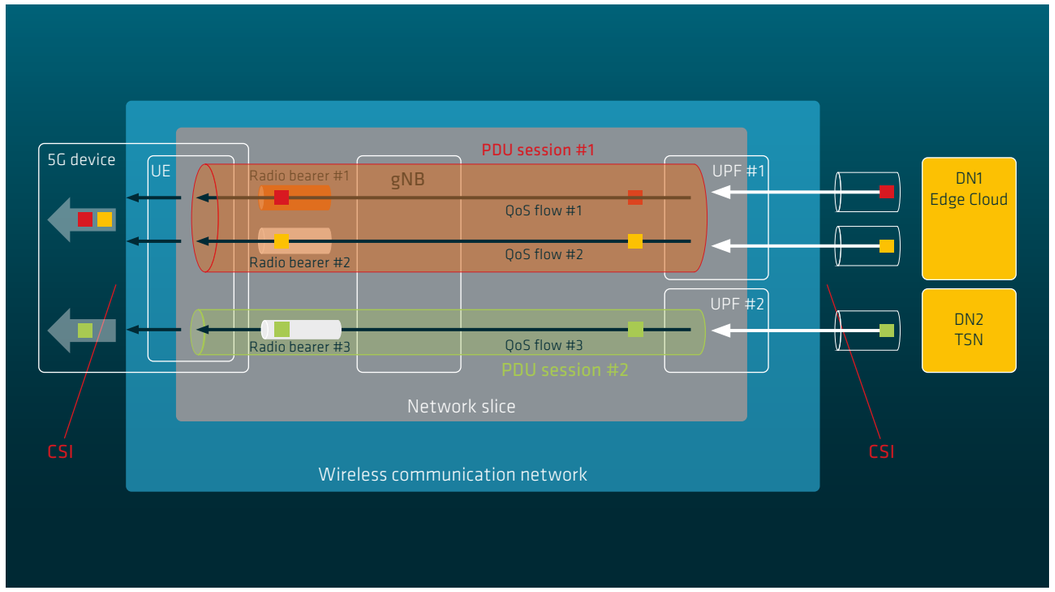
It's important to keep in mind that, although the figure shows each QoS flow associated with a different radio bearer, if allowed by the QoS profile it's also possible for multiple QoS flows to be associated with the same radio bearer.

Figure 5 shows a UE accessing a single network slice that is connected to two data networks: one that supports Edge Cloud-based services and a second that supports time-sensitive networking (TSN) services. The UE has requested the establishment of two PDU sessions, one for each service. In this scenario, each PDU session has multiple QoS flows that handle traffic differently for each service. For example, QoS flow #1 and QoS flow #2 are associated with the Edge Cloud services, while QoS flow #3 is used for TSN services. The 5G system specifications allow PDU session #2 to support TSN services via 5G TSN with a corresponding QoS profile for low latency, for example with a 5G network serving as a bridge, while PDU session #1 supports QoS profiles for Edge Cloud services.

Figure 6 provides another example: here a UE is concurrently accessing two network slices, one for a data network that supports services requested by Edge Cloud and the other for a network for providing TSN-based services.

The 5G system supports both of the scenarios shown in figures 5 and 6. It's up to the 5G network's owner to choose one. In figure 5, a single network slice is set up to support all services as required. The scenario shown in figure 6 may be appropriate if the 5QIs requested by QoS flows #1 and #2 can only be provided by network slice #1, while only network slice #2 supports TSN, depending on the service level specifications (SLS). The possible reasons for selecting one over the other aren't limited to QoS management considerations; they can also include geographical factors: for example, whether or not both network slices are available in the same area, whether traffic should be segregated in order to divide it between different network instances, whether there is a wish to facilitate lifecycle management for each network slice, whether a network needs to operate on its own or together with one or more others, and so on.

Figure 5: A UE accessing a network slice with two PDU sessions

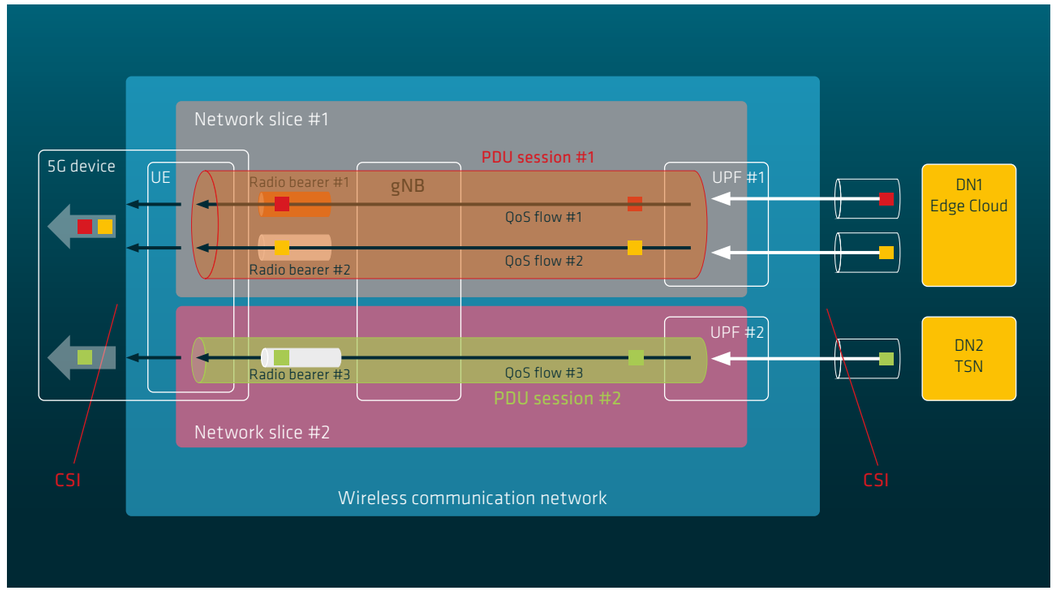


Source: 5G-ACIA

In all of these examples, each time that a PDU session is established or modified the 5G system only allows QoS flows with attributes that are supported by the corresponding network slices. In figures 5 and 6, if a network slice has been created to support a data rate of up to 50 Mbit/s per user and a minimum latency of 20 ms, and if a UE then requests a QoS flow with a data rate of 100 Mbit/s and/or a latency of 10 ms, the 5G system will reject it. Other requests are only authorized if they are consistent with the network slice's performance attributes.

The slices that the UE can connect to are determined when the UE first registers with the network, and they depend on how the UE and network are configured. The UE may request registration for multiple network slices, depending on the configuration defined by the network operator. The network provides a list of permissible slices based on available information on the user's subscription and the network's deployment and configuration. In every case, the list of slices requested by a UE must be confirmed by the network during the registration process. For a more detailed explanation of how applications select network slices, see chapter 8.

Figure 6: A UE accessing two network slices



Source: 5G-ACIA

3.4 QoS Monitoring

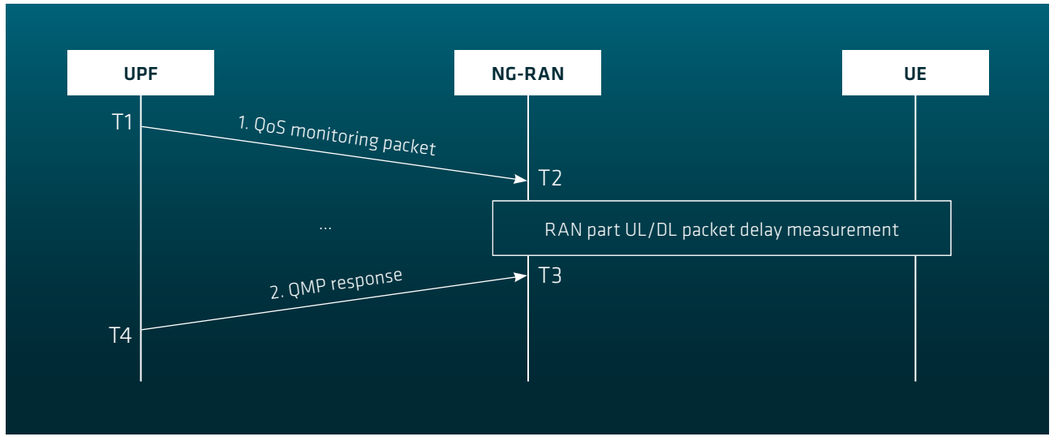
This section explains the QoS monitoring mechanisms that are supported in 5G. See section 4.4 for a discussion of the uses of QoS monitoring. For an in-depth description, see section 5.33.3 of reference [3].

The requirements for monitoring QoS in 5G systems were first addressed in connection with Release 16, as part of a 3GPP study on communication for automation in vertical domains (see reference [14]). The requirements identified by that study were then integrated into the 5G technical specification "Service Requirements for the 5G System" (reference [15]).

Release 16 applies QoS monitoring to measure packet delays between a UE and a user plane function (UPF) in the 5G system. For this to work and prevent packets from being fragmented, it's necessary to carefully determine the maximum packet size sent by the UE at the CSI (see also section 3.1). Assuming that this is the case, the total delay is the sum of the packet delays measured on the uplink (UL)/downlink (DL) of the radio access network (RAN) part as defined in [4] and the uplink/downlink of the core network part. The RAN integrates QoS monitoring by measuring the UL/DL packet delay. QoS monitoring of the UL/DL packet delay between the RAN and UPF can be carried out for affected services as shown in figure 7.

End-to-end measurement of UL/DL packet delays between a UE and UPF for a QoS flow can be activated when establishing or modifying a PDU session. The QoS monitoring request can contain monitoring parameters such as a DL/UL delay or round-trip packet delay, depending on the authorized QoS monitoring policy and/or local configuration. Regardless of whether or not the NG-RAN and UPF are time-synchronized (which depends on whether they share the same time reference), the UPF creates and sends monitoring packets to the RAN following this procedure, which is illustrated in figure 7:

Figure 7: QoS monitoring for packet transmission



Source: 5G-ACIA

1. The UPF encapsulates the QoS monitoring packet (QMP) indicator (which shows that the packet is used for measuring the UL/DL packet delay) and local time T1 (see section 5.5.2.1 of [5]) at which the UPF sends the DL monitoring packets.
2. The NG-RAN records local time T1 when the DL monitoring packets are received and local time T2 when they are received. The NG-RAN initiates the RAN part of the UL/DL packet delay measurement process.
3. The NG-RAN places the following values in the monitoring response packet: the QMP indicator, the RAN part of the measured UL/DL packet delay, the time T1 (see above), the local time T2 at which the DL monitoring packet is received, and the local time T3 at which NG-RAN dispatches the monitoring response packet to the UPF (see section 5.5.2.2 of [5]).
4. The UPF records local time T4 when the monitoring response packets are received and calculates the duration of the round trip (if not time-synchronized) or UL/DL packet delay (if time-synchronized) between the NG-RAN and UPF based on the time information contained in the received monitoring response packet. If the RAN and UPF aren't time-synchronized, the UPF calculates the UL/DL packet delay between the NG-RAN and the UPF according to the formula (T2-T1+T4-T3)/2. If the RAN and UPF are time-synchronized, the UPF calculates the UL and DL packet delays between the RAN and UPF (equal to T4-T3 and T2-T1, respectively). The UPF calculates the UL/DL packet delay between the UE and UPF based on the received RAN part of the UL/DL packet delay result and the calculated UL/DL packet delay between RAN and UPF.

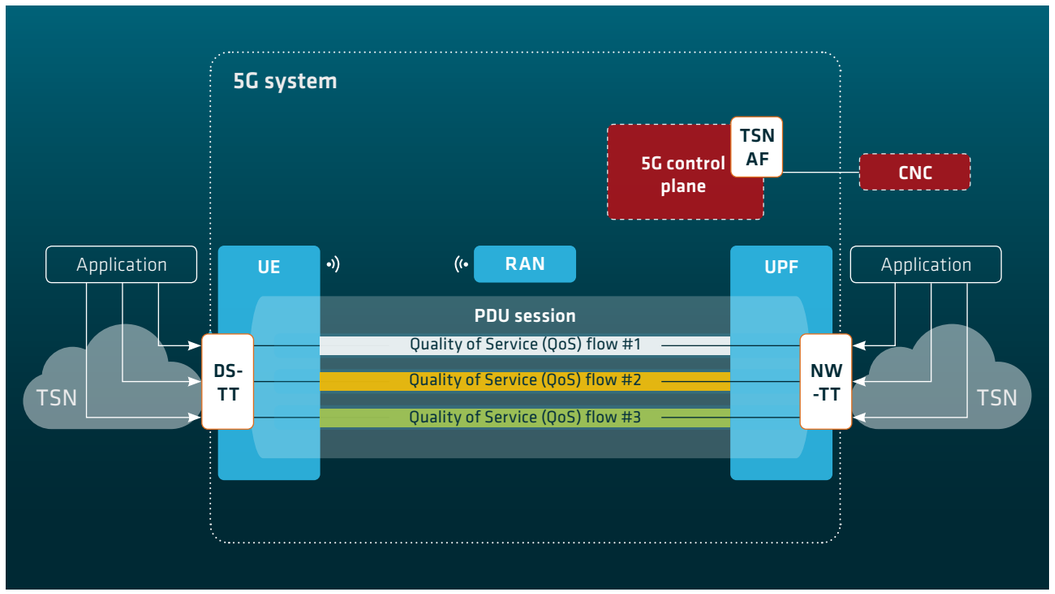
3.5 QoS and TSN

Time-sensitive networking (TSN) is a set of open standards developed by a IEEE working group to ensure deterministic, reliable, high-bandwidth, low-latency communication. Support for TSN was introduced in Release 16 of 5G and extended in Release 17. The fully centralized TSN configuration model as specified by IEEE 802.1Qcc has been adopted for 5G-TSN integration. The 5G system uses one or more virtual or logical TSN-capable bridge(s) of the TSN network to interact with the TSN network on the control or user plane (see [16] and [3]). Such a logical TSN-capable bridge is also referred to as a 5G system bridge. It includes TSN translator (TT) functionality for interacting with the TSN network. TSN translator functionality is available:

- on the control plane via a TSN application function (TSN AF),
- on the UE side via a device-side TT (DS-TT), and
- on the user plane function (UPF) side via a network-side TT (NW-TT).

