RESEARCH ARTICLE

Is Release 15 Ready for the Industry?

ANDRÉ PERDIGÃO[1,2], **JOSÉ QUEVEDO**[2], **(Member, IEEE),**
AND RUI L. AGUIAR[1,2], **(Senior Member, IEEE)**

[1]Departamento de Eletrónica, Telecomunicações e Informática (DETI), Universidade de Aveiro, 3810-193 Aveiro, Portugal
[2]Instituto de Telecomunicaçes (IT), 3810-193 Aveiro, Portugal

Corresponding author: André Perdigão (andreperdigao@ua.pt)

ABSTRACT 5G technologies are considered a cornerstone of the advent of the next industrial revolution. Promising performance improvements, along with advanced features and assurances in terms of reliability, flexibility and isolation, are expected to enable the realization of diverse and novel use cases, fostering industrial automation with optimized production lines and manufacturing systems. This document shares the experience and knowledge using a 5G SA network for industrial applications. Concretely, the paper examines whether and how the available technology could fulfil the demanding industry requirements, namely in terms of isolation, flexibility and performance. This gap analysis revealed 5G QoS mechanisms as a key driver towards 5G for industry. Thus, a comprehensive analysis of the existing mechanisms and their impact on the network performance are presented, serving as a reality check of 5G SA Release 15 technologies. Although results showed promising possibilities to support industrial deployments, there is still a gap between what's achievable and what is expected from 5G that will be gradually filled by the introduction of novel features in the upcoming releases. In general, the contributions and insights presented in this paper are considered to be valuable for industry, standards development organizations, manufacturers, and the wider 5G ecosystem. Moreover, this paper serves as a foundational component within a larger endeavour of automating network slicing mechanisms for industrial applications.

INDEX TERMS 5G SA, testbed, NPN, network slicing, release 15, Industry 4.0, QoS, industry.

I. INTRODUCTION

Industry 4.0 aims to connect everything and everyone within the factory to enhance safety, productivity, product quality, and product customization. A wireless technology capable of meeting the demanding requirements of various use cases deployed inside factories, while ensuring a high level of security and data isolation, can become the main driver of Industry 4.0. With its technological advancements, 5G is expected to fulfil the necessary requirements for implementing this new variety of use cases in a factory [1]. This has also been identified by relevant bodies in the 5G ecosystem, such as 5G-ACIA [2] and 3GPP [3]. Ultimately, the introduction of

The associate editor coordinating the review of this manuscript and approving it for publication was Stefano Scanzio.

5G technologies for industry use cases is expected to be advantageous from an economic perspective [4], [5].

Considering this, Standards Development Organizations (SDOs) like 3GPP have recognized the necessity of adapting the technology according to industrial requirements and have included several technologies and concepts in their technical specifications. One of these concepts is the Non-Public Network (NPN) [6], which is a 5G network designed for private entities, such as the industry. NPN includes the following two main deployment strategies:

i) Standalone NPN, where the vertical owns and has complete control over the network. This means that verticals bear all costs related to the purchase and maintenance of the network.

ii) Public Network Integrated NPN (PNI-NPN), where one or more network slices are created within the operator's

public network for the exclusive use of the vertical. This reduces the vertical cost while providing adequate isolation, security, and control of the vertical network. Several deployment options exist within PNI-NPN, and [6] presents some of the envisioned NPN deployment types. Each deployment has a different level of integration with the public network.

The network slices in 5G [7] offer several functionalities, with PNI-NPN being one specific use case. Each network slice may have varying functionality (e.g., priority, charging, policy control, security, and mobility) and performance (e.g. latency, mobility, availability, reliability, and throughput) requirements. In addition, network slices can cater to different user groups (e.g., corporate customers, public network users, or industrial users). Network slices, also, allow the deployment of multiple custom networks on a single network infrastructure.

This study focuses on assessing whether 5G technology in release 15 meets the stringent industry demands, ultimately evaluating its readiness for deployment in a factory floor for production. To this end, the work relies on a real-world commercial graded 5G SA Release 15 network and takes insights from: (i) white papers from industrial associations such as 5G-ACIA [2], [6]; and (ii) the requirements of several projects, including H2020 5Growth[1] [4], [8], Augmanity (Augmented Humanity)[2] [9], and Horizon-Europe Imagine-B5G.[3] To provide the reader with a more concrete contextualization of the paper's insights, examples of the Augmanity project are used throughout the paper. However, it is important to understand that this contextualization does not hinder the generalization of the contributions of paper.

The industry requires full control over the production line. To this end, the Manufacturing Execution System (MES) provides a comprehensive overview of the production line. MES provides centralized control to personnel, where is possible to monitor the condition of all assets and optimize resource usage. It stands to reason, that the underlying networking infrastructure should be considered as one of the industry assets. As such, the integration of the 5G network with MES becomes an essential aspect of the Industry 4.0 roadmap.

However, existing 5G management endpoints are complex and require specific expertise, making it challenging to integrate with the MES. Hence, an initial step towards the integration of 5G and MES, is to gain a thorough understanding of how the 5G network operates. Allowing the subsequent abstraction of the network management endpoints in alignment with the industry requirements.

In this context, the main contribution of this paper is to assess the capability of Release 15 technologies to support industrial scenarios by providing a gap analysis and a technical evaluation of the expected performance of a commercial SA 5G network with R15. This evaluation

aims to support the stringent and heterogeneous requirements imposed by industries for deploying such technology in their factories. The lack of support to fulfil the slicing requirements in the current solutions, prompted the need for a comprehensive analysis of the flexibility of the network's mechanisms that impact communication performance. This leads to the second contribution of the paper, which presents quantitative results on how adjustable the R15 5G network is in terms of communication performance. This not only allows to analyze whether current 5G technology can meet the industry expectations but also is considered to be a cornerstone aspect in the larger endeavour of automating network slice deployment. Furthermore, although not tackled in this paper the results presented could be explored to establish direct comparisons not only with the upcoming releases of 5G technologies but also with other concurrent technologies like Wi-Fi or cabled networks.

The remainder of this document is organized as follows: Section II presents relevant related work. Section III makes a brief presentation of the Augmanity project, outlining the main requirements imposed by the industry for the implementation of a 5G network in their facilities. This is followed by a description of the network infrastructure, giving an overview of how the different requirements imposed on the network were addressed. Since the main requirements involve the deployment and control of network slices, the document proceeds to examine the current state of network slicing in a commercial 5G network. The main focus is on the communication performance of a network slice, analyzing the flexibility available in an R15 5G network to adjust the communication performance. This analysis centres on the QoS mechanism present in 5G, as there is no direct mechanism to adjust the communication performance of each network slice. So, Section IV introduces the 3GPP QoS mechanisms for enforcing communication performance in 5G and the configurable parameters available in R15. Section V provides an overview of 5G software and configurations, discusses the QoS parameters to be validated, how evaluated parameters can be configured in the 5GAIner network, and the scenarios used to evaluate their effects. Section VI describes the tests performed, presents the results, and discusses the effect of each parameter. Section VII provides the document conclusions by discussing the current state of 5G networks, existing problems, and aspects that require improvement before the adoption of the industry. It also discusses the performance results obtained, considers how configurable a slice is at the moment, and discusses the current limitations expected in an R15 5G network. The section finalizes with a brief vision from the authors about future 5G releases and whether 5G will ever be ready for production deployment in the industry.

II. RELATED WORK
Numerous 5G testbeds have been deployed worldwide to develop and evaluate 5G technologies and use cases. Such testbeds are essential for 5G development, enabling academia

---

[1] https://5growth.eu/
[2] https://www.augmanity.pt/
[3] https://imagineb5g.eu/

and industry to experiment with the technology, assess new functionalities, and explore potential use cases. For instance, authors in [10] present the comprehensive design and deployment of a 5G standalone infrastructure under the scope of 5G-VINNI, while summarizing experimentation with various use cases across different verticals. Similarly, authors in [11] introduce a non-standalone 5G testbed and analyze its performance. Furthermore, authors in [12] present an industrial standalone 5G testbed, evaluate its performance, and conclude that the deployment's performance effectively meets the requirements of industrial use cases.

There are also developments of open-source solutions within the 5G market offering significant advantages. It streamlines technology development, fostering simpler applicability and interaction while mitigating vendor lock-in. This approach enables seamless interconnection and interoperability among various solutions. Moreover, the adoption of open-source solutions provides greater control and configurability over the 5G network, empowered by open interfaces and accessible source code. Concretely, multiple open-source initiatives are tackling open-source 5G solutions such as: free5GC,[4] Open5GS,[5] and Open Air Interface (OAI).[6]

In parallel, O-RAN Alliance[7] has been actively engaged in standard development and advocated for the development of open solutions. Consequently, considerable research efforts were directed towards the development and utilization of Open RAN solutions, as evidenced by the work in [13], [14], [15], and [16]. Additionally, authors in [8] already evaluate the use of Open RAN solutions in the deployment of vertical use cases. For this later work it can be concluded that despite the benefits associated with open solutions, the technology is still being developed, thus having lower performance when compared with commercial solutions. As such, in this paper we opted for using a top-of-the-line solution to assess a best case scenario on the reality of 5G.

Authors in [17] discuss various types of use cases that verticals can deploy with 5G, showcasing the benefits that verticals can derive from this technology. The paper also outlines the network requirements necessary for NPN deployment, encompassing security, privacy, and customization requirements. These requirements signify the necessary conditions that must be met before the technology is deemed ready for operational use. Authors in [18] and [19] also delve into a discussion about security and privacy, offering insights into the development and proposing of new solutions to ensure slice security and isolation. This highlights the ongoing research and development of new solutions aimed at addressing some of the existing challenges that must be resolved prior to technology adoption.

The work in [20] focuses on deploying several use cases with completely distinct requirements, which demands the utilization of the three envisioned types of 5G slices for simultaneous deployment. Although the 5G network can deploy the use cases, network resource usage is not optimized, wasting resources and limiting the number of use cases that can be deployed in a single infrastructure. So, as referred by the authors, an optimization of the usage of 5G resources is necessary, but for this, it is necessary to use mechanisms of quality of service in each slice to adjust the performance of communications to the use case.

Extensive research has also been conducted on the utilization, benefits and potential applications of 5G in the industrial sector. Authors in [21] conducted a theoretical analysis of the 5G deployment in the industry, presenting its benefits and functionalities that will benefit the industry. Authors in [22] analyse how the management of network slices can be done and the interactions of different stakeholders, by discussing the strategies that the 3GPP Network Slicing management functions allow for the deployment and control of the network slices that verticals will use. In addition, there are also organizations, such as 5G-ACIA and 5G-DNA,[8] dedicated to the standardization, promotion and dissemination of 5G for the industry.

Even with the extensive material discussing and presenting 5G in the industry, it is only possible to understand the requirements and constraints that exist in the deployment of 5G in industrial facilities by directly working with the industry. Therefore, to properly understand the requirements that 5G needs to fulfil, before being implemented in production inside industrial facilities, several projects like H2020 5Growth, Augmanity, and Horizon-Europe Imagine-B5G were created with a focus on the usage of 5G technologies by vertical industries. As a result, it was possible to understand the industrial requirements and adjust 5G technology in accordance.

To develop initial proof of concepts that demonstrate the usage of 5G by the verticals and its deployment in the production line, one most first assess the configurability of a 5G network and investigate how to adjust the performance of 5G slices tailored to the concrete use case. However, no relevant information was found in the existing literature regarding this topic. As a result, the focus was enlarged to studies of QoS mechanisms in communication technologies that offer insights into customising performance. Authors in [23] study the use of QoS in a network slice through simulation, but in terms of other communication technologies, exists several studies over the years, such as 802.11 networks [24] and [25], MPLS [26], 4G [27], SDN [28], and 5G [29]. Still, an in-depth study of the existing slicing mechanisms which demonstrate that the 5G network is flexible enough to ensure the requirements of the industry was not found in the reviewed literature.

