5G-ACIA White Paper

5G for Industrial Internet of Things (IIoT): Capabilities, Features, and Potential

5G Alliance for Connected Industries and Automation

Table of Contents

1. Executive Summary

The impact that 5G is having on Industrial IoT (IIoT) is a hotly discussed topic. Wireless communication is essential for the Smart Factory and Industry 4.0 because it enables seamless, pervasive, and scalable connectivity among machines, people, and sensors as well as with mobile entities such as mobile robots, automated guided vehicles (AGVs), drones, and humans. It also delivers benefits by removing cables from stationary, rotating, and other objects with limited mobility.

One major contribution of 5G is extremely reliable communication, paving the way for wireless isochronous real-time motion control, sensor systems for monitoring critical processes, and AR/VR applications. And all of these are served by a single wireless communication system. This isn't the only feature that makes 5G suitable for IIoT applications, however. Thanks to use cases published by 5G-ACIA, 5G technology has significantly evolved over the course of successive releases to provide ever-broader support for applications of these kinds. Besides radio capabilities, this white paper describes 5G capabilities that are relevant to IIoT applications, including support for Ethernet integration, time-sensitive networking (TSN), and security in nonpublic networks. It also talks about ways in which verticals can access 5G technology to drive the evolution of IIoT in terms of deployment and spectrum access.

The ultimate aim of this white paper is to facilitate a deeper understanding of capabilities and features of 5G that are important for industrial automation. Because 5G devices can be built with varying capabilities, it discusses which are needed for different functionalities. The same statement applies to features that are essential for integrating infrastructure.

About 5G-ACIA

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

2. Introduction

When selecting a communication solution, it's important to know how well it can be expected to perform in its intended use. This can be challenging when switching to a completely new regime, like when migrating to 5G from a legacy wired or wireless system that has very different criteria and terminology. This white paper attempts to smooth the transition by shedding light on technical criteria that are important for evaluating wireless systems for Industrial IoT (IIoT) use cases, and also by explaining the relevance of each such criterion and the use cases for which it is important. In addition, it provides a 5G benchmark for each criterion by explaining the capabilities and options supported by the standard and providing guidance on which features to look for in a 5G solution. The main focus is on the 5G features defined through Release 16 by the 3rd Generation Partnership Project (3GPP), a consortium spanning several standards organizations, while also presenting some Release 17 capabilities.