A 5G system can interact via a TSN AF with a centralized network configuration (CNC) entity that manages network resources for TSN applications (users). The interface between the TSN AF and CNC is standardized in IEEE 802,1Q. The 5G system exposes bridge, port, and topological information, such as the names and addresses of ports and bridges, numbers of ports, and the IEEE 802.1AB link layer discovery protocol (LLDP) (see [23]). The TSN AF also exposes QoS capabilities such as guaranteed maximum delays between ports in the 5G system bridge. The port used by a 5G system bridge can be either a DS-TT port on the UE side or a NW-TT port on the UPF side. 5G also supports various IEEE 802.1Q traffic classes (see [24]) and IEEE 802.1Q-based priority code points (PCPs) (see [24]) for prioritizing traffic. The supported traffic classes are also exposed to CNC via the TSN AF (see [3]).

Figure 8: QoS mapping between TSN traffic and 5G QoS flows



Source: 5G-ACIA

When TSN traffic arrives at the 5G system bridge, the system maps it to 5G QoS flows in a corresponding PDU session as shown in figure 8. A 5G system can receive QoS information for the TSN traffic from the CNC via TSN AF. The preconfigured mapping table in the TSN AF is used to identify a suitable 5G system QoS profile. Based on the information received, the 5G system selects an appropriate QoS profile for each TSN stream and then establishes a 5G QoS flow with the selected QoS profile for carrying the requested TSN stream. In a given PDU session, multiple 5G QoS flows can be established for various TSN streams with different QoS requirements. QoS and packet detection rules for packet filters (see [3]) at the input of the 5G TSN bridge can be used to map various TSN streams to corresponding 5G QoS flows.

The TSN AF can also calculate time-sensitive communication assistance information (TSCAI) from the per-stream filtering and policing (PSFP) information received from the CNC. This TSCAI can then be provided to the 5G RAN to enable it to more efficiently schedule periodic and deterministic traffic flows (see [3]).

3.6 QoS and NPN Deployment Scenarios

A non-public network (NPN) is a 5G network system that is deployed by a closed group of users for their private use. An example is an enterprise network on a company's premises. A previous 5G-ACIA white paper (reference [30]) extensively described several scenarios involving the use of NPNs in connection with the Industrial IoT. Two types of NPN are generally distinguished (see section 5.30 of [3]):

- **Standalone NPN (SNPN):** a non-public network that doesn't rely on functions provided by a PLMN
- **Public network integrated NPN (PNI-NPN):** a non-public network deployed for private use by an enterprise. Unlike a standalone NPN, it's completely or partly hosted on PLMN infrastructure. It is based on a contract between an enterprise and a mobile operator.

In the case of a standalone NPN (SNPN), the enterprise using it is also responsible for managing it (either directly or indirectly by outsourcing this task to a NPN operator or other partner), including configuration, troubleshooting, performance monitoring, and network maintenance for both control plane and user plane functions. UE subscriptions and QoS profiles have to be configured in the 5G system in order for applications to access the network and request the required QoS. This is usually done via standard exposed interfaces (such as NEF, CAPIF, SEAL, etc.) or other, nonstandard interfaces, which exceed the scope of this white paper. The enterprise may also have access to internal 5G interfaces exposed by different network functions, in which case it has greater flexibility for configuring the network. See section 4.6 for a more detailed discussion of operational aspects.

In the case of a PNI-NPN, the mobile operator provides support for implementation and network management, possibly creating a dedicated network slice for the enterprise. Network functions can be deployed within the enterprise or on the mobile operator's premises or both. Where exactly specific network functions are deployed depends on latency and/or privacy/security considerations. In order to access the network, a subscription must be obtained from the mobile operator for each 5G-compatible UE used by the IIoT application. The subscription can include the QoS configuration needed for the device in question. Like in SNPN mode, devices can be configured either via standard exposed interfaces (like NEF, CAPIF, SEAL, etc.) or via nonstandard interfaces, which aren't covered by this white paper. The internal 5G interfaces that can be used for detailed configuration of QoS profiles for the traffic of a subscription include one that is exposed by the policy control function (PCF). Reference [32] describes how internal interfaces of this type (with either complete access or SLA-based access restrictions) can be provided on the basis of an agreement between the NPN operator and MNO. However, there is no guarantee that mechanisms like those described in reference [32] will become widely available anytime soon. Reference [32] is part of Release 16, and so far 3GPP hasn't announced any plans to extend access to the internal interfaces of network functions. For the most part, when network functions expose internal 5G interfaces it is on the basis of agreements between the mobile network and NPN operators.

From the perspective of QoS management functions that are supported by the 5G network, these two NPN deployment options are equivalent. The signaling procedures for setting up a session with a given QoS are the same in both scenarios, as described in section 4.1. The differences between them have to do with the roles of and control by the involved stakeholders with regard to network functionality and the performance delivered to end user applications, and accordingly also business and engineering aspects related to network operation and maintenance. In case of an SNPN, the entire network is under the control of the enterprise, which – at least in theory – therefore has a free hand to make any changes whatsoever to the configuration. In the case of a PNI-NPN, the relationship between the enterprise and mobile operator is defined by a service level agreement. For example, if the enterprise needs to change the QoS attributes for a certain application, it must either do so via the available interfaces or else request the mobile operator to make the changes. Because mobile operators possess considerable experience in managing complex networks, they are able to tweak the 5G network slicing framework to let enterprise customers share hardware resources while still having their own dedicated networks. This puts them in a position to provide cost-effective network management services to enterprises as described in reference [13].

For large enterprises, it may be necessary to interconnect multiple campuses. In such a case, QoS is also relevant to links between them. Consequently, an application may have to meet QoS requirements not only for each individual campus, but also for links between campuses. In the case of SNPN, the enterprise itself is responsible for building the links between campuses or, alternatively, leasing lines from a service provider to ensure that all QoS requirements are met. A PNI-NPN will probably include all campus areas and can therefore be administered by the same mobile operator, which makes it easier to coordinate QoS requirements regardless of whether connections within a single campus or between different campuses are involved.

An enterprise may wish to have full control over its non-public 5G system for a number of reasons, which can include business choices, technical aspects, network configurability, security policies, and/or regulations. In order to deploy and

manage an SNPN, the enterprise will have to make appropriate investments to acquire knowledge and experience or else outsource the task to a service provider.

To sum up, although SNPNs provide greater flexibility by granting full control of all network functions (such as QoS, UE subscriptions, and other configurations), they can be more challenging to manage. Conversely, while PNI-NPNs may be a simpler and more cost-effective solution, especially for multiple campus deployments, their scope for configuration is more limited.

Additional details of QoS operation and management in NPNs are discussed in section 4.6.

4 Operation of 5G QoS

This chapter describes how application developers can take advantage of the various 5G QoS functionalities introduced in chapter 3. It looks at the interfaces between the user equipment (UE) and the 5G network on the one hand and the interfaces for exposing 5G network capabilities on the other. It also presents several examples of IIoT applications that use the described functionality.

Here it is assumed that the reader is familiar with how the characteristic parameters of a communication service (see section C.2.2 of reference [8]) are translated into 5G QoS attributes (parameters and characteristics) such as packet-delay budget, resource type, packet-error ratio, and guaranteed flow bit rate (GFBR).

4.1 Operational Aspects of an IIoT Application That Requests a Specific QoS

As described in section 3.1, an IIoT application can define the QoS it needs for its connections by specifying 5QI and other (optional) QoS parameters such as the GFBR, the maximum flow bit rate (MFBR) and so on. In Section 3.1 it was explained that all of these parameters are specified in a QoS profile and that a QoS flow is the lowest-level granularity for requesting differentiated QoS treatment of traffic. Each QoS flow is established and managed within a PDU session. A UE can establish up to 15 PDU sessions, and a PDU session is able to support up to 63 QoS flows (see section 11.2.3.1b of [18] and section 9.11.4.12 of [17]).

When multiple IIoT applications connect via the same UE and all of them need to send or receive data packets over the same data network, there is no need to initiate any additional PDU sessions. A single PDU session between the UE and the data network is enough to support the traffic of all of the IIoT applications. This lets multiple applications share the same PDU session if their traffic passes through the same data network. However, the 5G system also makes it possible to separate the connections of different IIoT applications into distinct PDU sessions when required, for example if some of them use IP connectivity while others use Ethernet.

Each PDU session belongs to a single network slice. In case the UE needs concurrent connections to more than one slice, it's necessary to establish multiple PDU sessions (at least one per slice). A network slice is associated with a service-level agreement (SLA) that includes a set of service-level specifications (SLS). A network slice can be engineered to support a specific range of 5QIs and QoS KPIs (see section 3.4.26 in [12]). Section 3.3 goes into greater depth on configuring the QoS of slices.

4.1.1 Requesting a PDU Session with a Specific QoS

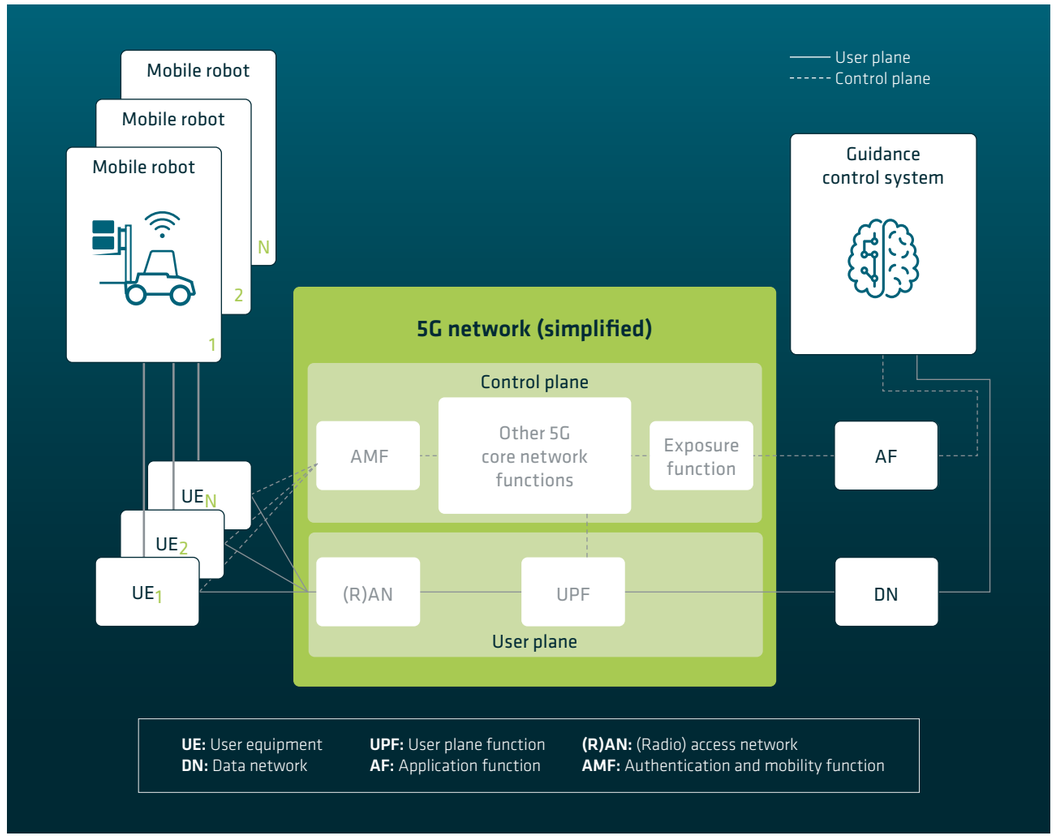
The 5QI values that can be used in a 5G system fall into two categories: standardized values (listed in section 5.7.4 of [3]) and preconfigured nonstandard values. The list of supported 5QI values (both standardized and nonstandard) should be included in the SLA and SLS. For example, say that a mobile robot requires a high-quality video stream that's sent from an embedded camera to a remote guidance control system.

The QoS for this stream can then be defined, for example, by specifying 83 as the 5QI value (see table 1 in chapter 3), plus additional parameters if the QoS flow needs a guaranteed bit rate.

It should be kept in mind that when the 5QI is set to 83, all other associated QoS characteristics are automatically chosen based on the values in table 1. In the case of a QoS flow with a guaranteed bit rate, the entity (the UE or AF, for example) requesting the QoS from the 5G system must include the QoS parameters for the guaranteed flow bit rate (GFBR) and maximum flow bit rate (MFBR) in the QoS profile for the QoS flow, separately for the UL and DL directions. In this example, the GFBR is set to 10 Mbit/s for the UL direction. The details of how to request a QoS flow with a specific QoS profile are described further below in this chapter.

In addition to the QoS flow described above, the mobile robot may also optionally use one or more additional flows with different QoS levels for other data, such as robot control and status information messages, and/or an additional flow for uplink audio sent to the remote guidance control system. As explained later in this chapter, a request for a connection with a particular QoS may contain the details of multiple QoS flows, each of which has a different QoS profile. Figure 9 shows, from a functional perspective, the 5G architecture for an application of this kind that is connected via the 5G system.

Figure 9: A mobile robot connected to a guidance control system with communication via a 5G system



Source: 5G-ACIA

In this example, it's assumed that there is one UE for each mobile robot. In the IIoT application, the guidance control system is typically connected to a data network via the 5G system's user plane function (UPF). For QoS operation, the guidance control system also links to an application function (AF) for sending QoS requests to the 3GPP system. The AF is connected to the 5G network via a 5G exposure function (for example the network exposure function (NEF)), which serves as an interface for exposing 5G system functionality to applications (typically only on the data network side). The AF can request the network to apply specific QoS settings to the connection. On the robot's side, the UE can also be used to send QoS requests to the network via the authentication and mobility function (AMF). The solid lines represent interfaces for sending and receiving application data through the 5G system (on the user plane), while the dashed lines represent interfaces used for network control messages (signaling).

In configurations of this kind, the application is distributed and can comprise multiple entities. There are two possibilities: either the application entity in the robot (connected to the UE) or the application entity in the guidance control system (connected to the AF) can send QoS requests to the 5G network. These two scenarios differ in terms of what can be controlled (i. e. defined, for instance, by the procedure and parameters).

This white paper describes how QoS works in 5G depending on which of these two application entities sends a QoS request to the 5G network. A QoS request is sent either by the application entity in the robot (connected to the UE) or by the application entity in the guidance control system (connected to the AF). The controllable aspects of QoS depend on which of these two sends a QoS request (the one connected to the UE or the one connected to the AF).