As such, this document analyzes the requirements of the industry based on a 5G deployment in industrial environments, examining the capabilities of R15 5G to meet the industrial requirements. Since QoS mechanisms are at the basis of slice implementations, the paper presents a study on the QoS mechanisms to assess the flexibility of an R15 5G network and provides a preliminary understanding of the capabilities that could be expected in a 5G slice implementation.

III. 5G INDUSTRIAL NETWORK

The conception of the 5G Industrial Network involved various stakeholders including universities, research institutes, operators, industries, IT (information technology), and OT (operation technology) companies. The resulting infrastructure was used for testing, development, and evaluation of the 5G use cases under the scope of different projects, partially leading to the results presented in this paper.

A. DESIGN, REQUIREMENTS AND CONSTRAINTS

Since the infrastructure is located in Portugal, it needs to comply with Portugal's regulations, which forbid anyone besides operators from owning a radio spectrum. This restriction limits the possibility of standalone 5G network deployments, as such deployments become dependent on the operators. From the deployment options discussed by 5G-ACIA in [6], the 5G deployment is restricted to a PNI-NPN.

During the implementation of the 5G network in the different projects, verticals imposed several requirements, but there are two main requirements that recurrently emerged across projects: 1) Security and isolation: Ensuring that any data produced by the vertical must be confined to their premises; 2) Network slicing: Provides mechanisms that allow verticals to control the communication performance of 5G communication in the network slices according to their requirements, and mechanisms to monitor the performance of the different slices deployed on the network.

B. IMPLEMENTED SOLUTION

To address the two requirements above, for deploying a 5G network in vertical's facilities, the 5G network was designed and adjusted accordingly throughout the execution of the different projects. This section describes the approach taken to tackle each problem. For providing better contextualization, in the remainder of this section, we will focus on the concrete examples of the Augmanity project.

1) SECURITY AND ISOLATION

To provide 5G coverage in the industrial facility, the 5GAIner [30] network was expanded to Bosch Thermo-Technology (TT) premises. 5GAIner is the 5G network used in the Augmanity project and is an integral part of the Portuguese facility of the Horizon-Europe Imagine-B5G project. The design of the infrastructure expansion took into account the above requirements. As a solution, Multi-access Edge Computing (MEC) was included in the industrial
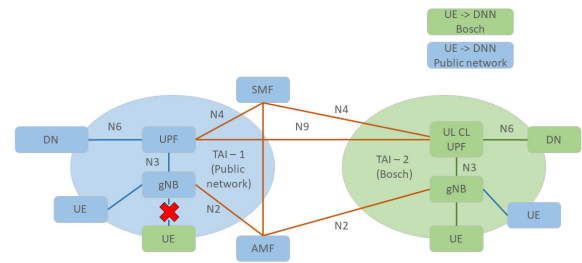

FIGURE 1. 5GAIner infrastructure.

deployment, providing a local breakout (LBO) User Plane Function (UPF) to address this requirement by design. The LBO UPF functions as an uplink classifier (UL CL) UPF, as shown in Figure 1.

The UL CL UPF controls any traffic crossing the 5G network and redirects it to the respective destination, while also providing isolation and restricting unauthorised communications. This functionality was complemented with a Local Area Data Network (LADN), a different tracking area (TA), and a different Data Network Name (DNN).

The LADN ensures that only industrial equipment has access to the Data Network (DN) at Bosch. Industrial equipment needs to access the network through the Bosch TA, accessing through the gNB at Bosch while using the Bosch DNN to gain access to the Bosch DN. If all these requirements are not fulfilled, the end device cannot access Bosch DN. Industrial equipment has no access to the public network, and cannot establish network connection in any other TA using the Bosch DNN. Public users can access the 5G network anywhere but can never communicate with the Bosch DN.

The infrastructure deployment at Bosch included 2 routers for redundancy, the MEC, and a RAN solution composed of 3 pRRUs to cover the production area of the factory. With this infrastructure and the MEC providing the LBO functionalities, it was assured that the industrial data plane was confined to the factory premises. As a result, no further assessment is required on this topic, and it can be concluded that the existing features in release 15 are sufficient to satisfy the industrial requirements.

2) NETWORK SLICING

To tackle this requirement, the system discussed in [22] would be necessary. However, at the moment, there is no available software that provides this network slicing. As an alternative, having different carriers with distinct communication performance was considered. However, this approach would be similar to using different technologies to implement each use case, with the technology choice based on the specific communication requirements. Therefore, it was realized that 5GAIner does not support any mechanisms of slice implementation from the beginning. Instead, the control of the slice is dependent on QoS flows, and like any R15 5G network, it is restricted to eMBB slices.

Since there are no integrated mechanisms for high-level slicing management, it was necessary to rely on QoS mechanisms to adjust the performance of each communication using the 5G network. The QoS mechanisms are based on channels, allowing the differentiation of each channel's performance. By configuring multiple channels, it is possible to have a specific communication service in each channel with distinct communication performance characteristics. However, these configurations need to be manually configured, and with the R15 network, they are limited to the configurability expected in an eMBB slice.

Therefore, even though the slicing that 5GAIner supports is limited to manual configurations, it was possible to implement end-to-end slicing in the network using the QoS mechanisms available. So in an R15 5G network is possible to support slicing, MEC, security, and isolation. Since QoS-based slicing is available in 5GAIner and verticals are highly interested in the configurability that can be obtained in a 5G slice. The rest of the document makes an analysis of the QoS mechanisms available in an R15 5G network.

IV. 5G QOS ENFORCEMENT MECHANISMS

In R15 [31] a network slice includes: Control Plane Functions and User Plane Network Functions in the network core, and for radio, it can include a New Generation Radio Access Network (NG-RAN) or a non-3GPP Access Network with N3IWF (Non-3GPP Interworking Function) functions. Each network slice is identified by a Single Network Slice Selection Assistance Information (S-NSSAI), which is composed of i) a Slice/Service Type (SST), which indicates the expected behaviour of the network slice concerning features and services; and ii) a Slice Differentiator (SD), which is optional and is used to differentiate multiple slices of the same SST.

Release 15 introduces the following standard SST values: 1, used for services requiring 5G enhanced Mobile Broadband (eMBB); 2, used for services requiring Ultra-Reliable Low Latency Communication (URLLC); and 3, used for services requiring Massive Internet of Things (MIoT). Each slice type focuses on a set of parameters, where eMBB is on throughput and network efficiency, URLLC is on latency and reliability, and MIoT is on connection density. These different types of slices will be essential for the deployment of the envisioned factory use cases, such as the ones presented in [32]. The requirements can be distinct, such as the synchronization of two machines, which requires a URLLC slice, and the application of predictive maintenance to machines, requiring a MIoT slice.

QoS is essential to define distinct communication characteristics for different services and eventually for different slices. This section briefly explains how the QoS process works in 5G. For a simplified understanding of the text, Table 1 presents the meaning of some abbreviations used, since there are various abbreviations and acronyms associated with 5G and QoS.

TABLE 1. Abbreviations.

5QI	5G QoS Identifier
AMBR	Aggregate Maximum Bit Rate
ARP	Allocation and Retention Priority
CDF	Cumulative Distribution Function
DSCP	Differentiated Services Code Point
DNN	Data Network Name
FAR	Forwarding Action Rule
GBR	Guaranteed Bit Rate
GFBR	Guaranteed Flow Bit Rate
MBR	Maximum Bit Rate
MDBV	Maximum Data Burst Volume
MFBR	Maximum Flow Bit Rate
PDB	Packet Delay Budget
PDF	Probability Distribution Function
PDR	Packet Detection Rule
PER	Packet Error Rate
QER	QoS Enforcement Rule
QFI	QoS Flow Identifier
QoS	Quality of Service
RQA	Reflective QoS Attribute
RQI	Reflective QoS Indication
SDF	Service Data Flow
SDU	Service Data Unit
S-NSSAI	Single Network Slice Selection Assistance Information
TOS	Type of Service
URR	Usage Reporting Rule

A. QOS MODEL

In terms of QoS, in release 15 [31], [33], the 5G QoS model is based on QoS Flows. Figure 2 demonstrates the components of a QoS Flow and the network functions affected by each component.
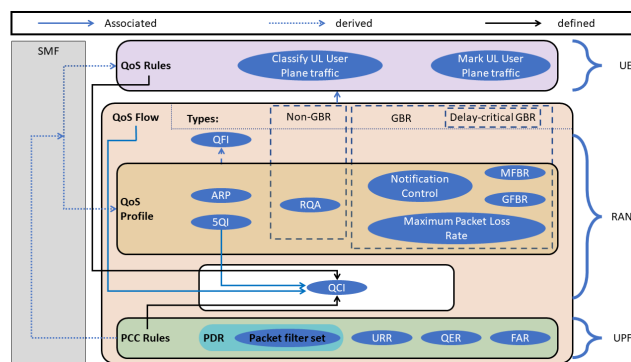

FIGURE 2. QoS model schematic.

5G supports the implementation of Non-Guaranteed Bit Rate QoS Flows (Non-GBR QoS Flows) and GBR QoS Flow, which can be a Delay-critical GBR QoS Flow. Each QoS Flow contains a PCC (Policy and Charging Control) rule and a QoS Profile. QoS Flows also have associated one or more QoS Rules.

PCC rules contain the information needed to detect packets in the user plane, apply policy control, QoS, and proper charging for a service data flow (SDF). The PCC rule has a Packet Detection Rule (PDR) for detection. The PDR contains a packet filter set with the information to identify

packets (for example, expected IP and source interface). As for the rest, PCC rules have the identification of the following rules to be enforced:

- QoS Enforcement Rule (QER) defines the bit rate limitations and QoS packet marking;
- Forwarding Action Rule (FAR) defines what to do with the packet if drop, forward or buffer them. It also defines packet encapsulation/decapsulation and the forwarding destination;
- Usage Reporting Rule (URR) defines how to count packets and report measurements to the control plane.

From the PCC rule, the SMF can derive the QoS profile, UPF (User Plane Function) instructions, and QoS rules. PCF provides additional information about the PCC rule.

The QoS Profile includes the components shown in Figure 2, which define the QoS parameters of the communication. In addition, the QoS profile is also associated with a QoS Flow Identifier (QFI).

Each QoS Flow is associated with one or more QoS Rules and a QoS Class Identifier (QCI). The QoS Rules define how the User Equipment (UE) classifies and marks UL User Plane traffic. While the QCI can be defined by the QoS Rule or PCC Rule, it can also be defined by the 5G QoS Identifier (5QI) in use, which is associated with a specific QCI.

QCI value is a scalar that is used as a reference for specific packet forwarding behaviour (e.g. packet loss rate and packet delay budget). Additionally, access network nodes use it as a reference for the parameter values used to control packet forwarding (e.g. scheduling weights, admission thresholds, queue management thresholds, and link layer protocol configurations). Operators are able to configure these parameter values on each access network node (e.g., gNodeB) to adjust communication performance.

Considering the protocol stack used by NG-RAN (composed of SDAP, PDCP, RLC, MAC, and PHY). MAC, RLC, and PDCP sub-layers have several features and services that are presented in [34]. Operators can use them to configure communication performance applying QoS Flow differentiation in the access network. The most relevant features and services are presented below.

- MAC Sub-layer
  - Priority handling between UEs using dynamic scheduling;
  - Priority handling between logical channels of one UE using logical channel prioritization;
- RLC Sub-layer
  - Transmission mode: with (AM) or without (UM) Acknowledgement
  - Sequence numbering independent of the one in PDCP (UM and AM);
  - Reassembly of SDU (AM and UM);
- PDCP Sub-layer
  - Maintenance of PDCP SNs;
  - Timer-based SDU discard;
  - Reordering and in-order delivery;

Besides the RAN configurable protocol services and features, 3GPP has standardized some QoS features in release 15 5G network [31] which are presented in Table 2.