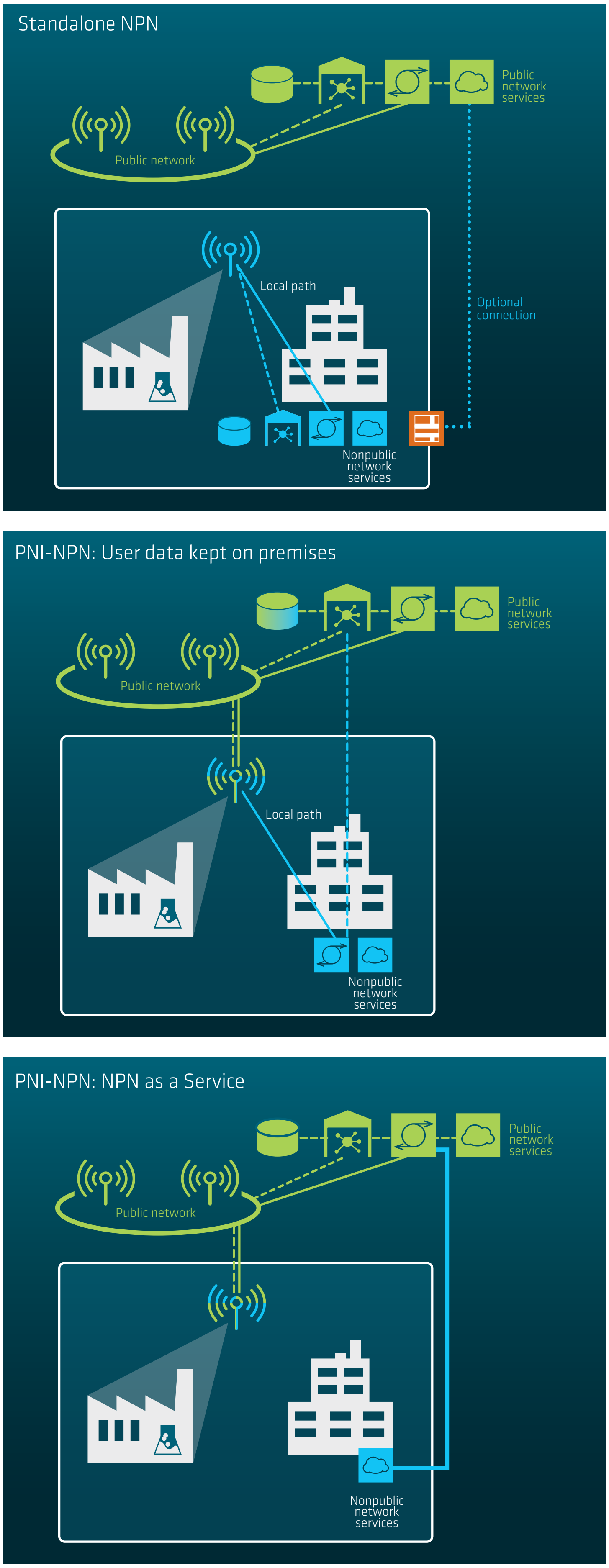
This document is structured by technical topics as follows: Chapter 3 talks about the flexibility of 5G, which can support many different use cases or be tailored for a particular use. Chapter 4 explains the spectrum access options available with 5G – it can use nationally or regionally licensed, locally licensed, or unlicensed spectrum – and how each of them can affect system performance. Chapter 5 describes key features that let 5G comply with strict IIoT performance requirements while delivering the benefits of a wireless system such as mobility. Chapter 6 explains how the 5G system presents its capabilities to the user. Chapter 7 introduces the capabilities that the 5G system offers in terms of supporting QoS in general and TSN in particular, as well as other Industrial Ethernet protocol versions with generic capabilities. An overview of 5G positioning features is given in chapter 8. Chapter 9 surveys the security features that protect industrial communications over a wireless 5G interface. Since a wireless system's components must meet certain specifications in order to ensure proper and compliant performance, Chapter 10 explains how those for 5G are defined and tested. Finally, chapter 11 wraps up the technical analysis and calls attention to 5G-ACIA documents that go into greater depth on various technical aspects.

3. Deployment Models: Nonpublic Networks (NPNs)

The 5G system's architecture is designed to flexibly serve different coverage areas and numbers of users. A physical network can also host multiple logical networks, each of which delivers a different set of capabilities as required. This ensures that networking solutions are available for a variety of IIoT use cases, which can range from regular cellular data subscriptions with virtually global service all the way to owning and operating a dedicated, purpose-built 5G IIoT network that locally meets all of a factory site's wireless communication requirements.

Many industrial IoT use cases, especially in the manufacturing sector, require a network that is tailored for a defined group of IIoT users and sealed off from users of public networks and other IIoT users. A 5G network of this kind is referred to as a nonpublic network (NPN). The 5G standards support two main kinds of NPNs: standalone NPNs (SNPNs), which are purpose-built 5G networks for IIoT operation only, and public network integrated NPNs (PNI-NPNs), which are deployed within the public network while being logically separate from it. A PNI-NPN can use a 5G-specific architecture called network slicing to create logical networks. These types of NPNs can be deployed in a variety of configurations. Some general examples are presented in another 5G-ACIA white paper (see [1]) and summarized in figure 1 below.