When the PDU session providing connectivity to the mobile robot is established, the 5G network applies policy charging and control (PCC) rules to set up a default QoS. This is preconfigured in the network and can depend on the UE subscription, the data network and network slice used, and other network configuration settings. The PCC rules can also define how the application is then able to alter the QoS. For example, although the application can request the network to apply a specific QoS profile, the operator or enterprise managing the 5G system network may wish to limit the QoS profiles (in terms of 5QIs and other QoS parameter values or ranges) that can be applied to the traffic of certain UEs and subscriptions. There can be multiple mechanisms for configuring the default PCC rules (for each UE, application, data network name (DNN), etc.) and the network slice used to establish PDU sessions. The default PCC rules can be configured in the 5G system by operation and maintenance (OAM) or AF via the 5G exposure function. PCC rules can be statically configured in the network or else dynamically created to support dynamic provision of QoS to PDU sessions. The method of application-detection-based QoS selection described in section 3.1 is an example of dynamically created PCC rules.

To configure the values defining a QoS (see table 1 for examples), the application can take one of the following three approaches:

1. The UE establishes a PDU session in which **PCC rules** are defined to obtain the **required QoS**.
2. The UE establishes a PDU session in which first **PCC rules** are defined to obtain a **default QoS** and then the **UE requests modifications** to the PDU session to obtain the **required QoS**.
3. The UE establishes a PDU session in which first **PCC rules** are defined to obtain a **default QoS** and then the **AF requests modifications** to the PDU session to obtain the **required QoS**.

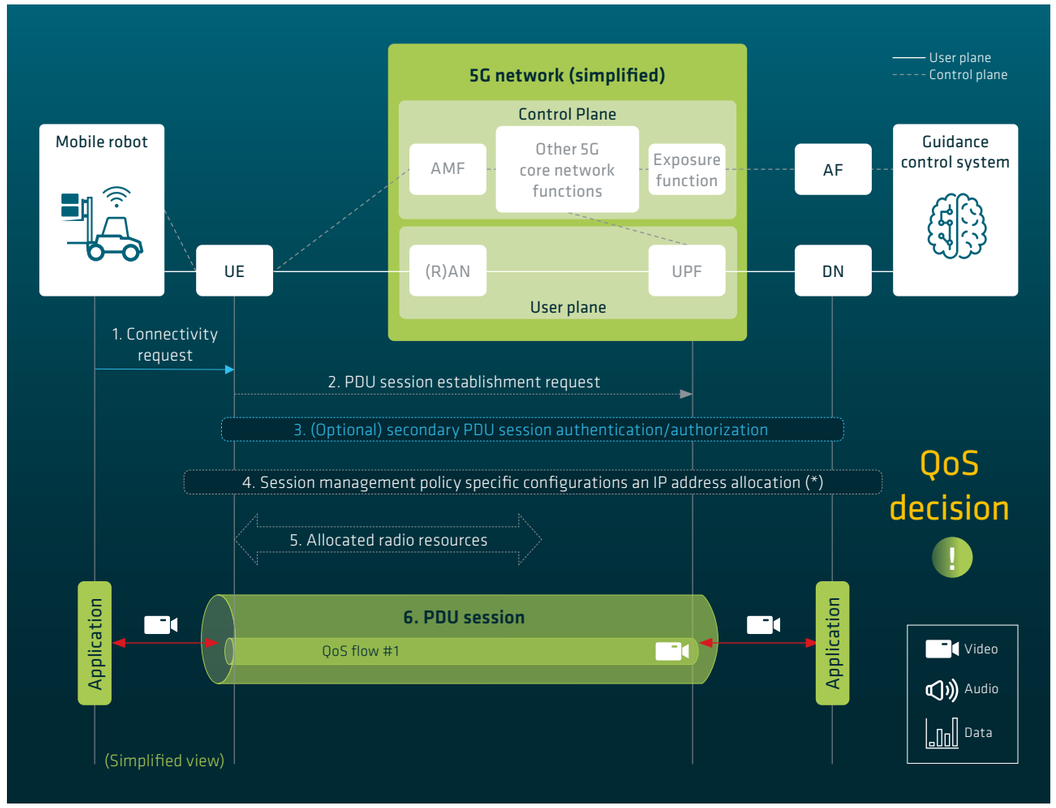
The first scenario calls for the PCC rules to be fully configured in the network with a simpler configuration in the UE application. These rules can be created based on a predefined set of packet data filters (described in section 3.1). Correct QoS profiles are then automatically assigned for all anticipated traffic patterns, which are identified by a set of packet data filters. It's necessary to know in advance which traffic patterns will be generated by the applications and what their QoS requirements are. This scenario is useful for applications with static requirements, in other words QoS requirements that don't change over time. Under conditions of this kind, the personnel managing the network can configure it so that the right QoS will be automatically assigned when the PDU session is established.

The last two scenarios can be applied whenever PCC rules are generated without knowing the application's QoS requirements in advance, or when there is a need for the network to quickly adopt a default configuration. In these scenarios, responsibility for requesting the required QoS is assigned to the UE or the AF. These scenarios are more useful in dynamic environments in which the QoS required by an application changes depending on its momentary context. It can be assumed that the application modules connected to the UE or AF are aware of their current context and therefore able to request an appropriate QoS. These three scenarios are described in greater detail in the following sections.

4.1.2 PDU Session Established with the Required QoS

In this scenario, a UE can establish a PDU session in which the required QoS is provided on the basis of default PCC rules. As shown in figure 10, in step 1 the UE detects the need for connectivity. This can happen after it registers with the network, for example because local applications have data to send or because the device operating system triggers a request in response to an internal event or configuration. In this context, it's important to note that the IIoT application running on the device doesn't directly request the 5G system to establish

Figure 10: A UE establishes a PDU session with a default QoS



Source: 5G-ACIA

a PDU session, because typically it's the terminal software (for example, the device's operating system) that decides to prompt the UE to send the request. The details of the interactions between the application and terminal software depend on the API that the latter makes available and are therefore beyond the scope of this white paper. Here it's assumed that in step 1, the application has some way to inform the UE – usually via the device's operating system – that it requires connectivity. In such a scenario, the UE can request the 5G network to establish a PDU session, as shown in step 2 of figure 10. In reality, establishing a new PDU session involves interaction among multiple network functions within the 5G network, and figure 10 therefore provides a simplified view of the overall procedure. If step 2 is successful (because the UE request is valid, the UE has a valid subscription, radio resources are available, local policies allow the PDU session, etc.), the network may decide in an optional third step to perform a secondary authentication. This is done on a data network authentication authorization and accounting (DN-AAA) server. For more information on this, please refer to section 5.6.6 of [3] and section 4.2.3, step 6 of [9].

In step 4, PCC rules are provided and applied to the PDU session. This includes defining the default QoS based on the current 5G network configuration. Depending on the PDU session type, an IP address can be assigned to the UE. Radio resources are then allocated to the PDU session in accordance with PCC rules as shown in the figure for step 5. If this is successful, the PDU session is established and the QoS flows are allocated according to default PCC rules. These flows can then be used by the applications for sending uplink and downlink packets. As explained in section 3.1, the 5G network maps the traffic in accordance with the packet filters. For example, when an application communicates with one or more servers in the data network in a PDU session, the traffic can be split into different QoS flows on the basis of source and destination port numbers, source and destination IP addresses, protocol identifiers, and other parameters.

Please note that the network also includes the details of the QoS for the PDU session in the message sent to the UE to confirm successful establishment of the PDU session (NAS message: "PDU SESSION ESTABLISHMENT ACCEPT"). See section 6.4.1.3 of [17] for additional details.

It's assumed that the default QoS configured for the PDU session will include the required QoS as indicated in table 1. The application can't use the procedure described above to request a QoS that differs from the configured default QoS. However, if the application wants to use a different QoS, it can use the described procedure to establish a default QoS and then request modification of the PDU session's QoS via the UE or AF. This scenario is described in the following two sections.

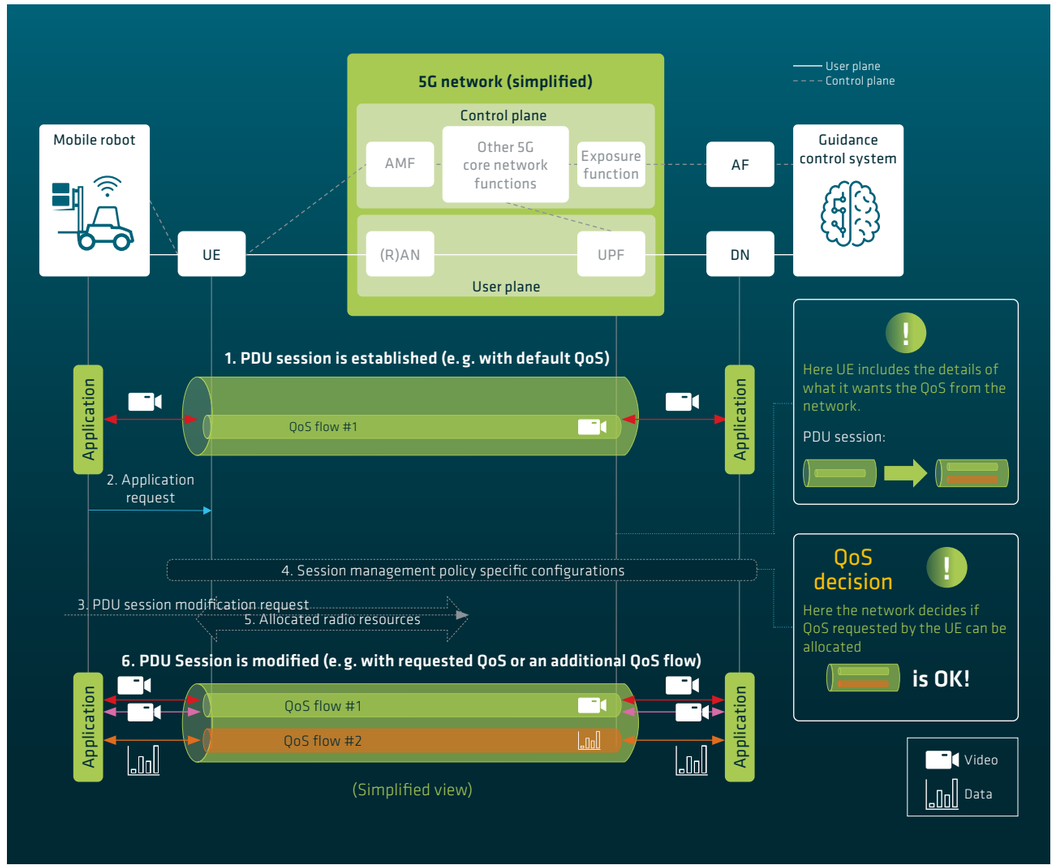
4.1.3 UE-Initiated QoS Modification

If the default QoS doesn't meet the UE's needs, the latter can request that it be changed. To accomplish this, the UE initiates a PDU session to modify, establish, or release one or more QoS flows (within the supported limits).

A UE may request the network to modify a previously established PDU session with a default QoS (or any previous QoS) by assigning a different QoS to it. In the example shown in figure 11, the first step is to establish a PDU session with only one QoS flow, namely the default QoS configured in the network. The UE then submits a request to modify the PDU session by adding a second QoS flow, for example for exchanging data between the mobile robot and guidance control system. This second QoS flow is added because the QoS requirements for exchanging data differ from those for video uploads. For this purpose, the example assumes that the UE receives specific input from the application, usually via the device's operating system as shown in step 2.

This input in turn prompts the UE to send a PDU session modification request message to the control plane interface of the 5G network as shown in step 3. This interface terminates in the application and mobility function (AMF), although the QoS-related part of the message is actually piggybacked onto a 5G network function – specifically, the session management function (SMF) – for serving requests of this kind. This network function is responsible for dealing with PDU session management requests (while applying the PCC rules) and therefore controls the QoS. The message contains the details of the second QoS flow to be added. The

Figure 11: A UE requests the modification of a previously established PDU session with a default QoS in order to obtain the required QoS



Source: 5G-ACIA

information that this request must contain is described in section 6.4.2 of [17].

In this example, it's assumed that the message in step 3 contains a request to create a new QoS flow, the desired 5QI, and the values of the other QoS parameters. The request doesn't need to contain the values of QoS characteristics (such as the packet delay budget, packet error rate, etc.) because these follow from the specified 5QI value. When the network (SMF) receives a PDU session modification request from the UE, it checks whether the requested changes are compatible with the current network status, available resources, and configurations. In particular, it checks whether the requested new QoS can be assigned to that particular PDU session (for example by consulting the policy assigned to it), the details of the subscription associated with the UE, the SLA associated with the network slice, and possibly also other network configurations.

All these actions are shown in step 4. In the event of a positive outcome, the relevant network resources are allocated and the PDU session is modified as requested by the UE, as shown in step 5. The network then executes a complex procedure called "network requested PDU session modification", in which the PDU session is modified as specified by the UE while adding the new QoS flow. The UE receives a "PDU SESSION MODIFICATION COMMAND" message from the network containing the details of the new QoS that is applied to the PDU session. This message, containing an authorized QoS rule, is sent after the SMF has authorized the request from the UE.

Each authorized QoS rule comprises the following set of parameters:

a) Whether or not the QoS rule is the default QoS
b) A QoS rule identifier (QRI)
c) A QoS flow identifier (QFI)
d) Optionally, a set of packet filters
e) A precedence value, which is needed to define a hierarchy of QoS rules when more than one applies to the same traffic pattern. For example, some QoS rules can contain a "match-all" packet filter (meaning that they match all of the traffic flowing between the UE and data network). In such a case, the QoS rule defers to other QoS rules that apply to a more restricted traffic pattern (e. g. traffic directed to a specific IP address).

It can also happen that the SMF is unable to apply the QoS requested by the UE. The reasons for this can include inadequate network resources, an invalid 5QI value, or issues with the request itself. In such a case, the PDU session modification request is rejected and a "PDU SESSION MODIFICATION REJECT" message is sent back to the UE. Reference [17] lists the possible causes of a rejection, some of which are given in the following table.