B. QOS CONFIGURATIONS

Figure 3 demonstrates a schematic representing where and how to configure QoS settings. The configurations of a QoS Flow can be static or dynamic. The **static** configuration types are:

- **Pre-configured** is the configuration of QoS rules, QoS profiles, and PCC rules on the specific device before communications. Most devices come with some pre-configurations already. In RAN comes pre-configured 5QI or QFI mapped to the standardized QoS characteristics, which are given in Table 5.7.4-1 of [31]. In UPF comes a basic PCC Rule pre-configured just for forwarding packets without QoS enforcement.
- **Subscription values**, which define the default Non-GBR QoS Flow of all devices that can access the network. These configurations are done in UDM.
- **Predefined PCC Rule** is configured in the network and cannot be modified at run-time. This can be configured in PCF, or configured in the SMF and UPF.

QoS rules can be delivered by SMF, pre-configured, or derived by the UE using Reflective QoS (explained in Table 2). In the case of **dynamic** configurations, these rules can be changed even during service transmission, but can only be enforced and modified by PCF.
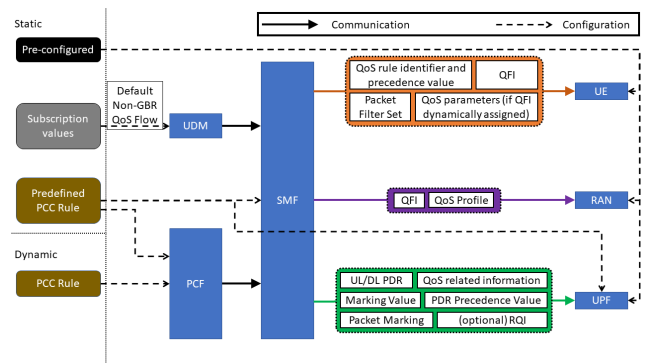

FIGURE 3. Configuration schematic of a QoS Flow.

SMF (Session Management Function) can configure a PDU (Protocol Data Unit) Session in these ways:

- Using default **subscription values** retrieved from the UDM (subscription values provide the default Non-GBR QoS Flow that UEs use to connect to the network and transmit data), which needs to have an ARP value and a Standardized Non-GBR 5QI value;
- Or using a **PCC rule**, in which the SMF assigns a QFI and uses a PCC (Policy and Charging Control) rule, binding them to the QoS Flow. This binding is based on QoS and service requirements. These rules can be configured in **SMF and UPF** or in **PCF**, which then sends the necessary PCC rule information to the SMF.

TABLE 2. 5G QoS parameters.

Parameter Name		Parameter Description
Generic QoS Flow parameters		
5QI		5QI is a scalar used as a reference for 5G QoS characteristics. It is associated with the value of the packet delay budget, priority level, packet error rate, and other communication parameters. In R15 and later releases, exists some standardized 5QI values, which have specific values for QoS parameters that are pre-configured in the AN.
Packet Filter Set		QoS rules and PDR use Packet Filter Set to identify the packets that belong to a QoS flow. The packet filter set contains one or more filters that can be applied in UL, DL, or both directions. These filters can be IP or Ethernet filters. For example, IPv4 filters can identify packets with any combination of source/destination IP address, source/destination port number, next header type, Type of Service (TOS), Security parameter index, and filter direction.
Precedence Value		Defines the order in which the QoS Rule and PDR are applied. Smaller values have higher priority.
QoS Flow type	Non-GBR	This is a common communication flow. This type of QoS Flow can be authorized with static configurations.
	GBR	Ensures throughput in communication. This QoS flow needs to be authorized "on demand". This requires a dynamic configuration of policies and charging control.
	Delay-critical GBR	Ensures communication throughput and requires dynamic configuration. But in this case, the PDB and PER values have different meanings. In addition, it has MDBV, which is a parameter that applies only to this type of QoS flow.
Priority Level		Priority level is linked to the 5G QoS characteristics defining the scheduling priority of resources between the different QoS Flows. Where smaller values have higher priority. In case of congestion, when all QoS requirements cannot be met, the priority level defines the transmission priority of QoS Flows. In case of no congestion, the priority level defines the distribution of resources among the QoS Flows.
Packet Delay Budget (PDB)		Defines the upper bound latency value between the UE and the last UPF in the communication. The packets that arrive after the PDB value count as lost in delay-critical GBR QoS Flows. In GBR QoS Flows, 98% of packets that do not exceed GFBR should have a delay below the PDB. And in the case of Non-GBR QoS Flows, 98% of packets should have a delay below PDB when the network is not congested. PDB in R15 is defined in RAN and may or may not include the value of CN PDB.
Packet Error Rate (PER)		Defines the upper limit of packets lost in transmission. In Non-GBR QoS Flows, this value only takes effect when the network is not congested. For GBR QoS Flows, PER takes effect on packets that do not exceed the GFBR value. For the delay-critical GBR QoS Flows, if the burst is less than MDBV and the packets do not exceed the GFBR value, the packets with a delay above the PDB count as lost and added to the PER value.
Non-GBR QoS Flow parameters		
AMBR	Session-AMBR	Limits the total bit rate of all Non-GBR QoS Flows for each UE PDU Session. Session-AMBR is controlled in UE, (R)AN, and UPF.
	UE-AMBR	Limits the total bit rate of all Non-GBR QoS Flows in a UE. Thus, the aggregate bit rate of all PDU sessions of Non-GBR QoS Flows in a UE cannot surpass the value of UE-AMBR. UE-AMBR is enforced by (R)AN.
Reflective QoS Attribute (RQA)		Specifies whether certain (not necessarily all) traffic carried from a specific QoS Flow is subject to Reflective QoS. When RQA is enabled, (R)AN informs the UE that AN resources have reflective QoS enabled using RQI (Reflective QoS Indication). Reflective QoS allows the UE to link UL User Plane traffic to the QoS Flow without QoS Rules from the SMF. For this, UE uses DL traffic to derive QoS rules (only possible for Non-GBR QoS Flows), which reduces the control traffic required between the UE and the network. Since the network does not need to send all QoS rules for UL traffic to the UE. The derived QoS rule contains QFI, Precedence Value, and a UL Packet Filter.
GBR QoS Flow parameters		
Allocation and Retention Priority (ARP)	Priority level	Defines the importance of a QoS flow when requesting resources. It is used for admission control of GBR QoS Flows. It helps in the decision of resource allocation for new QoS Flow, deciding the preempted QoS Flow when there is a resource shortage. Preemption only happens if preemption capability and vulnerability are enabled for the QoS Flows. The priority level values range from 1 to 15, with 1 being the highest priority.
	Preemption capability	Decides whether new data flows can obtain resources already assigned to other flows.
	Preemption vulnerability	Defines if the data flow can lose assigned resources, to admit a new data flow with higher priority. Preemption capability and vulnerability can be set to 'enabled' or 'disabled'.
Notification Control		Defines if RAN needs to notify the core (SMF and PCF) when the transmission conditions change. This can happen when RAN cannot ensure the guaranteed bit rate required or when it can ensure the guaranteed rate again. AF or NEF can use this information to adapt communication requirements to the transmission conditions.
Guaranteed Flow Bit Rate (GFBR)		Defines the flow guaranteed bit rate during the time of an Averaging Window.
Maximum Flow Bit Rate (MFBR)		Defines the highest bit rate expected by the QoS flow. Where excess traffic has no QoS guarantee. Thus, packets that exceed the MFBR value are subject to higher latency than defined in the PDB of QoS flow or can be dropped. Traffic between GFBR and MFBR values is transmitted depending on the QoS priority of the flow concerning the other flows using the network. UE and (R)AN enforces MFBR in UL and UPF and (R)AN enforces in DL.
Maximum Packet Loss Rate		Specifies the maximum percentage of packets lost for voice media GBR QoS flows. It takes effect when packets do not exceed the GFBR value.
Averaging Window		Defines the duration over which the GFBR and MFBR are calculated.
Delay-critical GBR QoS Flow parameters		
Maximum Data Burst Volume (MDBV)		MDBV defines the maximum burst that AN needs to be able to transmit within the period of a 5G-AN PDB.

In a PDU session establishment with a PCC rule the SMF sends i) the PCC rule identification to UPF, where the other instructions are configured, or all required information in case the rule is configured in PCF; ii) the QoS Profile to RAN; and iii) the QoS rule to UE, if reflective QoS is disabled; if reflective QoS is active, UE derives the QoS rule from the downlink flow.

Figure 3 presents a more complete list of all information that SMF can send. Where the information for UPF contains: i) QoS-related information, which can be MBR, GFBR, and MFBR for a GBR QoS Flow; ii) the marking value, which can be QFI; and iii) packet marking, which can be the DSCP value.

C. QOS ENFORCING

Figure 4 demonstrates a schematic representing how is the marking and mapping of QoS Flow packets, which is explained next.

In **DL transmission**, the UPF performs the following actions: i) traffic mapping of QoS Flows using PDRs; ii) Session-AMBR (Aggregate Maximum Bit Rate) enforcement; iii) packet marking using SMF QoS Flow indications; iv) packet forwarding through a tunnel belonging to the PDU Session, with the QFI and RQA (if enabled) in the tunnel encapsulation header. The (R)AN maps QoS Flow packets to specific AN resources, based on: QFI, associated 5G QoS profile, and N3 tunnel used by the packet. The UE
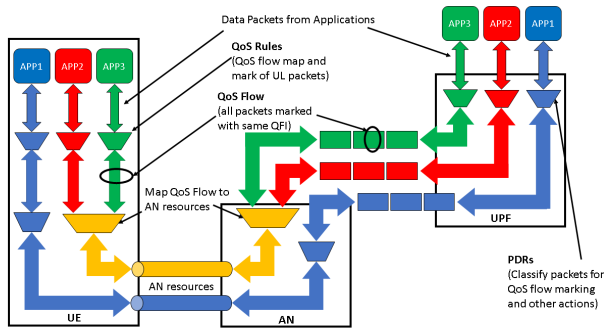
FIGURE 4. Schematic of QoS Flow classification and User Plane marking and AN resources mapping.

creates a new derived QoS rule in case of Reflective QoS is active.

In **UL transmissions**, the UE performs the following actions: i) maps the UL User Plane traffic to the QoS flows based on the QoS rules; ii) marks the packets with the QFI of the matching rule; iii) enforces the Session-AMBR; and iv) transmits packets using AN resources based on the provided (R)AN mapping. (R)AN executes as follows: i) forwards packets through the N3 tunnel to the Core Network (CN); ii) places the QFI value in the encapsulation header; and iii) marks UL packets based on: QoS Flow 5QI, priority level, and ARP priority. The UPF checks that the QFIs in packets are correct and enforces Session-AMBR.

V. EXPERIMENTATION OF QOS FEATURES IN REAL-LIFE
To test and validate several of the 5G QoS features presented above, the industrial 5G network which is a real-world 5G infrastructure based on a commercial SA implementation introduced in Section III is further presented in the following subsection. The rest of this section presents the validation scenario and the QoS parameters to be validated.

A. INDUSTRIAL NETWORK
The industrial network infrastructure is deployed over several sites as presented in Figure 1, having the core in the Instituto de Telecomunicações (IT) of Aveiro. IT and its project partners use this infrastructure to develop, test, and validate 5G technologies. The control network functions of the infrastructure at the moment are SMF, AMF, AUSF, NRF, NSSF, and UDM. Being these NFs the minimum necessary for supporting the development, testing, and deployment of all industrial use cases envisioned to be deployed in the network, while ensuring its good functionality. The baseline quantitative performance data of this deployment is provided in [30].