Figure 1: Example SNPN and PNI-NPN deployment scenarios



A standalone nonpublic network (SNPN) is a purpose-built, complete 5G network that can be either owned and operated by a user or fully or partially sourced from a third party as a service. It can be appropriately scaled for its intended purpose, which typically is to serve a local network. Sophisticated automation and self-optimization features are available to facilitate the operation and use of SNPNs. In the case of PNI-NPNs, at least part belongs to the public network and is licensed from the responsible telecommunications operator as a service. This ensures easy access to a larger served area. PNI-NPN options are available for keeping critical user data under the owner's complete control on the premises of an industrial operation.

5G edge computing capabilities can be included in all of these scenarios. Hosting edge cloud infrastructure in close physical proximity to the devices using the network helps achieve low-latency responses and efficiently use resources and bandwidth. A distributed edge computing framework makes it possible to build advanced services that make use of input aggregated from multiple sources. It can be taken advantage of to shift heavy computation and coordination loads from individual devices to a more centralized location and achieve both faster response times and greater bandwidth availability.

When appropriate, the 5G system can also be configured to meet local regulatory requirements such as lawful interception by legal bodies or emergency calls. When there are no such requirements, the corresponding features can be left out of the deployment.

4. Spectrum Access

5G flexibly supports different authorization approaches for accessing frequency spectrum. Table 1 lists various spectrum licensing models that are available for private 5G-based IIoT deployments, indicating their main characteristics and typical parameters. When possible and available, individual 5G deployments can use more than one type of spectrum. Here, "low-band" refers to the deployment spectrum up to 1 GHz, "mid-band" up to 7 GHz, and "high-band" above 7 GHz.

Table 1: Spectrum licensing models

Required authorization	**Nationally or regionally licensed**	**Locally licensed**	**Unlicensed**
Definition	Licensed to a single licensee (e.g. a mobile network operator) nationally or regionally (i.e. only one licensee may use a certain block of spectrum nationally or regionally). (*)	Licensed on an individual and local basis (i.e. different licensees are allowed to locally and exclusively use a certain block of spectrum within a specified geographic area.(*)	Anyone can use the spectrum as long as they follow proper channel access procedures.
Available bandwidth per network (typical, depends on national regulations)	Frequency-division duplexing (FDD): multiple 2x10–2x20 MHz, low- and mid-band Time-division duplexing (TDD): 20 to ≥100 MHz, mid-band 200 to ≥1000 MHz, high-band (e.g. 24–47 GHz range)	TDD: 40 to ≥100 MHz, mid-band 200 to ≥1000 MHz, high-band	TDD: Up to 500 MHz, mid-band Up to multiple GHz, high-band (e.g. the 52.7–71 GHz range in Release 17)

(*) Rights to use spectrum can be assigned on a shared basis to ensure coexistence with any incumbents within the relevant band (e.g. earth stations for fixed-satellite services, fixed links for backhauling) in some regulatory domains.

Each spectrum licensing model is different in terms of performance capabilities and considerations for private IIoT deployments.

Nationally or regionally licensed spectrum: This spectrum is typically licensed to mobile network operators (MNOs) and can be accessed by verticals (i.e. the companies, industries, and public sector organizations operating in a specific sector) using the PNI-NPN or SNPN model (directly or through a third party) or via a public 5G network. A vertical can lease spectrum from an MNO if this is allowed by the applicable regulations. The use of licensed spectrum for 5G NR (New Radio) results in better performance in terms of latency and reliability, since the deployed system has guaranteed access to the channel and there is no risk that unintended interference from other networks could cause delays.

Locally licensed spectrum: Regulatory bodies grant licenses for organizations to use spectrum on an exclusive basis within a defined area. The local licenses granted for use of the 3.7–3.8 GHz band in Germany are an example. Spectrum is administered by an authority that takes steps to shelter local deployments from detrimental interference from neighboring licensees. Exclusive access to spectrum resources can be assumed at a given location, so here 5G NR can be expected to perform optimally in terms of latency, capacity, and reliability. Models for less exclusively managed spectrum sharing also exist, like that in the USA for the 3550 to 3700 MHz range called the Citizens Broadband Radio Service (CBRS), which is primarily intended to protect incumbent users. IIoT systems may suffer from interruptions when operating in bands of this kind.