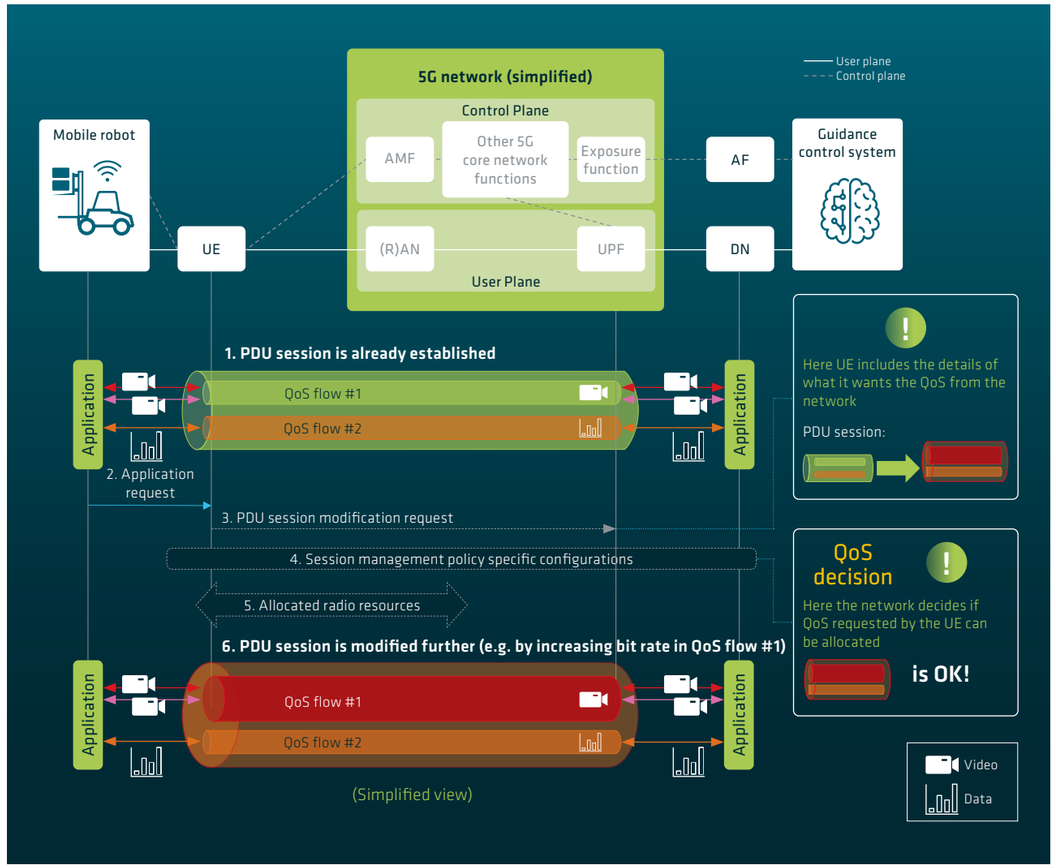
Table 2: Example causes of errors when attempting to modify a PDU session (from reference [17])

Cause number	Cause description
#26	Insufficient resources
#29	User authentication or authorization failed
#31	Request rejected for unspecified reason
#59	Unsupported 5QI value
#67	Insufficient resources for specific slice and DNN

As shown in figure 12, a UE can request the network to additionally modify a PDU session for which the QoS has already been changed. In this example, the request is made to modify the PDU session (which already comprises two QoS flows) by adding more bandwidth for the first QoS flow, which is used for video streaming to the guidance control system. This can be done, for example, by increasing the value of GFBR. For this purpose, the UE can send a PDU session modification request containing the parameters of the required QoS to the network via the control plane interface.

More information on the PDU session modification procedure, including a detailed description of all of the steps, is available in section 4.3.3 of reference [9]. The details of the information exchanged during this procedure can be found in sections 6.3.2.2, 6.4.2.4.1, 9.11.4.12, and 9.11.4.13 of reference [17].

Figure 12: The UE requests modification of a previously established PDU session with the default QoS in order to obtain the needed QoS



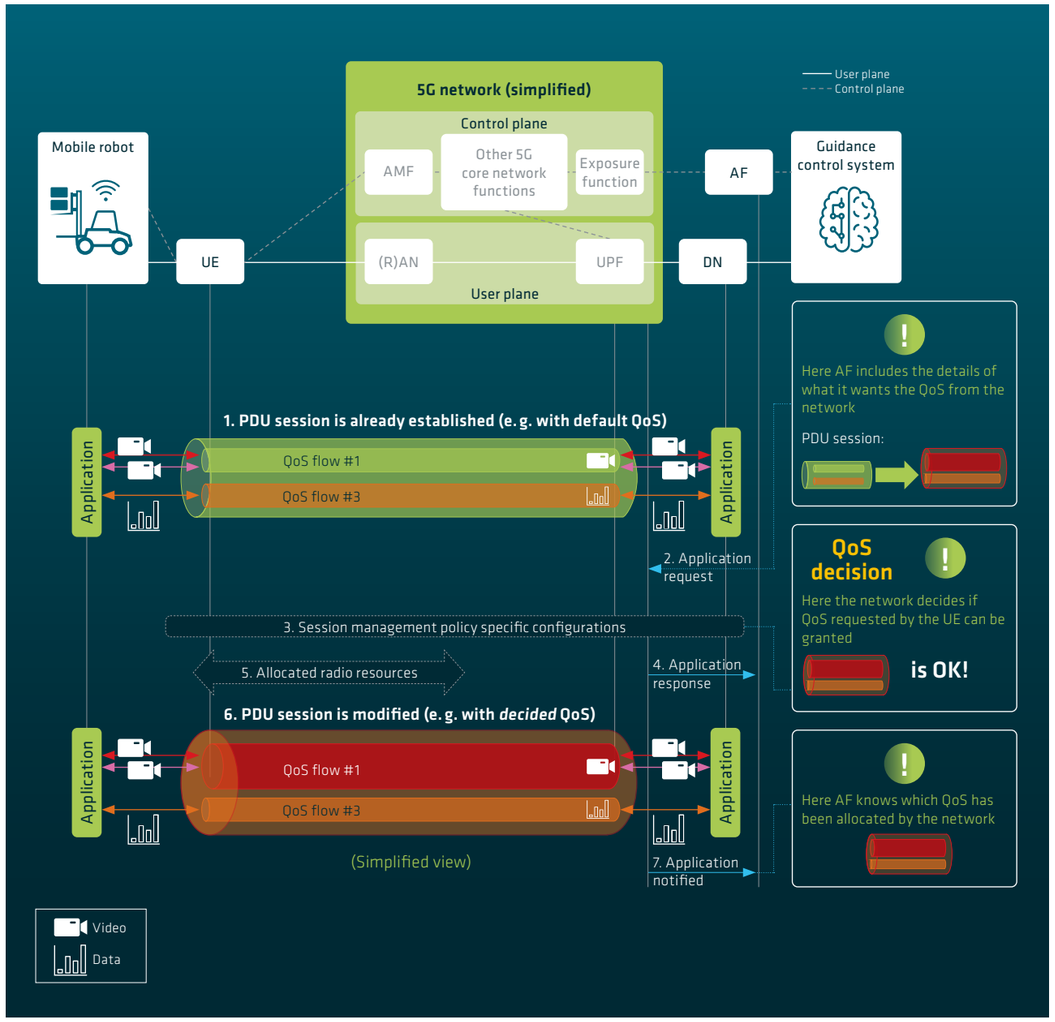
Source: 5G-ACIA

4.1.4 AF-Initiated Modification of QoS

Alternatively, the AF, which is connected to the guidance control system as shown in the example, may request modification of a PDU session's QoS. Since there can be multiple mobile robots, each of which is potentially connected via its own UE, the guidance control system application can use this procedure to request the same QoS for every robot's UE, or else to selectively apply a different QoS to each one. This scenario applies the "AF session with required QoS update" procedure. More information on this procedure is also available in section 4.15.6.6a of reference [9].

When the application function (AF) connected to the guidance control system submits a request to modify the QoS of a previously established PDU session, it's sent to the 5G network's exposure function as shown in step 2 in figure 13 below. The AF identifies the targeted PDU session by the UE's IP address (in the case of IP type PDU sessions) or the MAC address associated with the PDU session (for Ethernet-type

Figure 13: The AF requests modification of the PDU session previously established with a default QoS in order to obtain the required QoS



Source: 5G-ACIA

PDU sessions). From the perspective of the NEF, a request of this kind is called a "Nnef_AFsessionWithQoS Update request" and contains, among other things, an informational element called "QoS reference" that the application can use to specify the QoS. The 5G network uses this information to initiate a network-requested PDU session modification procedure for modifying the QoS as requested. In the event of a positive outcome, this procedure modifies the PDU session as requested by the AF. Figure 13 illustrates this procedure.

The "QoS reference" is a predefined set of QoS information that must be specified in the SLA. It can refer to an internally configured QoS reference identifier of the specific operator network, or else it can be an external QoS reference identifier that the NEF can map to an internal reference identifier. The SLA must define all possible QoS references, as well as their charging rates if applicable.

If the outcome is positive, the AF is notified by an Nnef_AFsessionWithQoS_Update message from the NEF as shown in step 4 of figure 13. This message contains a result parameter indicating whether or not the request has been granted and authorized and therefore whether the network has been able to initiate the PDU session modification procedure. The response message itself does not indicate whether the PDU session has been modified as requested.

Once the transmission resources corresponding to the QoS update have actually been modified (or not, if there are problems), the network sends another Nnef_AFsessionWithQoS_Notify message to the AF as shown in step 7 of figure 13.

The network may later modify the PDU session's QoS again in response to other events (such as inadequate resources, a policy change, a change to the SLA etc.). Also in that case, the AF can receive a Nnef_AFsessionWithQoS_Notify from the NEF detailing the changes.

Please refer to these 3GPP documents for additional details:

(1) [9], section 4.15.6.6a
(2) [10], section 6.1.3.22
(3) [11], section 4.4.13
(4) [19], section 4.4.9

4.1.5 QoS for Multicast

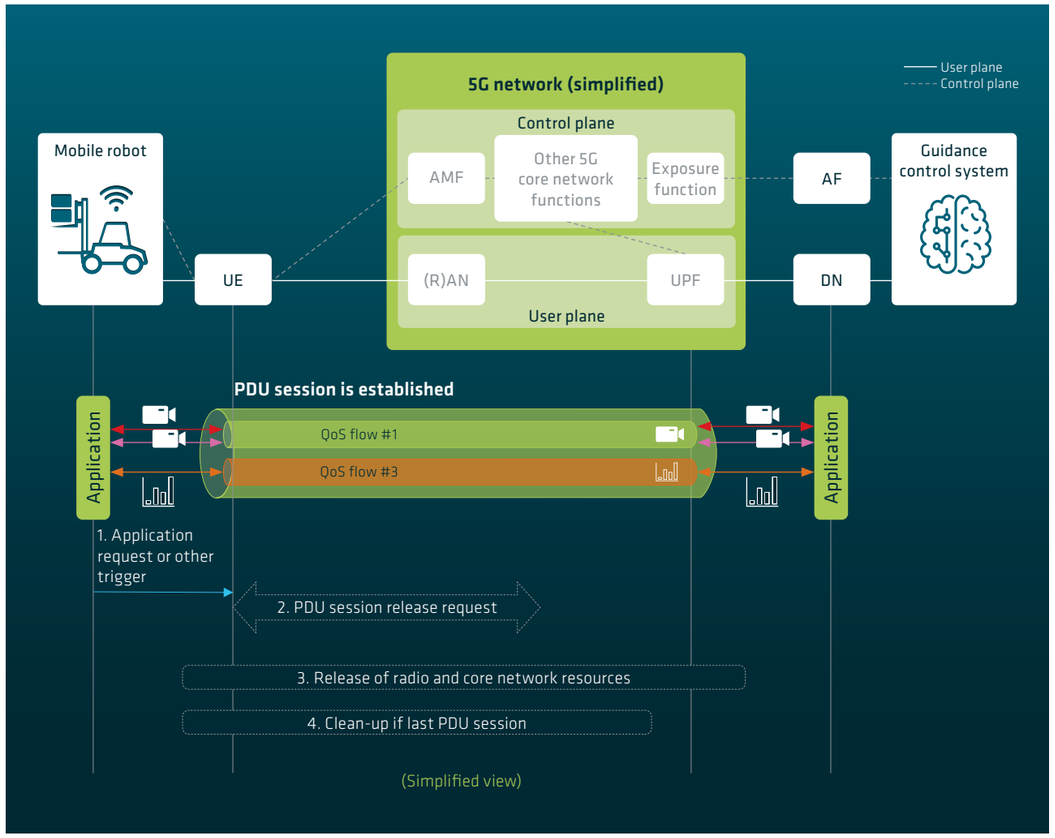
Future 5G releases are expected to introduce architectural enhancements to support QoS for multicast and broadcast services. The introduction of specific QoS handling is also anticipated. See reference [28] for more detailed information.

4.1.6 PDU Session Release

When a PDU session is released, so are all of the resources associated with it, including IP addresses, user plane resources, and access layer resources in the radio network. A release can be triggered by the UE or network. Network-initiated release of the PDU session is beyond the scope of this white paper. The procedure for PDU sessions released by a UE is depicted in figure 14.

Here it's assumed that the UE receives a specific trigger that prompts it to send the PDU session release request to the network. Examples include (1) determination by the device's terminal software that there is no need for connectivity and (2) explicit notification of the terminal software by the application that the connection isn't needed anymore. The trigger is shown in the figure below as step 1. After receiving a trigger, the UE sends a message to the network as indicated in step 2 (PDU session release request). After receiving the request, the 5G network initiates release of network resources in the core network and radio network (step 3). If the PDU session concerned is the last one in a given data network and network slice, clean-up operations may also be carried out. These can involve, for example, terminating any connections that participating core network functions have created to the repository containing the selected UE's subscription information.

Figure 14: A UE requests release of the PDU session along with the associated QoS



Source: 5G-ACIA

4.2 Operating QoS-Adaptive Applications

As explained in section 3.2 of this white paper, 5G QoS introduces support for adaptive applications that are compatible with different sets of QoS requirements. For example, a remotely controlled mobile robot could transmit a real-time video stream to a guidance control system. (See use case number four in [8], section A.2.2.3-1). The 5G network can be designed to provide ubiquitous support for high-quality video streaming, which is required for remotely controlled mobile robots operating faster than a certain speed. However, robots can continue operating at reduced speed despite interruptions in high-quality video streaming caused by temporary QoS degradation, provided that the QoS delivered by the network meets a set of alternative requirements. These can be chosen by the application, and may be supported by the network during rare episodes of QoS degradation. In the example, it's assumed that a mobile robot's speed can be adjusted between one and four m/s depending on the quality of the video stream. Specifically, it can operate in three different modes depending on the video stream's quality (high, medium, or low), with a different top speed in each case.

Table 3 below lists the 5G QoS attributes and top speeds associated with different operating modes. These and the associated guaranteed flow bit rates (GFBR) should only be taken as examples, however, because reference [8] doesn't provide any values of this kind. In addition, only the GFBR differs in the profiles shown, although in general any or all of the attributes can vary (such as the 5QI, packet delay budget, packet error rate, guaranteed flow bit rate and so on).