But, when experimenting with the network functionalities it was noticed that is particularly hard to: i) use end-to-end GBR QoS Flows. ii) and configure the Packet Error Rate of a QoS Flow. These restrictions are due to the specific implementation details of the 5G network. Even so, with this infrastructure is possible to evaluate most of the

network functionalities and understand their impact in a real network.

The current release of the network used is R15, which is the last release widely available at the moment. So it is necessary to recall that release 15 only supports eMBB slices, not supporting URLLC and MIoT slices and their features. So most of the functionalities focus more on controlling bandwidth than other parameters. Nevertheless, the industrial 5G network is a representation of what today's commercial infrastructure is, and this network is expected to be improved over time, receiving new features, network functions, and releases.

This network is owned by a research institute in Portugal, and the spectrum used in the infrastructure is a reserved band of an operator, Altice. Table 3 presents the antenna configurations used during the tests. These values can be used to understand the limitations and maximum values presented in the tests.

TABLE 3. gNodeB technical specifications.

Specification	Values
Maximum bandwidth	20 MHz with 30kHz subcarrier spacing
Frequency band	Center frequency of 3790.02 MHz (n78 band)
Output power per port	24 dBm
Demultiplexing	TDD
DL Modulation	BPSK; QPSK; 16/64/256QAM
UL Modulation	BPSK; QPSK; 16/64QAM
MIMO	4T4R
Network Slicing	eMBB Slices
Slot assignment	4 Downlink: 1 Uplink (Slot structure 2)

B. QOS PARAMETER CONFIGURATION
In the industrial 5G network is possible to configure several of the QoS parameters presented in Section V. This subsection presents how to configure the evaluated parameters. This information is necessary to fully understand the impact of each QoS parameter.

Scheduling priority and Guaranteed Rate are MAC protocol parameters. MAC configurations have a MAC parameter group ID, which is an integer used to identify a specific MAC configuration. This MAC parameter group ID is then associated with a QCI value. Averaging Window, Priority Level, and Packet Delay Budget are directly associated with a QCI value. In gNB, there is a mapping between QCI and 5QI values. The 5QI is associated with a UE in the UDM using subscription parameters.

MFBR parameter is configured in a PCC rule in UPF. This PCC rule is associated with a specific DNN (Data Network Name) and a specific UE. Therefore, the PCC rule is only enabled when the specified UE is using the defined DNN. In addition, this rule has a packet filter set associated with it, making it possible to associate the rule with a specific communication.

DNN-AMBR is set on UDM using a DNN QoS template. This template is a UE subscription value that is associated with a specific DNN and slice. UE-AMBR is a UE

subscription value defined in the UDM, which needs to be set before UE connects to the network.

DSCP can be configured by a remark rule, a QoS profile, and a gNB.

- The remark rule is a rule available in the network which is similar to the PCC rule in terms of configuration, but in this case, defines the value of DSCP or TOS of the packets. So, it can be linked to a specific UE, DNN, and/or filter. And marks the packets with the defined DSCP value when they leave UPF.
- A QoS profile can be configured in the SMF and can be a global QoS profile associated with all DNNs, or a specific profile associated with each DNN. The QoS profile maps a specific set of 5QI and ARP Priority levels to a specific DSCP behaviour. The configured DSCP value can be different for each 5G interface (N3, N6, and N9). The 5QI and ARP values are subscription parameters configured in the UDM for each UE.
- The gNB uses the User Data Type (UDT) Number to define the DSCP value of the packets, the UDT number is equal to the 5QI value used in communication. Each user data type number has a specific DSCP value associated with it, which is the value marked on the packets when they leave the RAN.

C. VALIDATION

Taking into consideration the features above, the functionalities of the following QoS parameters were selected for validation.

- Scheduling Priority Weight Factor;
- Guaranteed Rate in RAN;
- Averaging Window;
- Priority Level;
- Packet Delay Budget (PDB);
- Maximum Flow Bit Rate (MFBR);
- DNN-AMBR
- UE-AMBR;
- DSCP;

These QoS parameters are validated in a real-world deployment scenario presented in Figure 5 using industrial 5G infrastructure.

The tools used in the tests are iperf3,[9] simple python scripts, and 5G network metrics. Iperf3 is used for throughput tests and to generate traffic interference. The Python scripts can have a ping-like functionality or just send UDP packets. 5G network metrics are the metrics recorded by the 5G network.

All tests, unless specifically specified, are performed on the downlink. Therefore, the iperf3 commands are configured as reverse so that the transmission is on the downlink. The UEs used are Huawei 5G CPE pro 2 connected through ethernet to single-board computers that run the software. During the entire test, the UEs are static, indoor with line-of-sight, and within a 10-meter range of the antenna.
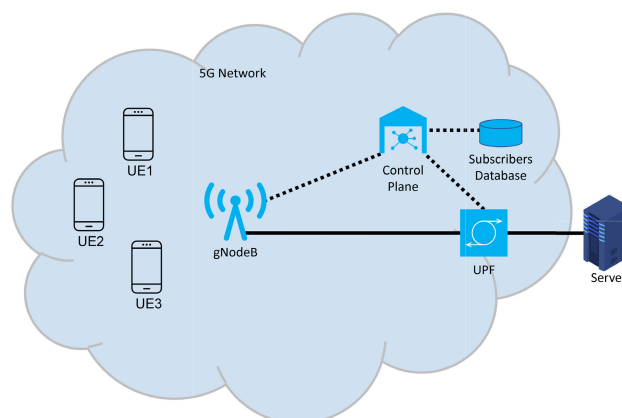
[9]Iperf3, https://iperf.fr/ (July 2022)

FIGURE 5. Validation scenario.

1) THROUGHPUT VALIDATION

In throughput validation scenarios iperf3 was used to generate data, except for the minimum throughput tests, where iperf3 didn't work adequately. In these situations, a simple Python script was used. Validation data were obtained with the 5G metrics, which provide throughput on the RAN at the RLC layer, which includes some overhead. When using iperf3, the server in Figure 5 has all the iperf3 servers, and the UEs work as iperf3 clients.

In the minimum value tests, it was used a simple Python script to send UDP packets, where we can adjust the data in each packet and the packets per second.

2) PACKET LOSS VALIDATION

The Packet loss validation scenario is similar to the throughput validation scenario, but the metrics are obtained with iperf3 in this case. For this purpose, iperf3 was configured with UDP, which gives the number of packets lost and packets sent in the transmission, used to calculate the packet loss percentage in the transmission during the test.

3) RTT VALIDATION

In RTT (Round-Trip Time) validation scenarios, a Python script with a ping-like functionality using UDP packets is used. Where the UE sends a packet, the server returns it, and the UE calculates the time between sending and receiving the packet, obtaining the RTT value.

The validations are performed on both an empty cell and a loaded cell. In the case of the loaded cell, two UEs are used with the basic configuration, which uses the standard configuration of 5QI value 9. These two UEs are using the entire bandwidth, where one uses the entire uplink bandwidth and the other uses the entire downlink bandwidth.

VI. EXPERIMENTAL RESULTS

This section describes the tests performed to validate each of the QoS parameters, presenting the results obtained and discussing the effects of each parameter. All tests were run

multiple times, but the results provided were of a single run as the results were usually consistent.

A. SCHEDULING PRIORITY

The Scheduling Priority Weight Factor is a MAC sub-layer parameter configured in each gNodeB, and the values vary between 1 and 1000. Three UEs were configured with different scheduling priorities to demonstrate this parameter's functionality. The Scheduling Priority Weight Factor values used for the UEs are (1) UE1 with low priority having 250; (2) UE2 with medium priority having 500; (3) UE3 with high priority having 1000. Each UE tries to use the maximum possible bandwidth for 540 seconds in the test. The test starts with UE1, 180 seconds later UE2 begins transmission, and 180 seconds later UE3 starts transmitting.

Figure 6 shows the results obtained for all UEs with different scheduling priorities (SchPr). UE1 can use all the bandwidth available at the antenna in the first three minutes. After three minutes, UE2 starts transmitting using around two-thirds of the bandwidth; while UE1 uses the other third.
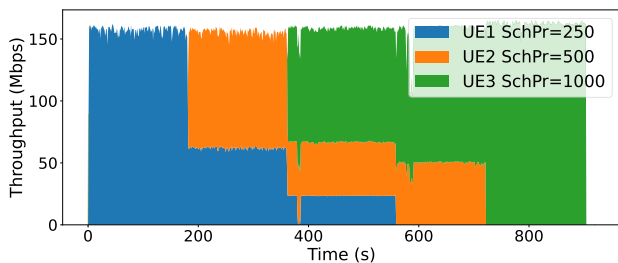

FIGURE 6. Throughput of three UEs with different scheduling priority (SchPr).

In the next three minutes, UE3 starts transmitting and utilizes approximately four-sevenths of the bandwidth; while UE2 uses around two-sevenths; and UE1 uses approximately one-seventh of the available bandwidth. Following this, in the subsequent three minutes, UE1 ceases transmission, allowing UE3 to utilize about two-thirds of the bandwidth, while UE2 utilizes around one-third. In the final three minutes, only UE3 transmits and uses all the bandwidth.

As seen in the results, the value of the scheduling priority weight factor defines the bandwidth distribution. Therefore, when only one UE is transmitting it uses all the bandwidth, regardless of its scheduling priority. When multiple UEs are transmitting at the same time, the bandwidth fraction allocated to each UE can be calculated with:

$$\frac{UE\ scheduling\ priority}{Sum\ of\ Scheduling\ priority\ of\ all\ UEs\ transmitting}$$

So, in the case of two UEs transmitting, 250/(250+500) = 1/3. Therefore, in the scenarios where two UEs are transmitting, around one-third of the bandwidth goes for the lowest priority UE, while the other gets the rest of the bandwidth.

In the case of three UEs transmitting, the same rule is applied, but in this case, the bandwidth is divided into seven parts. UE1 is allocated one part, UE2 receives two parts, and UE3 gets four parts of the bandwidth. Therefore, the Scheduling priority Weight Factor allows prioritizing the transmission of certain UEs over others for each gNB.

Other tests were conducted to determine if different scheduling priority values affect the time it takes for the network to provide full bandwidth to a UE, both when the antenna is free and when it has a load of 80 Mbps. Throughput values were measured every 100 ms, but no significant difference was observed in the time it takes to provide maximum bandwidth to a UE, regardless of its Scheduling Priority value.

B. GUARANTEED RATE

The Guaranteed Rate in RAN is a MAC sub-layer parameter configurable on each gNodeB. The Guaranteed Rate can ensure throughput in communication. To demonstrate the functionality of this parameter, three UEs are used: UE1 with 1 Scheduling Priority and 2 Mbps Guaranteed Rate; UE2 with 1 Scheduling Priority and no Guaranteed Rate; and UE3 with 1000 Scheduling priority.

UE1 demonstrates the functionality of the tested QoS parameter. UE2 works as a term of comparison between a UE with and without a Guaranteed Rate. UE3 generates traffic noise to simulate network congestion, while the high Scheduling priority value used in this UE simulates a scenario with many UEs connected and using the network.

In this test, UE1 and UE2 start an iperf3 transmission with 5Mbps throughput, and then UE3 starts an iperf3 transmission using all the bandwidth it can. The test has a total duration of 320 seconds and the throughput of UE1 and UE2 are recorded. Figure 7 demonstrates the results obtained.
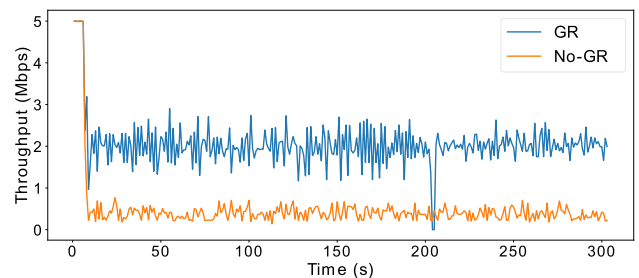

FIGURE 7. Throughput of two UEs where one has a Guaranteed Rate (GR) of 2Mbps with 2 seconds average window and the other without guaranteed rate (No-GR).