Table 3: Example top speeds in an adaptive application involving mobile robots with video streaming via a guidance control system that supports three different sets of QoS requirements.

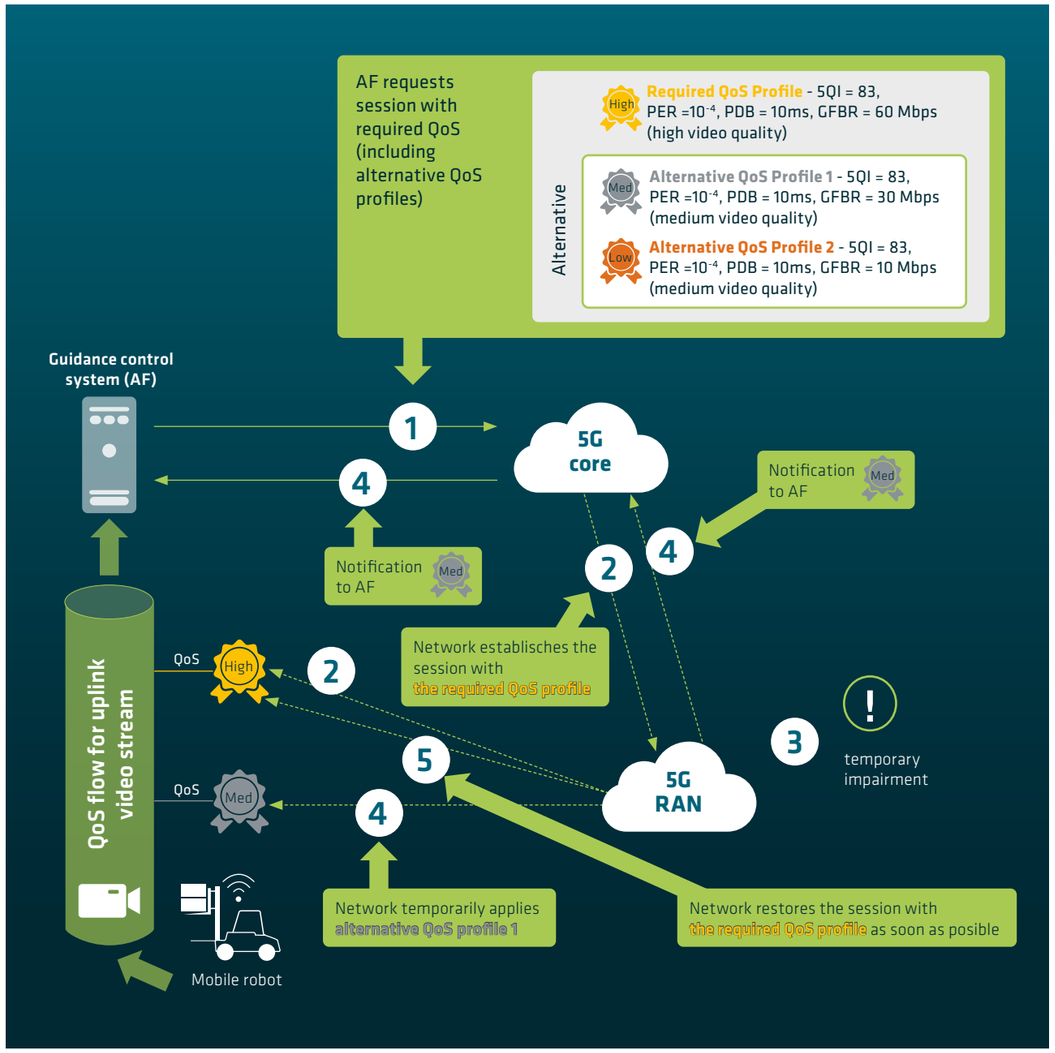
Order of preference	Operating mode	Top speed (meters per second)	5QI	PER	PDB	GFBR	Supported video resolution(*)
1st	High quality	4 m/s	83	10^{-4}	10 ms	60 Mbit/s	e. g. H.264, 2160p (4K), HDR, 24-30 fps
2nd	Medium quality	2 m/s	83	10^{-4}	10 ms	30 Mbit/s	e. g. H.264,1440p (2K), HDR, 48-60 fps
3rd	Low quality	1 m/s	83	10^{-4}	10 ms	10 Mbit/s	e. g. H.264,1080p, HDR, 24-30 fps

(*) The supported video quality is a key factor and depends on the codec (for example, H.264) and other implementation details, see reference [39].

During periods when the QoS temporarily drops, the network may not be able to provide what is needed for "high-quality" operation of all robots in a given service area, but may still be able to provide medium or low quality for some of them, thus allowing them continue operating at a reduced speed.

In the example illustrated below, it's assumed that the mobile robot is linked to the 5G system via a UE, while the guidance control system is connected to an AF that interacts with the 5G network by way of the 5G exposure function (not shown for simplicity's sake). Other configurations are also possible. The application running on the guidance control system (which, from a 3GPP perspective, is integrated in the control interface via the AF) requests the 5G network, via the 5G exposure function, to provide a particular QoS for the mobile robot's UE. The requested QoS can have either a single QoS profile or – in the case of adaptive applications – two or more prioritized alternative QoS profiles. Note that the UE isn't capable of directly submitting a list of requested QoS profiles to the 5G network.

Figure 15: Operational steps for alternative QoS profiles



Source: 5G-ACIA

In the case of a QoS flow used to stream video in real time to the guidance control system, the listed QoS profiles can be in the sequence shown in table 3 (high – medium – low). If the 5G network's condition prevents it from guaranteeing adequate QoS for high-quality video streaming, it can – instead of simply delivering the best possible QoS or dropping traffic for the affected QoS flow – temporarily choose and apply an alternative QoS profile from a list provided by the application to meet less demanding requirements. The network makes this selection based on current conditions and the specified order of preference.

The network applies the most suitable profile available while reverting to a QoS with a higher preference whenever possible. If network conditions degrade even further, the network attempts to deliver one of the other preferred modes of operation selected by the application. For example, if medium quality can no longer be supported, it tries to support low quality.

The AF and UE can request the network to notify them of any changes in the QoS, the supported set of QoS attributes, and the current QoS flow and profile.

The application can follow these steps (illustrated in figure 15) for applying an alternative QoS profile:

(i) Step 1: The guidance control system's AF requests a specific high-quality QoS profile from the 5G network via the 5G exposure function (e. g. the NEF) for one of the mobile robots in the service area. The AF provides "QoS reference" parameters as described in section 4.1.4. The 5G network then uses this information to determine the QoS profile for a specific QoS flow that the mobile robot will use for video streaming to the guidance control system. The AF also specifies – in a defined order of preference – various alternative QoS references for the same QoS flow. In this example, the AF has specified two alternative QoS references that the 5G network uses to determine the corresponding medium- and low-quality QoS profiles. Table 4 shows the details of these QoS profiles.

(ii) **Step 2:** The 5G core and RAN coordinate their actions to apply the selected QoS profile to the QoS flow in question while keeping the alternative QoS profiles in reserve in the event of temporary QoS degradation.

(iii) **Step 3:** An impairment occurs that prevents the 5G network from providing high QoS to the selected video stream. It can be related to any of the QoS KPIs in the QoS profile, thus making it impossible to achieve the guaranteed flow bit rate (GFBR) that is required for the high-quality QoS profile. Other QoS flows may still operate normally.

(iv) **Step 4:** The network selects the best alternative QoS profile for the QoS flow in question (in this case, medium), based on the available resources and the application's selected order of preference. At the same time, the guidance control system connected to the AF and the mobile robots affected by the change in the QoS profile are notified of the new applied QoS.

(v) **Step 5**: The conditions responsible for the impairment no longer exist, and the network for the mobile robot profile with the highest QoS is therefore reselected. The 5G system notifies both the AF and the UE of this.

Alternative QoS profiles in 5G enable adaptive applications (like the one described in this example) to communicate alternative QoS requirements for use in case problems temporarily prevent support for a set of higher-quality QoS prerequisites. This mechanism makes it possible to define a controlled way of downgrading QoS, with QoS levels changing as a result of applying predefined QoS profiles instead of by network decisions taken without knowledge of the application context.

4.2.1 Notifying the UE of Changes to QoS

The notification sent to the UE in steps 4 and 5 of figure 15 is a message called "PDU SESSION MODIFICATION COMMAND". In step 4 of the procedure described in section 4.2, this message is used to notify the UE that the network no longer supports the QoS profile that was most recently applied to the QoS flow, and has therefore chosen an alternative from the set of QoS profiles that the application previously requested. In step 5, the same message is used to notify the UE that the original QoS profile has been reapplied to the QoS flow.

In addition to other information, this message contains packet data filters and authorized QoS flow descriptions for each QoS flow of the PDU session:

- The packet data filters are used to describe how the data packets are mapped to QoS flows.
- Each QoS flow description contains all of the relevant QoS parameters (see section 3.1 for more information on these).

This notification is sent to the UE not just when an alternative QoS profile is selected for a QoS flow, but every time that a PDU session is modified by the network, for example in response to specific decisions on resource allocation. The UE can tell that a new QoS profile has been selected for a QoS flow by comparing it with previously stored information. This is based on the "notification control" functionality described in section 5.7.2.4 of reference [3].

The AF can also disable notification of the UE when there are changes to the QoS, namely by using the mechanism discussed in section 5.1.4 and setting the "disUeNotif" attribute as described in section 4.4.9 of [19].

For more details on this notification's format and content, see section 8.3.9 of [17].

4.2.2 Notifying the AF of Changes to QoS

The AF can be notified of changes via the 5G exposure function (for example, the NEF) by two different events:

- The "QOS_GUARANTEED" event, which tells the application that the requested QoS is available. It means that the preferred QoS profile requested by the application is currently supported for the QoS flow in question.
- The "QOS_NOT_GUARANTEED" event in which the currently applied QoS reference (if this has been received) optionally indicates the currently supported alternative QoS profile for the QoS flow. This means that the network is momentarily unable to support the requested QoS profile and has therefore selected an alternative QoS instead (if the network includes this information).

The 5G exposure function (e.g. the NEF) notifies the AF by sending a Nnef_AFsessionWithQoS_Notify message. The AF receives it every time it initiates AF an Nnef_AFsessionWithQoS create or update request operation or is used to open a new session or modify an existing one with a specific QoS. To stop receiving these notifications, the AF can send an Nnef_AFsessionWithQoS_Revoke request to the NEF. This is described in section 4.15.6.6a of [9].

Note that, depending on the operator configuration, the QoS reference identifiers received from the AF can be the same as or different from the QoS reference identifiers known to the UE. The 5G network exposure function can map the QoS reference identifier received by the AF onto a relevant QoS identifier known to the UE if configured to do so. The details of this mapping operation and how to configure it are beyond the scope of this white paper, however.

For additional details on notifying the AF of changes to the QoS, please refer to section 4.4.9 of [19], section 5.2.2.2.2.1 (steps 7 and 8) of [26], and section 4.2.6 of [27].

It should also be noted that the network notifies the AF of a change in QoS when it happens and not before. It's important to keep this in mind to avoid confusing such a notification with a potential QoS change notification (described in section 6.9 of [34]), which is used to communicate a possible change of QoS in a QoS flow at a specified future time. Both can be sent to the AF for the same QoS change event: the first when predicting a QoS change, and the second later when the QoS actually changes. The network doesn't currently support any mechanisms for correlating a potential QoS change notification with the notification sent when a QoS change actually occurs, even if both notifications are about the same QoS flow and change in QoS.

4.3 Using Network Slicing to Influence QoS

This section addresses the following topics:

- The relationship between application-specific QoS requirements in the IIoT and selection of a specific network slice
- How an application can interact with the 5G network management system when a network slice can't deliver the requested performance

As described in section 3.3 and chapter 8, network slices are selected when a UE first registers with the network. Selections are based on the 3GPP deployment configuration, user subscription, and user location. The procedure for selecting a network slice is described in greater detail in chapter 8. Each PDU session is associated with a specific network slice and data network, but a network slice can support more than one concurrent PDU session for the same UE and provide connectivity to multiple data networks.

Since a UE must register first, it can only establish PDU sessions associated with the permitted network slices that have already been assigned to it. When the UE requests the establishment of a PDU session, it includes the identifier of the network slice it wants to use for that PDU session (this is explained in section 4.1.2). The UE chooses the network slice for newly established PDU sessions based on the network slice selection policy (NSSP) included in the UE route selection policy (URSP). The 5G network provides these policies to the UE in accordance with the local configuration as defined in section 6.1.2.2.1 of reference [10]. For additional details, see section 8.2 below.

By way of example, consider the scenario of a 5G network that needs to support three different applications with the following characteristics:

- A time-sensitive application based on 5G TSN with the corresponding QoS requirements
- A second application that only requires a best-effort QoS
- A third application that requires stringent QoS attributes (for example, of the packet delay budget and guaranteed flow bit rate)

This scenario can be supported by either of the following deployment configurations:

- **Deployment configuration #1**: The 5G system is deployed in a single network slice with certain elements (UPFs, gNB, and UEs) configured as a TSN bridge while other elements don't support TSN but do support best-effort QoS and strict associated requirements. The UE is also configured to establish three different PDU sessions: one for TSN traffic, one for best effort, and one for stringent QoS attributes. All of the PDU sessions are established in the same slice.
  Note 1: 3GPP specifications allow a single UE to support both TSN and non-TSN traffic at the same time. The UPF can also be configured to act as a 5G TSN bridge for some UEs and traffic and as a non-TSN bridge for other UEs and traffic.
  Note 2: It isn't necessary to establish three separate PDU sessions unless all three applications require connectivity to different DNNs. As an alternative scenario, a single PDU session can concurrently support different QoS profiles in different QoS flows, for example the best-effort and stringent QoS attributes.
- **Deployment configuration #2**: Two different network slices are deployed in the 5G system, with network slice #1 devoted to the TSN application and network slice #2 devoted to other applications. In addition, the UE is configured to establish three different PDU sessions, one for TSN traffic associated with network slice #1 and two others associated with network slice #2a: one that supports best-effort QoS and another that supports the stringent QoS KPI.
  Note 3: Alternatively, network slice #1 can support the application of both TSN and stringent QoS attributes.

The criteria for choosing one or the other of these deployments aren't limited to the QoS requirements of specific applications. Various other aspects can also be applied for designing network slices, including topological properties, network separation and segregation (for example, one net-

work slice for TSN on the shop floor and other slices for the rest of a factory), security (for example, to enable secondary authentication of one network slice but not of any others), resource allocation (each network slice can have its own dedicated resources), requirements to restrict the use of certain network slices to particular customers (for example, in a PNI-NPN scenario), and so on. All of these design criteria are outside the scope of this white paper.

In deployment configuration #1, different application traffic and PDU sessions can be established and mapped for individual UEs on the basis of a URSP policy. Such a policy can prescribe mapping the TSN application's traffic to PDU session #1, Internet traffic to PDU session #2, and so on. When the 5G system then detects TSN traffic, PDU session #1 is established while applying the QoS configured for TSN traffic. Alternatively, a local configuration in the UE can achieve the same traffic mapping. All PDU sessions use the same network slice.

In the case of deployment configuration #2, the following happens upon registration:

- Network slice #1 is included in the list of allowed network slices that is provided to the UEs supporting the TSN application.
- Network slice #2 is included in the list of allowed network slices that is provided to the UEs supporting the other applications.
- Both network slice #1 and network slice #2 are included in the list of allowed network slices provided to the UEs that support both kinds of applications.

In deployment configuration #1, a UE can either map the traffic of different applications based on a local configuration or receive an appropriate policy from the network for mapping applications, PDU sessions, and network slices.

The key point is that – depending on the current 3GPP specifications – the associations between network slices, QoS, and application traffic are the result of network deployments and configurations performed by the network operator and not of choosing certain QoS requirements. In fact, an application running on the UE can't directly ask the 5G network to serve it with a slice that supports the specific QoS attributes it requires (like a network slice that supports a throughput of 200 Mbit/s and an end-to-end latency of one millisecond).

Instead, the UE on which an application is running can only ask the 5G network to connect it to a network slice that is referenced by a network slice identifier, within the bounds of how the network operator has deployed and configured the network. A network slice identifier is a number that does not explicitly refer to the QoS that the network slice supports. The association between a network slice identifier and the QoS capabilities it supports is based on the network configuration and an implicit association between the network slice deployed in the 5G network and its network slice identifier.

On the other hand, if an application needs support for specific functionalities on the network, one way to provide them is to create a specific network slice in which all network elements are configured to support those functionalities and the required QoS. The network slice can be created by a human actor and/or via the API exposed by management system, as described in reference [1]. A detailed description of this process for creating and managing the lifecycle of a network slice is beyond the scope of this white paper.

The 5G system also supports many other scenarios and options that aren't addressed here.

Summing up, the 5G system has been designed with the inherent assumption that an application running on a 5G device doesn't need to know anything about 5G network information managed at the UE level. It has also been taken as a given that the QoS levels needed to meet specific application requirements are managed as QoS flows in PDU sessions, which are in turn established on a suitable network slice based on correct configuration of the UE device, the user subscription, and other network configuration values. The assumption is that complex aspects will be dealt with on the network side.

4.3.1 Example Use Case: Automatic Guided Vehicles (AGVs)

Description
This example illustrates the selection and use of network slices. An AGV operates on the factory floor while navigating with the aid of time-sensitive services provided via TSN. Camera-based navigation with a high-speed uplink data rate and low latency is essential for safe operation. The assumption is that TSN services aren't used when the AGV isn't traveling.

Assumptions
The AGV's UE has credentials. It is also assumed that the 5G network is configured with two network slices, one of which provides TSN communication services while the other provides non-TSN-based communication services. The required network slice identifiers (also known as S-NSSAIs as explained in chapter 8) are included in the robots' subscription and available where they connect.

Note: the 5G network can also be configured with a single network slice that provides both types of services. In such a case, there is no need for network slicing functionality.

Slice Selection and QoS
The 5G system supports two possible mechanisms for selecting suitable network slices.

Method 1:
1. The AGV is preconfigured with the identifier(s) of the required network slice or slices.
2. The AGV performs a registration procedure for connecting to the network. To get its credentials verified, it sends a request to the 5G system indicating the identifier(s) of the TSN network slice or slices that will provide the TSN communication services. The AGV can either be preconfigured with this information or have registered previously with the 5G network .
3. The 5G network checks whether the AGV is allowed to access the requested network slice or slices, based on the subscription information and available network slices at the location from which it is registering. The 5G network then sends the identifiers of the allowed network slice or slices from step 2 to the AGV.
4. Registration is completed, and the AGV is then served by the corresponding TSN network slice or slices.

Method 2:
1. The AGV isn't preconfigured or else is configured but doesn't request the additional network slice identifier(s) required for the TSN communication services.
2. The AGV registers like in step 2 of method 1, but without sending the 5G system the identifier(s) of the requested TSN network slice or slices.
3. As in method 1.
4. As in method 1.

Follow-Up
After successfully registering, the AGV initiates a PDU session for TSN communication services from the selected network slice as described in section 4.1.1.

4.4 QoS Monitoring

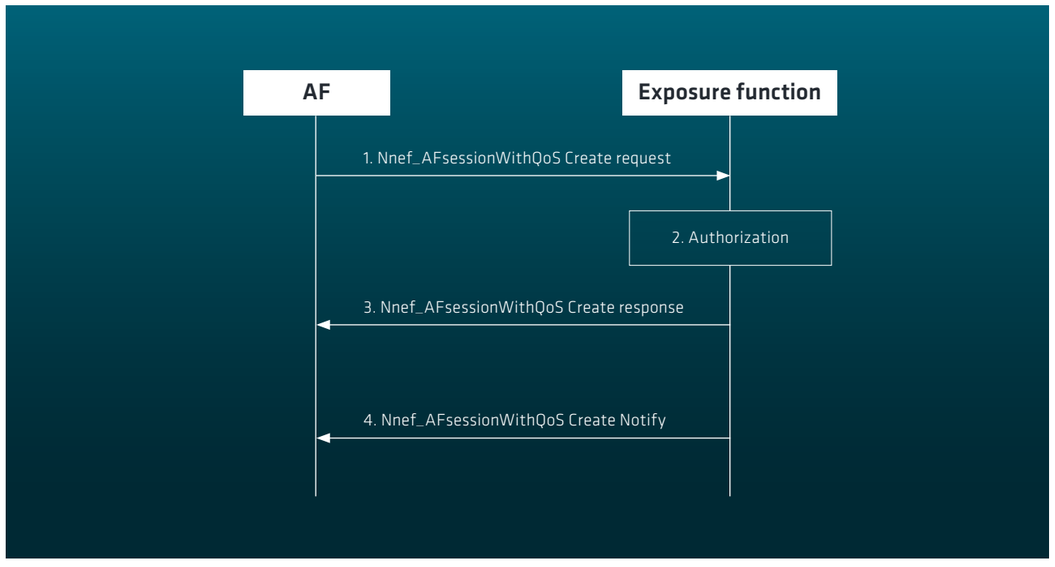
This section explains the procedure for an application function to request QoS monitoring services from the 5G system, which then provides a monitoring report to the application. For an in-depth description, see the related section 4.15.6.6 of [9]. As illustrated in 4.15.6.6 of [9], an AF is allowed to set up an AF session with the required QoS for the service data flows involved. This service is also used to support subscription and notification of QoS monitoring for URLLC as described in section 3.4 (see section 5.33.3.2 of reference [3] for details).

As shown in figure 16, the procedure for setting up an AF session with the required QoS and QoS monitoring functions consists of the following steps:

- The AF sends a Nnef_AFsessionWithQoS_Create request message to the 5G exposure function (e. g. NEF) for establishing an AF session. The 5G exposure function than assigns a transaction reference ID to the Nnef_AFsessionWithQoS_Create request (see [11]).

For QoS monitoring purposes, it's also necessary to include the QoS parameter(s) that must be measured, the reporting frequency, and the reporting target in the Nnef_AFsession-WithQoS_Create request message (for more details, see section 6.1.3.21 of [10]). As described in table 4, the QosMonitoringInformation data type defines the QoS monitoring and reporting configuration parameters (see section 5.14.2.1.6 of [11] for details).

Figure 16: Setting up an AF session with the required QoS procedure (simplified from figure 4.15.6.6-1 in reference [9])



Source: 5G-ACIA

Table 4: Definition of the QosMonitoringInformation data type (texts adapted from table 5.14.2.1.6-1 in [11])

Attribute name	Data type	Range	Description
reqQosMonParams	array (RequestedQos-MonitoringParameter)	1 to N	Specifies monitoring of the UL/DL packet delay and/or round-trip packet delay between the UE and UPF.
repFreqs	array (ReportingFrequency)	1 to N	Specifies the reporting frequency, e. g. when triggered by an event, periodic, when the PDU session is released, and/or any combination of these.
repThreshDl	UInteger	0 or 1	An unsigned integer identifying a threshold in units of milliseconds for DL packet delay. This parameter is used when the AF requests to receive a report every time the downlink delay exceeds the DL delay threshold.
repThreshUl	UInteger	0 or 1	An unsigned integer identifying a threshold in units of milliseconds for UL packet delay. This parameter is used when the AF requests to receive a report every time the UL delay exceeds the UL delay threshold.
repThreshRp	UInteger	0 or 1	An unsigned integer identifying a threshold in units of milliseconds for round trip packet delay. This parameter is used when the AF requests to receive a report whenever the round-trip delay exceeds the round-trip delay threshold.
waitTime	DurationSec	0 to 1	Specifies the minimum waiting time between successive reports in seconds. Only applicable when the "repFreqs" attribute above includes "EVENT_TRIGGERED".
repPeriod	DurationSec	0 to 1	Specifies the time interval between successive reports in seconds. This parameter is used when the AF requests periodic delay reports.

- The 5G exposure function (e. g. NEF) authorizes the AF request. If authorization isn't given, the 5G exposure function replies to the AF that authorization has failed in step 3.
- The 5G exposure function sends a Nnef_AFsession-WithQoS_Create response message (Transaction Reference ID, Result) to the AF. The result indicates whether or not the request has been granted.
- The 5G exposure function sends a Nnef_AFsession-WithQoS_Notify message with the event reported by the 5G system to the AF (see section 5.14.2.1.4 of [11]). Specifically, the 5G exposure function can report the QoS flow level event(s) to the AF.

Report types are defined in section 6.1.3.18 of reference [10]. Event reports on QoS monitoring for URLLC include the packet delay for UL, DL, or round trip for a single UP path or two UP paths in the case of redundant transmission (see sections 4.4 and 5.33.3.2 of [3]). As shown in table 5, the QosMonitoringReport data type defines the QoS monitoring report parameters (see section 5.14.2.1.8 of [11]).

Table 5: QosMonitoringReport types (based on table 5.14.2.1.8-1 in reference [11])

Attribute name	Data type	Range of reported delay	Description
ulDelays	array (UInteger)	0 to N	Uplink packet delay in milliseconds*
dlDelays	array (UInteger)	0 to N	Downlink packet delay in units of milliseconds*
rtDelays	array (UInteger)	0 to N	Round trip delay in units of milliseconds*

* This specification release limits the maximum number of elements in an array to 2.

4.5 Using TSN Features

Figure 17 shows an example TSN network based on the IEEE 802.1 Qcc fully centralized configuration model (see [16]). The centralized user configuration (CUC) captures applications' requirements in the network and forwards them to the CNC. The CNC either already knows a network bridge's capabilities and boundaries from file descriptors or else can read them at runtime. To meet the stream QoS requirements indicated in the CUC, the CNC calculates the paths, transmission schedules etc. and then configures TSN bridges along the selected path in the TSN network. After the CNC has been created, the CUC forwards it to the end devices and initiates the exchange of user plane traffic between the listener and talker as defined.

Figure 17 shows, in the context of 5G-TSN integration, a 5G system as part of a TSN network along with other, wired bridges. The central network configuration (CNC) interacts with a 5G bridge similarly to other bridges.

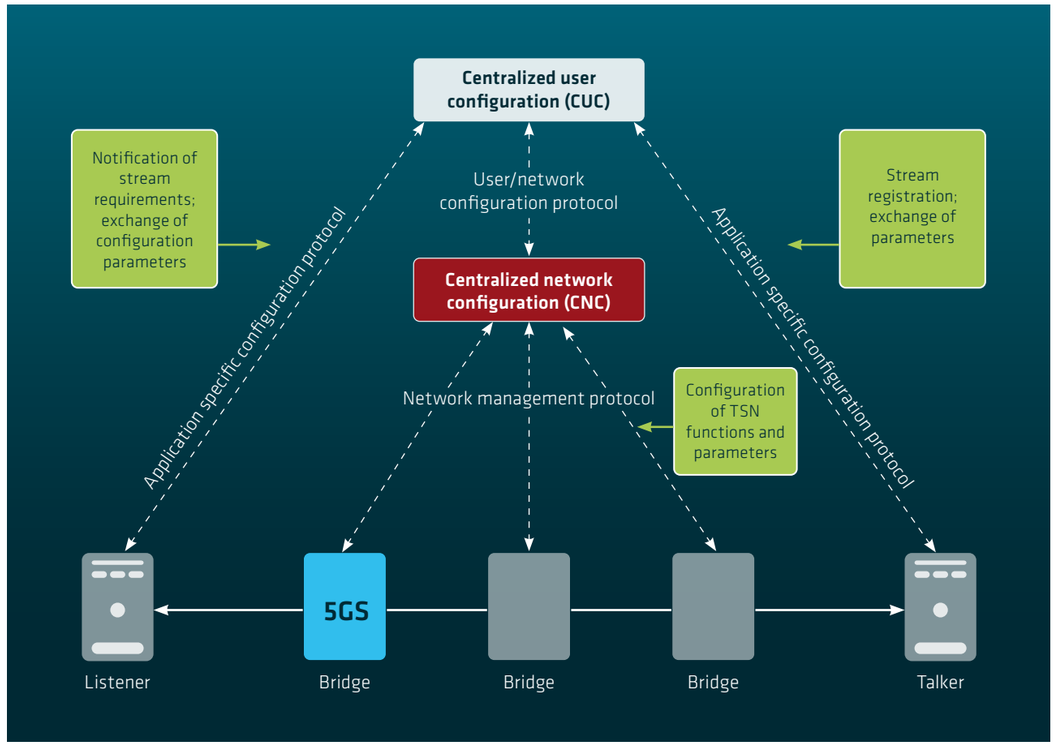
The CNC collects information on bridges (including the 5G system bridge), their capabilities, and the network's topology. This enables it to perform the necessary calculations and select bridges and network paths for meeting the QoS requirements of the TSN streams. When the CNC finishes computing paths and scheduling, it sends the configurations to the corresponding bridges. The configuration can include traffic forwarding information, traffic classes and prioritization, scheduling information as specified in IEEE 802.1Qbv, and per-stream filtering and policing (PSFP) information as specified in IEEE 802.1Qci.