As seen from the results obtained in the first 20 seconds, both UEs have a transmission of 5 Mbps. Then, when UE3 starts its transmission, causes a throughput drop in both UEs. Where UE1 (GR) maintains a throughput of around 2 Mbps due to the Guaranteed Rate (GR), while UE2 (No-GR) throughput drops to around 400 Kbps. By analyzing the results obtained, we concluded that by using the Guaranteed Rate, one can ensure that a UE has a minimum throughput value even when the network is congested. This can ensure

the communication of critical services as long as the network is functioning properly.

It was also verified that the Guaranteed Rate does not have a maximum value. It was possible to ensure 140 Mbps of Guaranteed Rate to a UE when two UEs were transmitting and the maximum bandwidth of the antenna is around 160 Mbps. The Guaranteed Rate (GR) granularity was tested, and although the value can be set to a granularity of 1 Kbps, the results shown in Figure 8 present that a difference lower than 100 Kbps does not present a clear distinction in the throughput.
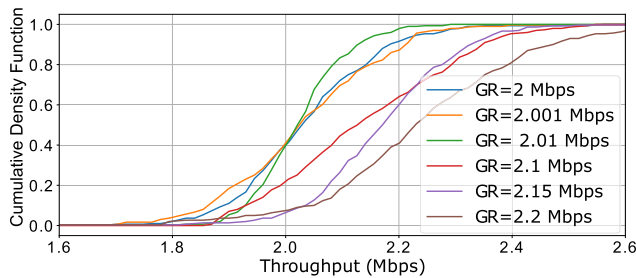
FIGURE 8. Cumulative distribution function of guaranteed rate (GR) granularity test.

C. AVERAGING WINDOW

For the validation of Averaging Window functionality, three UEs were used: (i) UE1 with 1 Scheduling priority, 2 Mbps Guaranteed Rate, and 4095 ms Averaging window; (ii) UE2 with 1 Scheduling priority, 2 Mbps Guaranteed Rate, and 100 ms Averaging window; (iii) UE3 with 1000 Scheduling priority.

The possible Averaging Window value to configure ranges from 0 to 4095 ms. Therefore, the first two UEs will show the difference between high and low Averaging Window values. Since the Averaging Window is used to define the time window for counting the throughput of the UE, to show the effect it is necessary to use this count. Therefore, the Guaranteed Rate is set to use this count. The Scheduling priority is set to simulate a large number of users connected to the network, as in the previous scenario.

The test to validate the effect was conducted for 300 seconds, where all UEs were transmitting simultaneously. UE1 and UE2 try to transmit 5Mbps with iperf3, while UE3 aims to transmit as much as possible. Only the throughput values of UE1 and UE2 were recorded. Figure 9 demonstrates the results over time and the cumulative distribution functions (CDFs) obtained for both UEs with different averaging windows (AW) values.

As seen in the figure, UE2 is much more likely to achieve a throughput of 2 Mbps compared to UE1, and the throughput values for UE2 are less spread out. Most of UE2's throughput values range from 0 to 5 Mbps, while for UE1 the throughput values range from 0 Mbps to 7 Mbps.

Consequently, a lower value of the Averaging Window value can provide a more stable throughput when enforcing
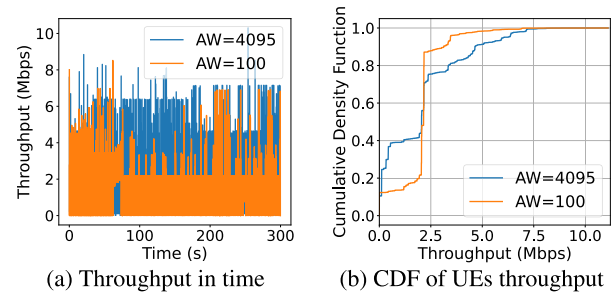

(a) Throughput in time   (b) CDF of UEs throughput

FIGURE 9. Two UEs with a guaranteed rate of 2Mbps and averaging window (AW) of 4095 and 100.

GBR or MBR values. On the other hand, a higher value ensures that the average throughput aligns with the GBR and MBR values, but the instantaneous throughput value can exhibit more variation.

D. PRIORITY LEVEL

Several tests were performed to verify the impact of the priority level value. It was found that the priority level does not significantly affect throughput and latency to a noticeable extent. However, the packet loss percentage of a transmission on a free and loaded cell was evaluated to determine if this parameter affects it. The validation measured the number of packets lost and the total of packets sent every 30 minutes throughout a full day for each value of priority level.

The UE under measurement was receiving 10 Mbps per second from the server using iperf3. Iperf3 records the number of packets lost and the number of packets sent per second, which were later converted to a 30-minute interval to generate the graphics.

In the loaded cell case, one UE is using all the available downlink bandwidth, and both UEs have the same Scheduling Priority Weight Factor. Thus, the maximum value that the UE measuring could receive is around 80 Mbps. Since the measured throughput of 10 Mbps is below the maximum value, it does not influence the packets lost.

With the obtained values, the packet loss of each 30 min interval during the transmission was calculated. The results are shown in Figure 10, with different priority (Pr) values. The results reveal that the packet loss in the free cell is lower than in a loaded cell. However, maybe surprisingly, there is no significant difference in the results obtained for the different priority level values.

E. PACKET DELAY BUDGET

PDB defines the maximum latency of communication. To validate the PDB, two separate tests were performed: a 15-minute test in a loaded cell and another 15-minute test in an empty cell. These tests were performed for several PDB values. The results obtained are presented in Figure 11.

The values of each line in the graphs are the PDB values configured on the network. The PDB values range from 0 to 1023, having a unit value of 0.5 ms, so the
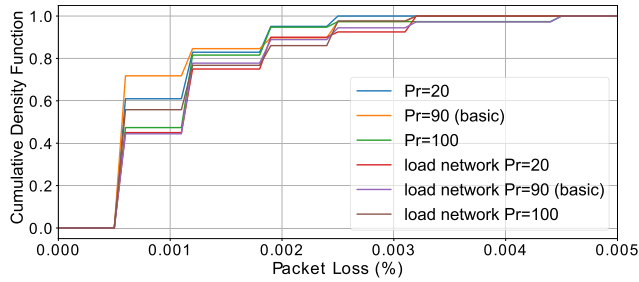
FIGURE 10. Packet loss of transmission for different priorities (Pr).
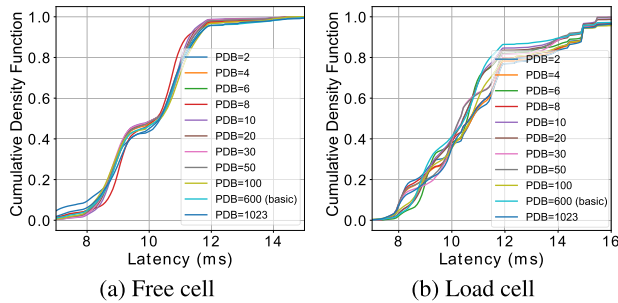

(a) Free cell   (b) Load cell

FIGURE 11. RTT for different values of PDB.

actual value range is from 0 to 601.5 ms. As referred in Table 2, the PDB in Non-GBR QoS Flows only ensures that 98% of packets have a latency lower than the specified value in non-congested scenarios. The real impact of this parameter becomes noticeable for the 5-10% of packets with higher latency. Figure 12 demonstrates the probability of packets with higher latency for each PDB value.

(a) Free cell   (b) Load cell
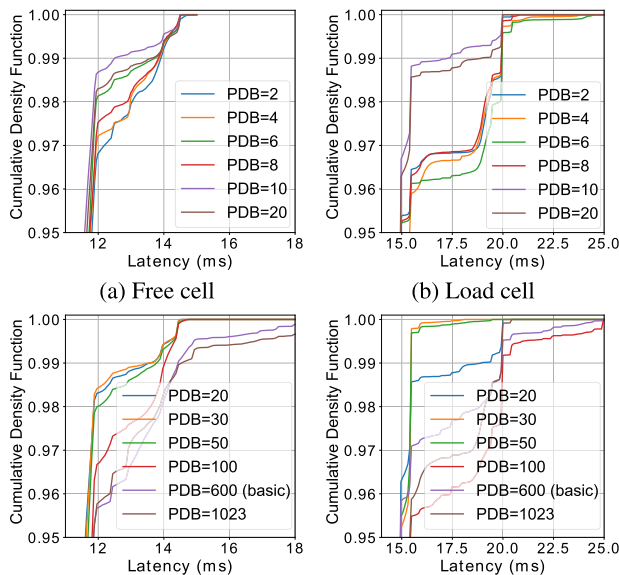
FIGURE 12. Zoom of CDF of RTT for different PDB values.

From the figure, it is possible to see that for PDB values below 10, the algorithms of the infrastructure used

do not perform correctly. For values above 10 to 30, the infrastructure can provide better performance. However, it is only from 30 (15 ms) onward that an increase in the packet latency can be noticed as the PDB values increase.

F. MFBR

MFBR can be configured for GBR QoS Flows, limiting the maximum throughput that a UE can transmit in each QoS Flow. To demonstrate the impact of MFBR on communication, only one UE was used sending all data through a single QoS Flow. This UE was configured to transmit for 600 seconds and try to use as much bandwidth as possible. Since we can dynamically change the MFBR value during a UE transmission, 180 seconds and 360 seconds after the start of the UE transmission, the MFBR value is changed. The MFBR value started with 2 Mbps, changed to 3 Mbps, and then to 1 Mbps. Figure 13a presents the results obtained in the test.
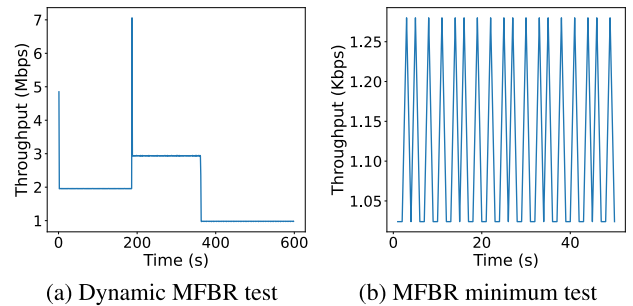

(a) Dynamic MFBR test   (b) MFBR minimum test

FIGURE 13. Show the throughput of a UE while it is bounded with MFBR.

As can be seen from the results obtained, the value of MFBR limits the UE throughput, and there is a low variation in throughput when MFBR is constant. In the results exists two peaks demonstrating that UE tries to transmit more than the network allows, being limited right after.

MFBR can be used to limit the throughput of a UE or a particular communication using filters, this can ensure that high-priority communications do not use more bandwidth than is necessary for a given QoS level agreed, leaving more bandwidth for lower-priority communications.

The minimum value and granularity of MFBR were also tested. Figure 13b presents the results of the minimum value test and can be seen that MFBR can limit throughput to its minimum value. The results are above 1 Kbps due to the measures considering higher-layer protocol overhead. The oscillation is caused by the average window, which has a value of 2 seconds, so the limit algorithm reduces the throughput every 2 seconds to ensure 1Kbps of user plane data.

In the granularity test, although the value can be set to a granularity of 1 Kbps, the results shown in Figure 14 present that small increments below 0.5% from the value used becomes difficult to differentiate.
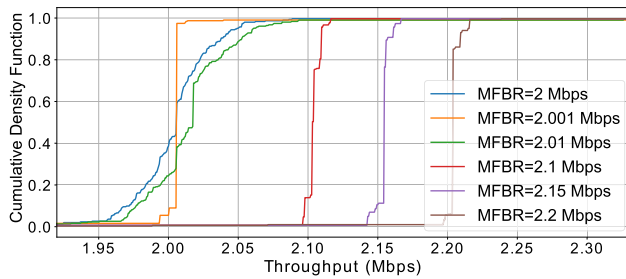
FIGURE 14. MFBR granularity test.

(a) CDF of granularity test

(b) Minimum test

FIGURE 16. AMBR granularity and minimum test.

G. AMBR

Since there are two different AMBR values, we decided to validate the AMBR functionalities and constraints as a generic AMBR parameter, and then differentiate the effect of each AMBR parameter. AMBR in this situation defines the maximum bandwidth of the aggregate throughput of all Non-GBR QoS Flows of a single UE. To validate the effect of AMBR on communication, a UE with 10 Mbps of AMBR was used. This UE was configured to transmit for 300 seconds as much throughput as possible. The results obtained can be seen in Figure 15.
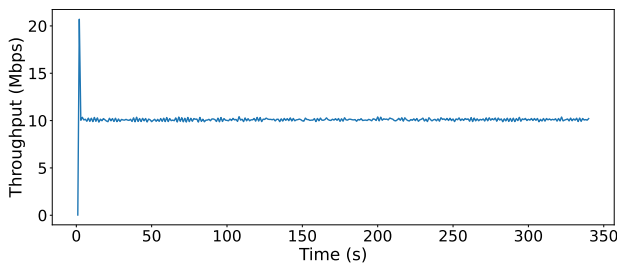

FIGURE 15. Throughput of a UE with 10Mbps of AMBR.

As observed at the beginning of the test, the UE attempts to transmit data at a rate exceeding the AMBR value, but the network promptly restricts the UE's throughput to adhere to the specified limit. Consequently, the UE's throughput remains close to 10 Mbps throughout the test duration.

This parameter has the same functionality as MFBR, limiting throughput. However, while MFBR restricts the maximum throughput of a GBR QoS Flow, the AMBR parameters limit the throughput of all Non-GBR QoS Flows. This ensures that situations like those observed in the Guaranteed Rate and Averaging Window validation scenarios do not occur, where one UE generating communication noise uses more than 99% of the total antenna bandwidth, leaving other UEs without Guaranteed Rate with less than 1 Mbps of throughput to use.

The granularity and minimum value of AMBR were also tested. In the granularity test, even though the value can be defined to a granularity of 1 bps, the results shown in Figure 16 demonstrate that a difference of lower than 100 Kbps from the value used becomes difficult to differentiate.
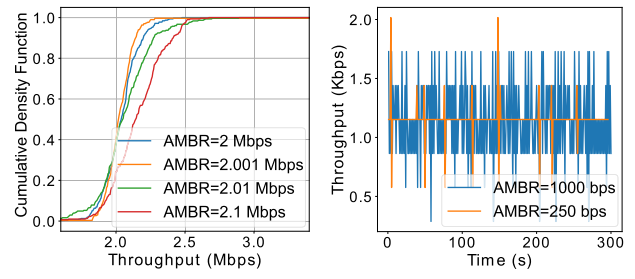
Figure 16b demonstrates the results of the minimum value test, where for values less than 1 Kbps the network is unable to limit throughput to the defined value.

H. DNN AMBR AND UE AMBR

To validate DNN and UE AMBR two PDU sessions in the same UE are necessary at the same time. DNN-AMBR is equivalent to the Session-AMBR in the standards and should limit the throughput of each session separately. UE-AMBR is expected to limit the throughput sum of both sessions. In validation, a single UE connects to two DNNs and, using iperf3, tries to transmit the maximum bandwidth through both DNNs. In both tests, the UE starts transmitting the maximum bandwidth possible through DNN1, and 30 seconds later starts transmitting the maximum bandwidth possible through DNN2. Then DNN1 ceases transmission and DNN2 continues sending for some more time.

To validate DNN AMBR, DNN1 has an AMBR value of 5 Mbps, while DNN2 has a value of 15 Mbps. Figure 17 shows the results obtained. From the results in Figure 17a, it can be seen that the outcome is different than expected. It was expected that DNN1 have a 5 Mbps limit and DNN2 have a 15 Mbps limit all the time. But instead, DNN1 has a 5 Mbps limit when DNN2 is not transmitting. When DNN2 starts transmitting, the maximum bandwidth changes to the sum of both AMBRs and the bandwidth is divided by both PDU sessions equally. Then, when DNN1 ceases transmission, DNN2 keeps the maximum bandwidth at the sum of both AMBR values.
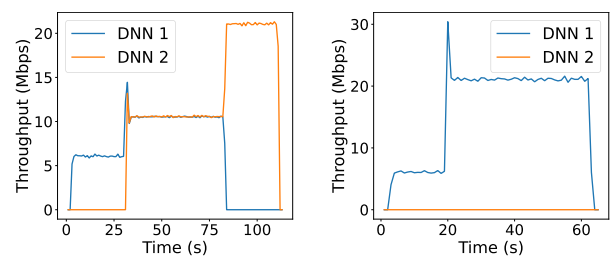

(a) Both sessions transmitting

(b) One session transmitting

FIGURE 17. Throughput of a single UE with two sessions in different DNNs with distinct DNN AMBR.

Figure 17b demonstrates the effect of adding both AMBR values without DNN2 using significant bandwidth. In this case, DNN1 starts transmitting the maximum bandwidth possible and is limited by the DNN AMBR value of 5 Mbps, but when DNN2 sends the periodic packets to keep the session alive, the maximum bandwidth changes to the sum of the DNN AMBR of both sessions. This is an artefact of the specific implementation not compliant with the standards.

To validate UE AMBR, the value was set to 10 Mbps. Figure 18 demonstrates the results obtained. As expected, when only one DNN is transmitting, it uses the maximum bandwidth allowed by the UE AMBR value. However, by the time both DNNs are transmitting, the bandwidth is equally divided by both sessions, while keeping the sum at the UE AMBR value.
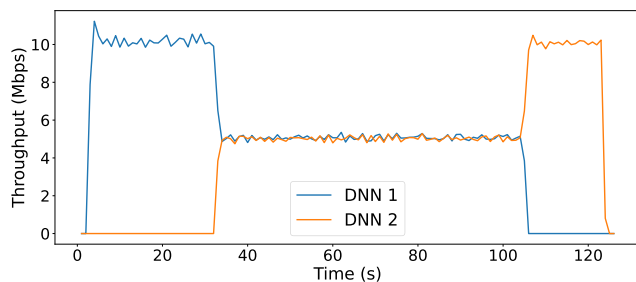

FIGURE 18. Throughput of a single UE with two sessions in different DNNs limited by UE AMBR.

I. DSCP

DSCP is a field [35] in an IP packet that classifies traffic, allowing the transport network to ensure a specific quality of service level. DSCP has several standardized values explained in [36] that are intended to provide specific QoS levels in communication. Some of the DSCP values are BE (Best-effort or Default Forwarding [DF]), AF (Assured Forwarding), and EF (Expedited Forwarding).

The DSCP value of communication in industrial 5G infrastructure can be defined in UPF and RAN. This configuration enforces a specific DSCP value on any packet for which the configuration is applied. To validate the impact of DSCP value on network configurations, a test was performed with various values. The RTT was measured for 15 minutes when the network had no traffic, and for another 15 minutes when the network had the maximum traffic load that a single cell could handle.

Figure 19 demonstrates the results obtained. As can be seen, there is no major difference in performance in a free cell. When the used cell is loaded, a slight difference in RTT can be noticed for the values AF21 and AF31. This makes sense since AF21 is designed for low latency and AF31 is designed for multimedia streaming, and both services require low latency.

As the transport network is not fully loaded, the results obtained do not present the actual impact of the DSCP values. However, it already demonstrates the impact in terms of RTT that each DSCP value has.
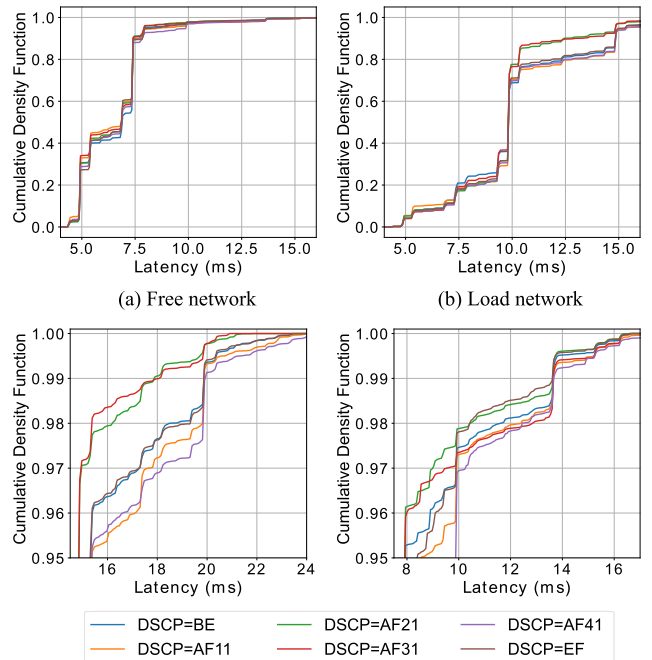

FIGURE 19. RTT for different DSCP values. Bottom images are a zoom of the top images.

VII. DISCUSSION

The different projects had a close collaboration with the industry, enabling a comprehensive understanding of their requirements and concerns regarding the integration of this emerging technology into their production line. Two primary industry-imposed requirements were addressed through this collaboration. 1) The security and isolation of vertical data were addressed using MEC, providing LBO UPF. 2) For network slicing, given the absence of a high-level control mechanism. This adjustment was achieved through manual configurations on the network using QoS mechanisms.

Although slicing is an important 5G aspect for the industry, at the moment, the network used has no network functions or 5G functionality that allow high-level implementation and control of slices. Since these mechanisms do not exist, network slicing cannot be attested. However, this document contains numerous results showcasing the impact of configurations on the communication performance of network slices. This was done with network hardcoded configurations. However, implementing this in production becomes unfeasible due to the number of commands required for configuration, which can lead to a significant workload and errors, potentially affecting use cases already running on the network. Leaving for future work the development of a system that automates the configuration of the network, so 5G can support the network slice that reflect the performance demanded by the verticals.

The usage of the QoS mechanism does not provide monitoring capabilities over the network slice to the verticals but already allows the adjustment of communication performance. Where if each slice uses a specific QoS flow, is possible to adjust the performance of the entire slice.

A. REALIZING NETWORK SLICING: QOS-BASED SLICING

The performance analysis provided in the document demonstrates that QoS mechanisms allow for the adjustment of the communication performance of a network slice. It is also evident from the granularity and minimum value tests that using trustworthy values for parameters is crucial, and they should be associated with reasonable values rather than extremely low values. This precaution is likely necessary because of the algorithms implemented in the systems.

The Averaging Window defines the interval that the network uses for bandwidth control. Therefore, the usage of this parameter could be extremely important in use cases with more burst traffic and in those that require more stable traffic. A high value for the Averaging Window could be used in use cases with bursty traffic, while a low value could be used in use cases that require more stable and consistent traffic.

The tests with PDB already show some differentiation in performance that, if used in conjunction with the DSCP values, can make a critical difference in latency performance for some use cases. However, since the currently available release does not fully support URLLC slices and Delay-critical GBR QoS Flows, the true impact of this parameter cannot be fully observed. In terms of DSCP value performance, since the evaluation was in an infrastructure with a limited amount of traffic, the differentiation between each value is not so distinct. However, it is already possible to notice a performance difference between the values with lower latency than the rest.