The CNC provides rules for handling TSN traffic via the TSN AF, and the 5G system translates them into corresponding 5G QoS rules and profiles for creating QoS flows. The QoS mapping table preconfigured by the TSN AF is used to identify a suitable 5G system QoS profile that follows the rules for incoming CNC traffic handling. The 5G system uses this profile to establish 5G QoS flows for delivering TSN traffic between the ingress and egress ports of the 5G bridge. The packet filters on the UE and UPF sides can be used to map various TSN streams to corresponding 5G QoS flows.

The TSN AF has information on ports on the UPF/NW-TT and UE/DS-TT sides. Based on the PSFP and traffic forwarding information provided by the CNC, the TSN AF identifies the ingress port and egress port for a given stream. For uplink traffic, the 5G system forwards traffic to an appropriate NW-TT port based on the traffic forwarding information provided by the CNC. For downlink traffic, the TSN AF determines the DS-TT MAC address used by the PDU session to identify the UE whose traffic needs to be routed. The PSFP information can be also used by the TSN AF to derive TSCAI, which the RAN then sends to provide effective support for TSN streams.

The 5G system can also receive configuration information on time-aware scheduling from the CNC, as defined in IEEE 802.1Qbv, which the TSN AF can then forward to relevant egress ports in DS-TT(s) and NW-TT. The time-aware scheduling feature requires DS-TT and NW-TT ports to support a hold and forward mechanism as described in IEEE 801.2Qbv.

Figure 17: A centralized TSN network configuration



Source: Time-Sensitive Networking for Dummies

4.5.1 Example Use Case: Robot Control with an Interchangeable Tool

Application
Control-to-device (C2D) communication between a programmable logic controller (PLC) and a robot with a wireless tool

Situation
A robot arm docks onto an interchangeable gripper using a special tool that, due to environmental conditions, requires a wireless connection and acts as a UE. Time synchronization and QoS mechanisms are required for all components in order to meet high accuracy requirements.

Service Flow
1. The CNC acquires the necessary parameters and information from TSN end stations, TSN bridges, and the 5G system bridge.
2. The CNC performs path computation and scheduling to meet the QoS requirements of the TSN streams, sends the configurations to the corresponding bridges, and specifies traffic handling rules for TSN traffic via the TSN AF.
3. The 5G system translates these rules into corresponding 5G QoS rules and profiles and sets up QoS flows.

4. The TSN AF forwards scheduling information to the ingress and egress ports for the streams involved. The 5G system forwards uplink traffic to the appropriate NW-TT port. The TSN AF determines the DS-TT MAC address used by the PDU session and routes downlink traffic to the UE.
5. The TSN AF uses PSFP information and derives TSCAI, which it sends to the RAN.

Follow-Up
The robot and the PLC communicate via Industrial Ethernet, with the tool (which is part of the gripper) being wirelessly connected to the PLC via 5G. All components support TSN features.

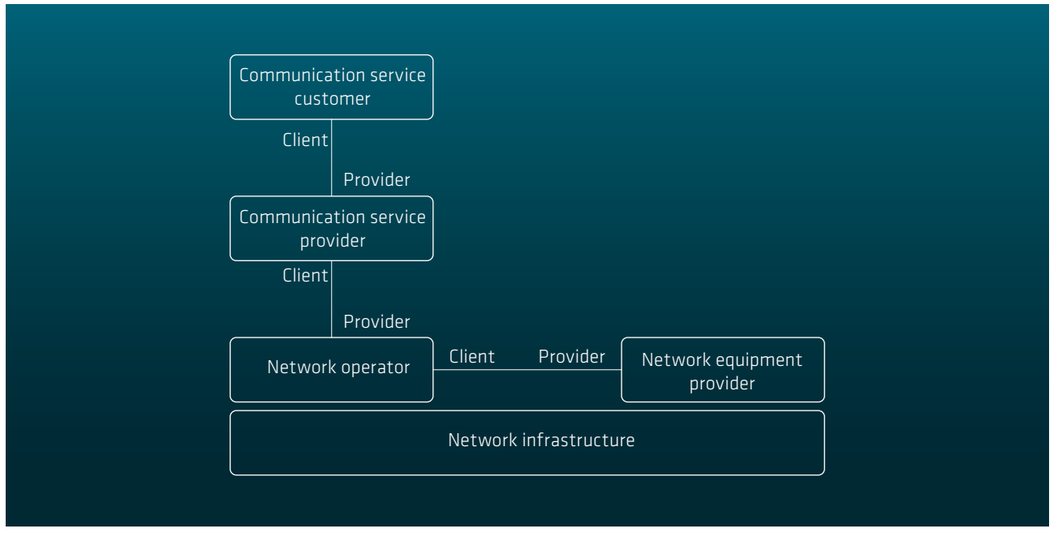
4.6 Using QoS Differentiation in Non-Public Networks

Section 3.6 introduced the concept of non-public networks (NPNs), broken down into standalone non-public networks (SNPNs) and public-network-integrated NPNs (PNI-NPNs). The 5G QoS framework and NPN deployment model are independent of one another. As mentioned in section 3.6, the main impact of NPNs is on OAM (operations, administration, and maintenance).

Management of network configurations (such as QoS profiles, subscription data, etc.) affecting the QoS supported in a NPN is performed by a "network operator" corresponding to the role model defined in reference [37] (see figure 18). The network operator uses network management services exposed by the network equipment. The network operator can expose management services to a communication service provider by limiting access to specific configurations.

Reference [38] defines the following roles for managing an NPN as shown in figure 18:

Figure 18: Abstract from reference [38], figure 4.8.1 "high-level model of roles"



Source: 5G-ACIA

- The NPN operator (network operator), which designs, builds, and operates an NPN while providing all required network services and resources.
- The NPN service provider (communication services provider), which provides, designs, builds, and operates nonpublic communication services via an NPN. These services are supported by network services provided by the NPN operator.
- The NPN service customer (communication service customer), which consumes services from an NPN service provider. In the present case, the IIoT application provider is the NPN service customer.

These three roles apply to both the SNPN and the PNI-NPN deployment models. According to reference [38]:

- For managing an SNPN:
  - The NPN service provider role can be performed by a vertical (or 3rd-party service provider acting on its behalf) or an MNO that provides nonpublic services.
  - The NPN operator role can be performed by either a vertical (or a private company on its behalf) or a MNO that manages the SNPN.
- For managing a PNI-NPN:
  - The NPN service provider role can be performed by a vertical (or a private company acting on its behalf) or an MNO that provides the NPN service.
  - The NPN operator role can be performed by an MNO or shared between an MNO and a vertical (or a private company acting on its behalf).

When different roles are implemented by different administrative entities (e. g. by different companies or different administrative departments within the same company), exposure of management services by the NPN operator to an NPN service provider is regulated by a service level agreement (SLA) among them.

The NEF provides a standardized interface for exposing the network capabilities of the 5G system, including the possibility of an IIoT application requesting a specific QoS for certain traffic.

The Common API Framework (CAPIF) (see reference [25]) aims to offer a unified northbound API framework across multiple 3GPP functions. It should be noted that CAPIF by itself doesn't expose any additional services, but is only a mechanism for discovering and exposing APIs provided by underlying network functions. An example is NEF APIs exposed using CAPIF.

The service enabler architecture layer (SEAL) provides a set of shared services for use by vertical applications. It facilitates the effective development and deployment of verticals in a 5G network.

4.6.1 Example Use Case: Asset Tracking

Objective
Tracking of an asset in a private network on the premises vs. tracking in a public network during transportation

Situation
An asset is tracked during the production process and in outbound logistics before it leaves the premises for shipping. Tracking is performed by a 5G connection to an SNPN on premise.

Service Flow
1. While QoS is monitored, the UE approaches the boundary of an SNPN.
2. When the QoS levels reach the minimum required thresholds, the UE terminates the ongoing PDU session and deregisters from the SNPN.
3. The UE registers with the new network and opens a PDU session with the requested QoS.
4. QoS monitoring resumes.

Follow-Up
The asset leaves the factory premises, loses SNPN coverage, and connects to a PLMN or PNI-NPN.

5 Conclusions

QoS is undeniably one of the most important properties of the connectivity services provided by the 5G system. This white paper describes the principal concepts, functionality, and operational aspects of 5G QoS in the context of 3GPP Release 16 and the relevant Release 17 functionality that has progressed sufficiently for technical specifications to be formulated for it. Specifically, it discusses and explains the following aspects:

- Methods that an application can use to select the desired QoS
- Parameters and procedures that an application can use to specify the requested QoS
- Functionality that the 5G system provides to applications for adapting to changes in the QoS
- QoS aspects of network slicing that can be relevant to an application functioning in a network environment that supports more than one slice
- The functionality available to applications that need to monitor QoS
- QoS aspects of TSN
- QoS aspects of various NPN deployment options
- Operational aspects of requests by applications for a specific QoS for a connection when establishing a new PDU session, modifying an ongoing PDU session, or releasing a PDU session

As far as possible, references are included to known 3GPP specification work in progress. Additional technical aspects are also described in detail in chapter 8 (annex).

The expectation is that 3GPP Release 17 and subsequent releases will make available additional functionality related to QoS. Since QoS is a very important topic for Industrial IoT applications, 5G-ACIA plans to review relevant new functionality when the corresponding specifications reach maturity.

6 Key Terms and Definitions

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

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

5G exposure function
A 5G function that implements a service exposed to IIoT applications using the 5G system (see reference [1]).

Application function (AF)
In 3GPP terms, the AF interacts with the 5G network to provide services, for example to request a specific QoS or otherwise interact with the 5G exposure function. In this white paper it is assumed that the AF isn't trusted by the provider of the 5G network and therefore interacts with the 5G network via the 5G exposure function in the core network (via the En reference point). See section 6.2.10 of reference [3].

Connection
In 3GPP terms, an active connection between the UE and data network (via the 5G core network and a UPF). This connection is established by a protocol data unit (PDU) session and packet flow descriptions (PFDs). The concept was introduced as a "device connection" in reference [1].

Data network
In 3GPP terms, a data network (DN) is a network external to the 5G network that is integrated with it via an N6 reference point and the user plane function (UPF). Application functions of the IIoT application are deployed in it. See reference [3].

Data network name (DNN)
In 3GPP terms, a DNN in 5G or an APN in earlier 3GPP releases. It is the fully qualified domain name of a gateway between a mobile network and another network. See reference [29] for more information.

IIoT application
A set of application functions needed to manage industrial processes. IIoT applications can be deployed and executed on any computing entity connected to the 5G network exposure interface. See reference [1].

Quality of service (QoS)
The set of characteristics of a communication service that affect its ability to satisfy stated and implied needs of the service's users. See reference [20].

QoS attribute
A generic term referring to any of the QoS parameters or characteristics defined by 3GPP. See reference [3].

QoS flow
The smallest granularity that can be used to differentiate traffic for scheduling, queue management, rate shaping, etc. within the 5G system. All traffic mapped to the same 5G QoS flow receives the same forwarding treatment (e. g. scheduling policy, queue management policy, rate shaping policy, RLC configuration, etc.). Separate 5G QoS flows are required to provide differentiated QoS forwarding treatment. For more information, see section 5.7 of reference [3].

PDU session
A logical connection within the 5G system that carries IP packets or Ethernet frames between the UE and UPF. It can contain one or more QoS flows. This definition has been adapted from the one provided in reference [3] while striving to preserve the original 3GPP concept.

User equipment (UE)
In 3GPP terms, the equipment that grants an application access to network services. In the context of 3GPP specifications, the interface between the UE and the network is called the radio interface. See reference [31].

Network function
In a network, a 3GPP-adopted or 3GPP-defined processing function with defined behavior and interfaces. It can be implemented as a network element on dedicated hardware, a software instance running on dedicated hardware, or a virtualized function instantiated on an appropriate platform such as cloud infrastructure. See reference [3].

7 Acronyms

3GPP	3rd Generation Partnership Project
5G-ACIA	5G Alliance for Connected Industries and Automation
5G-EF	5G exposure function
5G system	5G system
5QI	5G QoS identifier
AF	Application function
AGV	Automated guided vehicle
AMF	Authentication and mobility function
API	Application programming interface
ARP	Allocation and retention priority
CAPIF	Common API framework
CNC	Centralized network configuration
CSI	Communication service interface
CUC	Centralized user configuration
DL	Downlink
DNN	Data network name
DSCP	Differentiated service code point
GBR	Guaranteed bit rate
GFBR	Guaranteed flow bit rate
gNB	Next generation NodeB
GTP-U	GPRS tunnelling protocol for user data
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IIoT	Industrial Internet of Things
IP	Internet Protocol
ITU	International Telecommunication Union
IUT-T	Telecommunication standardization sector of ITU
LLDP	Link layer discovery protocol
MAC	Media access control
MES	Manufacturing execution system
MFBR	Maximum flow bit rate
mMTC	Massive machine-type communications
MPLR	Maximum packet loss rate
ms	Milliseconds
NEF	Network exposure function
NG-RAN	Next-Generation Radio Access Network
NPN	5G Non-Public Network
NSSAI	Network slice selection assistance information
NSSP	Network slice selection policy
OAM	Operation and maintenance
OS	Operating system
OSS	Operation and support system
PCC	Policy and charging control
PCF	Policy control function
PCP	Priority code point
PDB	Packet delay budget
PDU	Packet data unit
PER	Packet error rate
PFD	Packet flow description
PLMN	Public land mobile network
PNI-NPN	Public network integrated NPN
PSA	PDU session anchor
PSFP	Per-stream filtering and policing
QFI	QoS flow identifier
QoS	Quality of service
RAN	Radio access network
RQA	Reflective QoS attribute
RTT	Round trip time
SEAL	Service enabler architecture layer for verticals
SLA	Service level agreement
SLS	Service level specification
SMF	Session management function
SNPN	Standalone NPN
S-NSSAI	Single-network slice selection assistance information
TSCAI	Time-sensitive communication assistance information
TSN	Time-sensitive networking
TT	TSN translator
UE	User equipment
UL	Uplink
UP	User plane
UPF	User plane function
URL	Uniform resource locator
URLLC	Ultrareliable low latency communication

8 Annex: Network Slice Selection

Before describing the network slice selection mechanism, first it's necessary to introduce the most important network slice terminology. Each network slice is uniquely identified by an S-NSSAI (= Single Network Slice Selection Assistance Information), which has two fields: one containing the slice/service type (SST) and the other containing an optional slice differentiator (SD). The SST is one of a set of values that has been standardized by 3GPP for describing the network slice's expected behavior in terms of features and services. The SD is used to distinguish between network slices with the same SST and is assigned by the corresponding public land mobile network (PLMN). An NSSAI (Network Slice Selection Assistance Information) is a collection of up to eight S-NSSAIs.