From the results, the MFBR and AMBR performed as expected when reasonable values were used, except for an artefact with DNN-AMBR. Disregarding that, the UE-AMBR, DNN-AMBR, and MFBR give different control of maximum throughput that can be used to impose different bandwidth limitations on a UE. The UE-AMBR limits the overall non-GBR throughput of the UE, the DNN-AMBR limits the throughput of all non-GBR flows in a PDU session, and the MFBR can be used for finer-grained control, being able to limit the throughput of each flow when the UE has multiple communications in a single PDU session.

In the documentation, it is described that the Priority Level parameter is used to select the configurations of specific 5G technologies, such as Discontinuous Reception (DRX), when a UE is using multiple QoS Flows. These mechanisms utilize the configurations of the QoS Flow with a higher priority. Therefore, this parameter does not have a direct impact on communication performance, confirming the hypothesis that the Scheduling Priority Weight Factor has the functionality of the Priority Level described in the standards. This alignment is consistent with the results obtained in the performance analysis.

Even though the deployment of URLLC and MIoT use cases with this release is extremely limited, the appropriate usage of all the evaluated QoS parameters provides huge flexibility and control over an eMBB slice. The lack of end-to-end GBR QoS flow and the bandwidth limitation in the RAN, not the core, prevent testing of the GFBR functionality in the core. However, similar results to the ones expected can be achieved using the guaranteed rate parameter in the RAN, demonstrating that even unavailable parameters can be replaced by others that provide similar functionalities.

Up to this point, most of the 5G network analysis presented in this document was focused on QoS, avoiding network slicing. This is because there is no real network slicing in 5G networks at the moment, as the construction of network slices is not as simple as expected. At the moment, it is possible to define network slices in a 5G network and associate them with UEs. The current functionality of the slices is to define which network functions a UE can use, having no significant impact on 5G network communications for now.

All the QoS features presented in the document are crucial for network slices since these features can become the basis for performance differentiation between network slices. But to achieve that, it is required to associate an entire infrastructure in terms of physical components and management components. The network used for the demonstration of 5G functionalities in this document has only one sample of each control plane network function deployed, being UPF the only network function with two instances. So, network slices for now in this network can only differentiate the access to a specific UPF and its local network.

B. NETWORK LIMITATIONS

While the 5G network is expected to provide many features, it's important to note that several of these features will only be available in later releases. For instance, URLLC slices are expected to be implemented in Release 16, and MIoT slices will be introduced in subsequent releases.

The commercially available release at the start of the project was R15, which is the release deployed in the 5GAIner infrastructure, supporting only eMBB slices. These slices are primarily focused on bandwidth. Hence, most of the currently available QoS parameters concentrate on controlling bandwidth. Later releases are expected to offer more comprehensive control over 5G communications. However, at present, most configurations define the bandwidth and priority of each communication. Despite these limitations, a thorough analysis of QoS can demonstrate the performance and flexibility that a 5G network currently provides, offering valuable insights for future releases.

Even though one could notice some differences in the results when analyzing parameters that do not affect throughput, the variations in results are really small. This is expected in the 5G release used, as this particular release prioritizes throughput over other performance metrics.

During the network design phase, similar to the design of the 5GAIner network, many others might consider that PCF is not a crucial network function for supporting industrial use cases. However, the 5G network does not necessarily require this function to provide communication. The absence of PCF can significantly limit the flexibility of network performance, depending on how the 5G network was implemented. This limitation became apparent when attempting to test several

functionalities that any 5G network should support, such as usage of end-to-end GBR QoS Flows, configuration of PER, and dynamic adjustment of communication performance while the UE is transmitting. On the 5GAIner network, only MFBR allows for dynamic configuration.

Currently, the network lacks a precisely synchronized common clock among all NFs, UEs, and servers. Such precise clock synchronization would be essential for conducting more accurate assessments of the low latencies associated with a 5G deployment. This limitation hinders the ability to conduct an in-depth analysis of communication latency, including the examination of how each network component of the user plane affects communication latency.
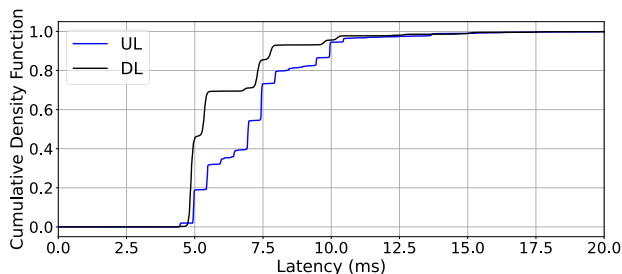

FIGURE 20. 5GAIner latencies.

In the 5GAIner network is possible to implement hard-coded slices, but the R15 is not ready for the industry lacking controllability and an easier way to adjust network performance. A R15 does not have URLLC, so the control of the latency is extremely limited. Even though the latency values obtained in the 5GAIner network are shown in Figure 20, demonstrating that most packets have a latency below 10 ms.

C. FUTURE RELEASES

Despite the limitations of the current R15, it is evident that commercial equipment already offers flexibility in defining the performance of slices. However, the majority of parameters are limited to influencing communication throughput. It is anticipated that later releases will introduce new parameters that impact other KPIs.

Release 16, which incorporates URLLC, already introduces new features in network configurations that enable improved control over the latency performance of slices. Additionally, in release 17, further features are introduced, also affecting low-power communications.

The new features expected in upcoming releases will significantly enhance the management of 5G communications, facilitating the establishment of various slices beyond eMBB. Moreover, they will enable superior control over diverse communication parameters crucial to specific vertical use cases. For example, some of the features anticipated in subsequent releases and their impact on specific KPIs include the following: (i) latency - configured grant, PDCP Out-of-order Delivery, and Time Sensitive Communication (TSC); (ii) reliability - PDCP duplication, Multi-TRP, and Low Block

Error Rate (BLER) Modulation Coding Scheme (MCS) and Channel Quality Indicator (CQI) table; (iii) energy efficiency - Wake-Up Signal (WUS), Reduce Capabilities (RedCap), Small Data Transmission (SDT), and Mobile Initiated Connection Only (MICO); among other anticipated features and functionalities.

Where release 18, should already support most of the problems identified here, and in the meantime, most of the problems identified by other researchers in the literature should be solved. So there is an optimism that in a later release, the 5G network will become ready and much easier to use, allowing verticals to adopt and use the technology without requiring such a deep knowledge of 5G. While later releases will offer enhanced performance and flexibility, it is anticipated that release 15 SA will be the primary offering for operators in the coming years due to the time it takes for subsequent releases to be properly materialized and assessed.

D. CONSIDERATIONS ON SECURITY AND ISOLATION

5G brings many security features that are known as key enablers for realizing use cases with different degrees of security risks, 5G-ACIA in [37] delves into four different levels of security which impose different requirements on the network to ensure the data in the 5G network is secure all the time.

Considering the functionalities outlined in the document, in terms of security and isolation within release 15, it is possible to define filters Layer 3, Layer 4, and Layer 7 using PCC rules, which define the communications rules for end devices. Layer 3 and Layer 4 filters can define the IPs, Layer 4 protocols, and ports that each PCC rule controls. On the other hand, Layer 7 filters can specify the URLs and method types (such as GET, POST, CONNECT, etc.) controlled by a PCC rule. The PCC Rule defines if the traffic corresponding to that filter can pass or is blocked on the UPF.

In subsequent releases, it is anticipated that the 5G network will support at least User Plane (UP) integrity protection and UP confidentiality protection. These features serve to safeguard user plane data during communication.

The significance of security and isolation within 5G and network slicing has been extensively addressed by multiple stakeholders. For instance, 5G-ACIA delves into this critical aspect in [37], while 3GPP offers insights into network slice security in 5G and B5G (Beyond 5G) in [38]. Moreover, various cybersecurity agencies highlighted numerous threats associated with 5G network slicing and proposed corresponding mitigation strategies in [39].

Additionally, while exploring private 5G deployments, several design choices can further increase the level of isolation of the 5G network. Ranging from (SNPN) to the various flavours of (PNI-NPN) the network user and control planes can be more or less confined to industrial deployment.

Furthermore, since the objective was to test the best performance possible in a 5G network, and since is acceptable in some scenarios, due to the data being limited to the local

domain, minimal security measures were used in the 5G domain.

E. FUTURE WORK

For a broader adoption of 5G technologies by the industry network slicing is of utmost importance. However, the manual deployment of slices, as demonstrated in this work is unfeasible, due to being error-prone, time-consuming, and requiring specialized knowledge in 5G technology. Hence, automating the management of network slices emerges as a necessity. However, to achieve this automation, it is vital to comprehend the underlying mechanisms within the 5G network. This document primarily focuses on elucidating the operational functionality of 5G networks and delves into the exploration of underlying mechanisms that can be used in the realization of network slices.

Future works will aim to scrutinize the outcome of this work to establish an automated mechanism for managing network slices in a 5G network for the realization of vertical applications. In doing so, we will follow standardization efforts related to the automation of network slicing mechanisms [40], [41], and [42].

REFERENCES

[1] J. Cheng, W. Chen, F. Tao, and C.-L. Lin, "Industrial IoT in 5G environment towards smart manufacturing," *J. Ind. Inf. Integr.*, vol. 10, pp. 10–19, Jun. 2018, doi: 10.1016/j.jii.2018.04.001.

[2] *Industrial 5G Edge Computing Use Cases, Architecture and Deployment*, 5G Alliance for Connected Industries and Automation (5G-ACIA), Germany, 2023. [Online]. Available: https://5g-acia.org/whitepapers/industrial-5g-edge-computing-use-cases-architecture-and-deployment/

[3] *Service Requirements for Cyber-Physical Control Applications in Vertical Domains*, document 22.104, Version 17.7.0, 3GPP, 2020.

[4] D. Corujo, J. Quevedo, R. L. Aguiar, P. Paixão, H. Martins, and Á. Gomes, "An economic assessment of the contributions of 5G into the railways and energy sectors," *Wireless Pers. Commun.*, vol. 129, no. 1, pp. 71–94, Mar. 2023, doi: 10.1007/s11277-022-10086-5.

[5] R. Kiesel, J. V. Roessel, and R. H. Schmitt, "Quantification of economic potential of 5G for latency critical applications in production," *Proc. Manuf.*, vol. 52, pp. 113–120, Jan. 2020, doi: 10.1016/j.promfg.2020.11.021.

[6] *5G Non-Public Networks for Industrial Scenarios*, 5G Alliance for Connected Industries and Automation (5G-ACIA), Germany, Sep. 2021. [Online]. Available: https://5g-acia.org/whitepapers/5g-non-public-networks-for-industrial-scenarios/

[7] S. Wijethilaka and M. Liyanage, "Survey on network slicing for Internet of Things realization in 5G networks," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 2, pp. 957–994, 2nd Quart., 2021, doi: 10.1109/COMST.2021.3067807.

[8] D. Corujo, J. Quevedo, V. Cunha, A. Perdigão, R. Silva, D. Santos, R. L. Aguiar, P. Paixão, P. E. Silva, R. Antunes, C. Marques, and Á. Gomes, "An empirical assessment of the contribution of 5G in vertical industries: A case for the transportation sector," *IEEE Access*, vol. 11, pp. 15348–15363, 2023, doi: 10.1109/ACCESS.2023.3243732.

[9] J. Meira, G. Matos, A. Perdigão, J. Cação, C. Resende, W. Moreira, M. Antunes, J. Quevedo, R. Moutinho, J. Oliveira, P. Rendeiro, P. Oliveira, A. Oliveira-Jr., J. Santos, and R. L. Aguiar, "Industrial Internet of Things over 5G: A practical implementation," *Sensors*, vol. 23, no. 11, p. 5199, May 2023, doi: 10.3390/s23115199.