Network slice selection, defined in section 5.15 of reference [3], takes place when a UE registers with the 5G system. At that time, the UE lets the 5G system know which network slices it needs by submitting a list of network slice identifiers. This is the single network slice selection assistance information (S-NSSAI). The UE creates the list from the S-NSSAIs stored in its configuration, which is called the Configured NSSAI (in other words, a configured collection of S-NSSAIs), plus a list of network slices that the UE may connect to (called the Allowed NSSAI, a collection of allowed S-NSSAIs), which it has received earlier from the network. Configured NSSAI and Allowed NSSAI are always associated with a PLMN, since S-NSSAIs aren't globally unique but only unique within a particular PLMN. This calls for a dedicated mechanism for the roaming scenario, which is beyond the scope of this paper. When registering, the 5G network assigns the Allowed NSSAI to the UE while taking into account the network slices requested by the UE, those that are configured in the user subscription, the network slices available at the location from which the UE is registering, the access type (3GPP or non-3GPP), and information on the network configuration. It isn't mandatory for the UE to have a Configured NSSAI, and it can also refrain from requesting a specific network slice when registering. In the second case, the network assigns an Allowed NSSAI to the UE (if the subscription information includes designated default network slices). The network can update the allowed network slice assigned to the UE at any time, for example if the controlling AMF, the subscription information, or other relevant aspects have changed. The network can also allow the UE to reregister.

New functionality introduced in Release 17 makes it possible to limit the maximum number of UEs that may register with each of the 5G system's network slices. This can be done to enforce the "maximum number of UEs" parameter defined in the GSMA slice template; see reference [12].

A PDU session is bound to a specific network slice (S-NSSAI) and data network name (DNN), but a network slice can support multiple PDU sessions and DNNs. Consequently, if a UE registers with a given PLMN with a certain network type (3GPP or non-3GPP) and receives an Allowed NSSAI at that time, it will only be able to request the establishment of PDU sessions that are associated with the allowed network slices (in other words, whose DNNs are associated with the permitted S-NSSAI). The network will reject requests for PDU sessions that aren't associated with the allowed network slice.

The UE selects the S-NSSAI from the Allowed NSSAIs in compliance with the network slice selection policy (NSSP) contained in the UE's route selection policy (URSP) or according to its local configuration (defined in section 6.1.2.2.1 of reference [10]) and, if available, the DNN to which the PDU session is related. The 5G network assigns to the UE a URSP containing rules that specify how it must map application traffic and the associated PDU sessions, DNNs, the network slice selection policy, and the preferred access type. Application traffic is described similarly to the corresponding QoS rules, with the possibility of adding an application identifier.

The serving 5G network can use control plane procedures to deliver the URSP policy (including an NSSP) at any time during the lifetime of the UE's registration (see section 4.2.4 of reference [9]). Alternatively, the UE can select a network slice using locally configured information that isn't standardized by 3GPP. If the UE is unable to determine which network slice it should use for a newly established PDU session, it also won't be able to provide this information. In this case, the 5G network chooses a suitable network slice for the PDU session.

The 3GPP specifications permit up to 16 subscribed network slices, called subscribed S-NSSAIs, to be defined in the subscription information. Depending on the operator's policy, one or more subscribed S-NSSAIs can be marked as default S-NSSAIs. In this case, as a minimum the network will be ex-

pected to make this network slice available to the UE unless the latter sends an S-NSSAI to the network in a registration request message.

When an IIoT application residing in the UE wants to request a specific network slice (S-NSSAI) for its traffic, there are two possible scenarios:

1. The IIoT application has no information on available slices in the 5G system.
2. The IIoT application knows about available slices in the 5G system because they are exposed by an API that is also running on the UE. Although APIs of this type haven't been standardized by 3GPP yet, the UE's operating system can provide them to the IIoT application.

In the first scenario, the IIoT application isn't required to have any knowledge of the available network slices provided during registration or of the PDU sessions that the UE has established. In this case, it's assumed that the UE is configured locally or provided with the URSP policy by the PLMN. When the application starts sending traffic, the UE checks whether the traffic complies with the policy for routing data in the URSP or local configuration and performs mapping in accordance with the matching rules in the URSP. If the UE has already established a PDU session that maps to the outgoing data packets, traffic is routed via that session. If there is no active PDU session, the UE requests the establishment of one via the corresponding network slice as indicated in the policy so that the data packets can be routed accordingly. The IIoT traffic is then mapped to a network slice and PDU session in accordance with the URSP policy or UE local configuration.

Here it's important to note that if the application is associated with a specific PDU session and network, say the one for industrial applications (S-NSSAI = x), but that slice isn't available (for example, because S-NSSAI = a and S-NSSAI = b are permitted but not S-NSSAI= x), the UE will be unable to establish a PDU session on it. So, if the UE initiates the PDU session establishment procedure associated with S-NSSAI=x, the network will reject the request. Conversely, if S-NSSAI = x is included in the Allowed NSSAI, the UE will be able to establish a corresponding PDU session.

In the second scenario, the UE exposes information on available network slices and PDU sessions to the IIoT application residing in it. In this case, the IIoT application will be able to select S-NSSAI and a related PDU session but the UE will comply with the USRP policy configuration and reject S-NSSAI and the PDU session for noncompliance. The 5G system will approve the request to establish a PDU session in view of the Allowed NSSAI setting, user subscription profile, and other settings that aren't covered by this paper.

The AF may interact with the OAM exposure interface in order to access user subscription information on the subscribed slice and properly configure the network slice selection procedures. However, so far at least 3GPP has not standardized any APIs for this. If the IIoT application residing on the UE needs to request a specific network slice that isn't currently available or doesn't support the establishment of QoS flows with a particular QoS profile, no interface to the 5G system will be available for doing so either. In this case, the application will have to use the interface between the AF and the 5G exposure function to modify the network slice configurations, for example interfaces exposed via 5G OAM. Alternatively (or additionally), human intervention may be required to modify the network's deployment and configuration.

9 References

[1] 5G-ACIA white paper "*Exposure of 5G Capabilities for Connected Industries and Automation Applications"*, version 2, March 2021.

[2] 3GPP Technical Specification 23.434 *"Service Enabler Architecture Layer for Verticals (SEAL); Functional architecture and information flows"*, version 17.2.0, June 2021.

[3] 3GPP Technical Specification 23.501 *"System Architecture for the 5G System (5G System); Stage 2"*, version 17.1.1, June 2021.

[4] 3GPP Technical Specification 38.314 *"NR; Layer 2 Measurements"*, version 16.3.0, March 2021

[5] 3GPP Technical Specification 38.415 *"NG-RAN; PDU Session User Plane Protocol"*, version 16.5.0, July 2021.

[6] 3GPP Technical Specification 23.203 *"Policy and Charging Control Architecture"*, version 17.1.0, June 2021.

[7] 3GPP Technical Specification 29.281 *"General Packet Radio System (GPRS) Tunnelling Protocol User Plane (GTPv1-U)"*, version 17.0.0, March 2021.

[8] 3GPP Technical Specification 22.104 *"Service Requirements for Cyber-Physical Control Applications in Vertical Domains"*, version 17.6.0, June 2021.

[9] 3GPP Technical Specification 23.502 *"Procedures for the 5G System (5G system);Stage 2"*, version 17.1.0, June 2021.

[10] 3GPP Technical Specification 23.503, *"Policy and Charging Control Framework for the 5G System (5G system); Stage 2"*, version 17.1.0, June 2021.

[11] 3GPP Technical Specification 29.122 *"T8 Reference Point for Northbound APIs"*, version 17.2.0, June 2021.

[12] GSMA NG.116, *"Generic Network Slice Template"*, version 5.0, June 2021.

[13] GSMA, *"Network Slicing, Use Case Requirements"*, version 1.0, April 2018.

[14] 3GPP Technical Report 22.804 "*Study on Communication for Automation in Vertical Domains (CAV)*", version 16.3.0, July 2020.

[15] 3GPP Technical Specification 22.261 "*Service Requirements for the 5G System*", version 17.7.0, June 2021.

[16] 5G-ACIA white paper "Integration of 5G with Time-Sensitive Networking for Industrial Communications", January 2021.

[17] 3GPP Technical Specification 24.501 "*Non-Access-Stratum (NAS) protocol for 5G System (5G system); Stage 3*", version 17.3.1, July 2021.

[18] 3GPP Technical Specification 24.007 "*Mobile Radio Interface Signalling Layer 3; General Aspects*", version 17.2.0, June 2021.

[19] 3GPP Technical Specification 29.522 "*5G System; Network Exposure Function Northbound APIs; Stage 3*", version 17.2.0, June 2021.

[20] ITU-T Recommendation E.800 "*Quality of Telecommunication Services: Concepts, Models, Objectives and Dependability Planning – Terms and Definitions Related to the Quality of Telecommunication Services*", September 2008.

[21] IEEE P802.1Qcc-2018, *"Standard for Local and metropolitan area networks – Bridges and Bridged Networks – Amendment: Stream Reservation Protocol (SRP) Enhancements and Performance Improvements"*, October 2018.

[22] 5G-SMART European project deliverable – "*D1.4 Radio Network Deployment Options for Smart Manufacturing*", November 2020.

[23] IEEE 802.1AB-2009, "*IEEE Standard for Local and Metropolitan Area Networks – Station and Media Access Control Connectivity Discovery"*, 2009.

[24] IEEE Standard 802.1Q-2018, "*IEEE Standard for Local and Metropolitan Area Networks: Bridges and Bridged Networks*", July 2018.

[25] 3GPP Technical Specification 23.222 "*Functional Architecture and Information Flows to Support Common API Framework for 3GPP Northbound APIs*", version 17.5.0, June 2021.

[26] 3GPP Technical Specification 29.513 *"5G System; Policy and Charging Control Signalling Flows and QoS Parameter Mapping; Stage 3"*, version 17.3.0, June 2021.

[27] 3GPP Technical Specification 29.514 "*5G System; Policy Authorization Service; Stage 3*", version 17.1.0, June 2021.

[28] 3GPP Technical Specification 23.247 *"5G Multicast-Broadcast Services; Stage 2"*, version 2.0.0, September 2021.
[29] 3GPP Technical Specification 23.003 "*Numbering, Addressing and Identification*", version 17.2.0, June 2021.
[30] 5G-ACIA white paper "*5G Nonpublic Networks for Industrial Scenarios*", July 2021.
[31] 3GPP Technical Specification 21.905 "*Vocabulary for 3GPP Specifications*", version 17.0.0, July 2021.
[32] 3GPP Technical Specification 28.533 "*Management and Orchestration; Architecture Framework*", version 16.7.0, April 2021.
[33] 3GPP Technical Specification 27.007 "*AT Command Set for User Equipment (UE)*" version 17.2.0, July 2021.
[34] 3GPP Technical Specification 23.288 "*Architecture Enhancements for 5G System (5G System) to Support Network Data Analytics Services*", version 17.1.0, June 2021.
[35] 5G-ACIA, "*Performance Testing of 5G Systems for Industrial Automation*", 2019, https://5g-acia.org/whitepapers/performance-testing-of-5g-systems-for-industrial-automation-2/
[36] 3GPP Technical Specification 28.554 *"Management and Orchestration; 5G End to End Key Performance Indicators (KPI)"*, version 17.3.0, June 2021.
[37] 3GPP Technical Specification 28.530 "*Management and Orchestration; Use Cases and Requirements*", version 17.1.0, April 2021.
[38] 3GPP Technical Report 28.807 "*Study of Management of Nonpublic Networks (NPN)*", version 1.2.0, June 2020.
[39] Google, recommended upload encoding settings at https://support.google.com/youtube/answer/1722171?hl=en#zippy=%2Cbitrate, accessed on October 28, 2021.

5G-ACIA White Paper
5G QoS for Industrial Automation

Contact
5G Alliance for Connected Industries and Automation
(5G-ACIA), a Working Party of ZVEI e. V.
Lyoner Strasse 9
60528 Frankfurt am Main
Germany
Phone: +49 69 6302-209
Fax: +49 69 6302-319
Email: info@5g-acia.org
www.5g-acia.org

Published by
ZVEI e. V.
www.zvei.org

November 2021
Design: COBRAND Berlin

10 5G-ACIA Members

As of November 2021

5G to go
AALBORG UNIVERSITY DENMARK
ABB
AI-LINK
ALTRAN Part of Capgemini
arm
ASKEY
ASOCS
ATHONET
aurelis
Baicells
BAYFU
BECKHOFF
BOSCH
Canon
celona
中国移动 China Mobile
cisco
CONGIV
DASSAULT SYSTEMES
DENSO
Deutsche Messe
DFKI
CATAPULT Digital
docomo
Druid
EMERSON
Endress+Hauser
ERICSSON
ETRI
FESTO
flex
Fraunhofer
GHMT
HARTING
HIRSCHMANN A BELDEN BRAND
HMS
HUAWEI
IDLab INTERNET & DATA LAB
ifak
ifm
III
Infineon
inIT
intel
ITRI Industrial Technology Research Institute
KETI
KEYSIGHT TECHNOLOGIES

Lenovo
LS telcom
MAVENIR
MC TECHNOLOGIES
Microsoft
MITSUBISHI ELECTRIC
MOXA
MUGLER TELCO NETWORKS.
Nitto
NOKIA
NXP
orange
Panasonic
PEPPERL+FUCHS
PHOENIX CONTACT
Qualcomm
RELIABLE REAL-TIME RADIO
Radisys
ROHDE&SCHWARZ
SAL SILICON AUSTRIA LABS
salzburgresearch
Schneider Electric
SICK
SIEMENS
SINTEF
SoftBank
SONY
st life.augmented
T
TRUMPF
TZI
ublox
UPLINK
verizon
VIAVI VIAVI Solutions
vodafone
VOLKSWAGEN AKTIENGESELLSCHAFT
WAGO
Weidmüller
XITASO
YOKOGAWA
ZTE

5G ACIA

www.5g-acia.org