[10] M. Ghassemian, P. Muschamp, and D. Warren, "Experience building a 5G testbed platform," in *Proc. IEEE 3rd 5G World Forum (5GWF)*, Sep. 2020, pp. 473–478, doi: 10.1109/5GWF49715.2020.9221109.

[11] Y. Wang, A. Gorski, and A. P. da Silva, "Development of a data-driven mobile 5G testbed: Platform for experimental research," in *Proc. IEEE Int. Medit. Conf. Commun. Netw. (MeditCom)*, Sep. 2021, pp. 324–329, doi: 10.1109/MeditCom49071.2021.9647461.

[12] Y. R. Wei, A. S. Keshavamurthy, R. Wittmann, and A. R. Zahonero, "A standalone 5G industrial testbed design considerations for industry 4.0," in *Proc. 52nd Eur. Microw. Conf. (EuMC)*, Sep. 2022, pp. 884–887, doi: 10.23919/EuMC54642.2022.9924323.

[13] C. Coletti, W. Diego, R. Duan, S. Ghassemzadeh, D. Gupta, J. Huang, and K. Yan, "O-RAN: Towards an open, software-driven, and intelligent radio access network," *RS Open J. Innov. Commun. Technol.*, vol. 4, no. 9, 2023. [Online]. Available: https://rs-ojict.pubpub.org/pub/ji8c94of/release/2

[14] S. Iqbal and J. M. Hamamreh, "A comprehensive tutorial on how to practically build and deploy 5G networks using open-source software and general-purpose, off-the-shelf hardware," *RS Open J. Innov. Commun. Technol.*, vol. 2, no. 6, pp. 1–28, Dec. 2021, doi: 10.46470/03d8ffbd.4ccb7950.

[15] A. Akman, S. Gu, J. Huang, I. Wong, H. Akhtar, S. Poretsky, and A. Buldorini, "O-RAN minimum viable plan and acceleration towards commercialization," *RS Open J. Innov. Commun. Technol.*, vol. 4, no. 9, 2023. [Online]. Available: https://rs-ojict.pubpub.org/pub/gsry0u68/

[16] A. Pinchuk, R. Odarchenko, V. Samoilenko, and A. Imanbayev, "5G network deployment based on open-source projects: A comparative analysis," in *Proc. IEEE 12th Int. Conf. Intell. Data Acquisition Adv. Comput. Syst., Technol. Appl. (IDAACS)*, vol. 1, Sep. 2023, pp. 596–601, doi: 10.1109/IDAACS58523.2023.10348675.

[17] S. Guo, B. Lu, M. Wen, S. Dang, and N. Saeed, "Customized 5G and beyond private networks with integrated URLLC, eMBB, mMTC, and positioning for industrial verticals," *IEEE Commun. Standards Mag.*, vol. 6, no. 1, pp. 52–57, Mar. 2022, doi: 10.1109/MCOM-STD.0001.2100041.

[18] T. Wichary, J. Mongay Batalla, C. X. Mavromoustakis, J. Zurek, and G. Mastorakis, "Network slicing security controls and assurance for verticals," *Electronics*, vol. 11, no. 2, p. 222, Jan. 2022, doi: 10.3390/electronics11020222.

[19] V. A. Cunha, N. Maroulis, C. Papagianni, J. Sacido, M. Jimenez, F. Ubaldi, M. Gharbaoui, C. Y. Chang, N. Koursioumpas, K. Tomakh, and D. Corujo, "5 Growth: Secure and reliable network slicing for verticals," in *Proc. Joint Eur. Conf. Netw. Commun. 6G Summit (EuCNC/6G Summit)*, 2021, pp. 347–352, doi: 10.1109/EuCNC/6GSummit51104.2021.9482536.

[20] M. Xie, A. J. Gonzalez, P. Grønsund, H. Lønsethagen, P. Waldemar, C. Tranoris, S. Denazis, and A. Elmokashfi, "Practically deploying multiple vertical services into 5G networks with network slicing," *IEEE Netw.*, vol. 36, no. 1, pp. 32–39, Jan. 2022, doi: 10.1109/MNET.001.2100361.

[21] S. K. Rao and R. Prasad, "Impact of 5G technologies on Industry 4.0," *Wireless Pers. Commun.*, vol. 100, pp. 145–159, May 2018, doi: 10.1007/s11277-018-5615-7.

[22] J. S. Walia, H. Hinen, K. Kilkki, and S. Yrj, "5G network slicing strategies for a smart factory," *Comput. Ind.*, vol. 111, pp. 108–120, Oct. 2019, doi: 10.1016/j.compind.2019.07.006.

[23] Z. Shu and T. Taleb, "A novel QoS framework for network slicing in 5G and beyond networks based on SDN and NFV," *IEEE Netw.*, vol. 34, no. 3, pp. 256–263, May 2020, doi: 10.1109/MNET.001.1900423.

[24] S. Perez and H. Facchini, "An evaluation of QoS for intensive video traffic over 802.11e WLANs," in *Proc. Int. Conf. Electron., Commun. Comput. (CONIELECOMP)*, 2015, pp. 8–15, doi: 10.1109/CONIELE-COMP.2015.7086933.

[25] H. Zhu and M. Li, "A survey of quality of service in IEEE 802.11 networks," *IEEE Wireless Commun.*, vol. 11, no. 4, pp. 6–14, 2004, doi: 10.1109/MWC.2004.1325887.

[26] D. Zhang and D. Ionescu, "QoS performance analysis in deployment of DiffServ-aware MPLS traffic engineering," in *Proc. 8th ACIS Int. Conf. Softw. Eng., Artif. Intell., Netw., Parallel/Distrib. Comput. (SNPD)*, vol. 3, Aug. 2007, pp. 963–967, doi: 10.1109/SNPD.2007.541.

[27] Y. Guo and H. Chaskar, "Class-based quality of service over air interfaces in 4G mobile networks," *IEEE Commun. Mag.*, vol. 40, no. 3, pp. 132–137, Mar. 2002, doi: 10.1109/35.989773.

[28] K. S. Ibarra-Lancheros, G. Puerto-Leguizamón, and C. Suárez-Fajardo, "Quality of service evaluation based on network slicing for software-defined 5G systems," *TecnoLógicas*, vol. 21, no. 43, pp. 27–41, Sep. 2018.

[29] Q. Wang, J. Alcaraz-Calero, R. Ricart-Sanchez, M. B. Weiss, A. Gavras, N. Nikaein, X. Vasilakos, B. Giacomo, G. Pietro, M. Roddy, and M. Healy, "Enable advanced QoS-aware network slicing in 5G networks for slice-based media use cases," *IEEE Trans. Broadcast.*, vol. 65, no. 2, pp. 444–453, Jun. 2019, doi: 10.1109/TBC.2019.2901402.

[30] J. Quevedo, A. Perdigão, D. Santos, R. Silva, and R. L. Aguiar, "5GAIner: Taking the verticals into the 5G road," in *Proc. Joint Eur. Conf. Netw. Commun. 6G Summit (EuCNC/6G Summit)*, Jun. 2023, pp. 514–519, doi: 10.1109/EuCNC/6GSummit58263.2023.10188375.

[31] *System Architecture for the 5G System (5GS)*, document TS 23.501, V15.13.0, 3GPP, Mar. 2022.

[32] *5G ACIA, Key 5G Use Cases and Requirements*, 5G Alliance for Connected Industries and Automation (5G-ACIA), Germany, May 2020. [Online]. Available: https://5g-acia.org/whitepapers/key-5g-use-cases-and-requirements/

[33] *Policy and Charging Control Architecture*, document TS 23.203, V15.5.0, 3GPP, Jun. 2019.

[34] *NR; NR and NG-RAN Overall Description*, document TS 38.300, V15.13.0, Jun. 2021.

[35] *Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers*, document RFC2474, DSCP Field, Dec. 1998.

[36] *Configuration Guidelines for DiffServ Service Classes*, document RFC4594, DSCP Values, Aug. 2006.

[37] *Security Aspects of 5G for Industrial Networks*, 5G Alliance for Connected Industries and Automation (5G-ACIA), Germany, 2021. [Online]. Available: https://5g-acia.org/whitepapers/security-aspects-of-5g-for-industrial-networks/

[38] (May 2023). *3GPP*. [Online]. Available: https://www.3gpp.org/technologies/slicing-security

[39] *ESF Potential Threats to 5G Network Slicing*, U.S. Dept. Defense, Dec. 2022. [Online]. Available: https://media.defense.gov/2022/Dec/13/2003132073/-1/-1/0/POTENTIAL%20THREATS%20TO%205G%20-NETWORK%20SLICING_508C_FINAL.PDF

[40] *Management and Orchestration; 5G Network Resource Model (NRM)*, document TS 28.541, V 18.4.1, 3GPP, Jun. 2023.

[41] *Management and orchestration; Provisioning*, document TS 28.531, V 18.3.0, 3GPP, Sep. 2023.

[42] *Study on Network Slice Management Capability Exposure*, document TR 28.824, V 18.0.1, 3GPP, Jul. 2023.

ANDRÉ PERDIGÃO received the M.S. degree in electronic and telecommunications from the University of Aveiro, in 2018, where he is currently pursuing the Ph.D. degree in electrical engineering. He was a Junior Researcher with Instituto de Telecomunicações (IT), in 2016 and 2017. Since 2018, he has been at IT as a Researcher. During this time, he worked with different communication technologies, such as Wi-Fi, LoRa, SDN, 2G, 802.11p, and 5G, and working with different industrial networks and technologies. It was involved in the designing and planning of PASMO and 5GAIner networks. Then, he implemented, deployed, and maintained the 5GAIner networks, during this time contributed to several projects, such as PASMO, 5GASP, 5Growth, Augmanity, Imagine-B5G, and 5GAIner. Work in the last years, he was focused on optimizing industrial communication systems based on 5G. More focused on QoS and slicing, but analysing any functionality of 5G that can be used in I4.0.

JOSÉ QUEVEDO (Member, IEEE) received the Ph.D. degree in telecommunications from the MAP-Tele Doctoral Program in Telecommunications, in 2020. His early research activities were focused on information-centric networking (ICN) approaches for supporting the Internet of Things (IoT) scenarios. This work conducted at the Telecommunications and Networking-Av Group (TN-Av), Instituto de Telecomunicações (IT-Av), and the University of Aveiro (UA), Portugal, has been disseminated in book chapters, conference papers and journal articles, and contributions to open-source software. He has been involved in the different stages of several research projects, such as H2020 5Growth, H2020 5GASP, and HE Imagine-B5G. He has been further involved in the academy by working as an Invited Adjunct Professor with the University of Aveiro—Águeda School of Technology and Management (ESTGA). Currently, he is the Executive Manager of the 5GAIner Laboratory and a Senior Researcher with IT-Av, with a focus on networking protocols, network programmability, and 5G and beyond systems.

RUI L. AGUIAR (Senior Member, IEEE) was the Founder of the ATNOG Research Group, Advanced Telecommunication Research Group, Universidade de Aveiro. He is currently a Full Professor with Universidade de Aveiro. He is also co-coordinating a research line with Instituto de Telecomunicações, on the area of networks and services. He has been an Advisory for the Portuguese Secretaria de Estado das Comunicações and a member of the task force for 5G cybersecurity. He is a Chartered Engineer and a member of ACM. He has served as the Portugal Chapter Chair for the IEEE Communications Society and has been serving as the Steering Board Chair for Networld Europe, the European ETP representing the telecommunications community, engaged in the discussions of the future European research and development work program for telecommunications. As further community engagement, he has served as the Technical and General (Co)Chair for several conferences, ICNS, ICT, ISCC, Mobiarch, Monami, and NTMS. He is a regular keynote speaker in the future of mobile communications and digital society, with dozens of talks across the whole world. He is an Associate Editor of *Emerging Telecommunication Technologies* (Wiley) and *Wireless Networks* (Springer).

• • •