Unlicensed spectrum: A technology called 5G New Radio Unlicensed (NR-U) can be used for unlicensed spectrum. Several gigahertz of this kind of spectrum are now available: the 5 GHz and 6 GHz bands as well as the 52.7–71 GHz band defined in Release 17. A drawback is that there is no guarantee of very low packet latencies in unlicensed spectrum (which in many cases uses Listen Before Talk (LBT) channel access mechanisms) unless the environment is fully controlled. “Fully controlled” means ensuring that only NR-U equipment of the same network uses a given frequency carrier while minimizing all interference. This can be hard to achieve in fairly open environments such as ports, university campuses, etc. Channel access rules for the high-band range are still in the assessment phase.

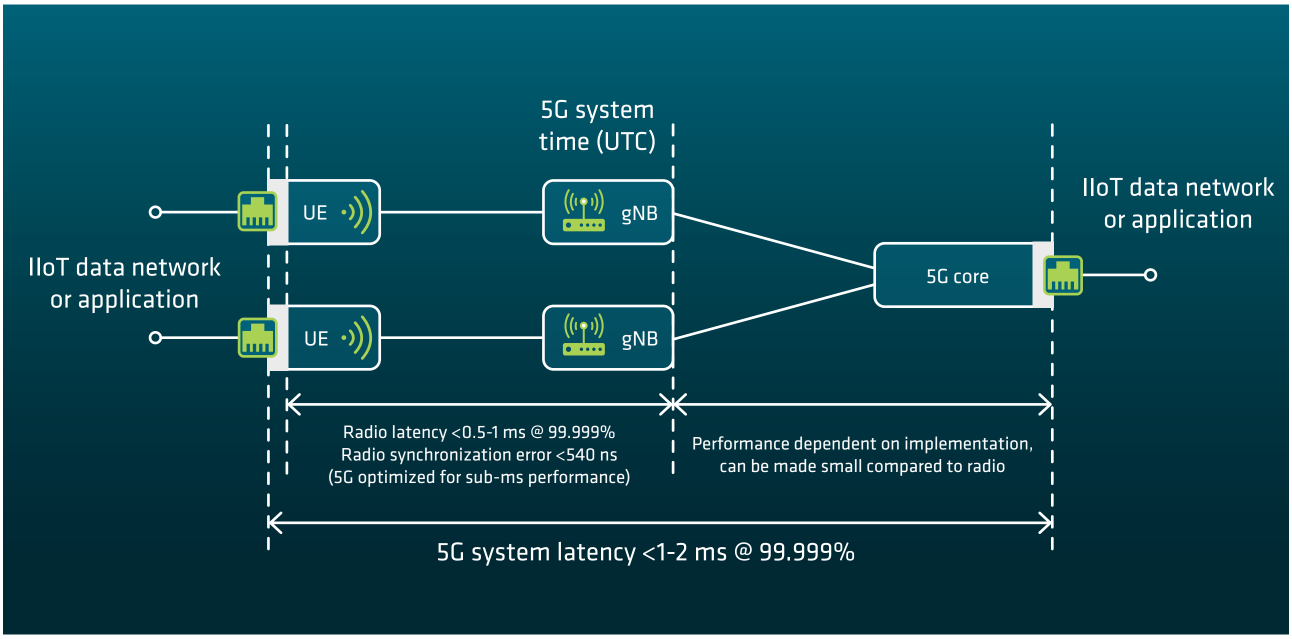
5. 5G Performance

5.1 Introduction

This chapter describes the main 5G radio access network (RAN) capabilities and radio performance that are required to support ultra-reliable low-latency communications (URLLC) and IIoT services for industrial communications. 5G RAN standards are continually evolving to support new and enhanced features and capabilities, some of which are specifically designed for industrial communications.

Figure 2 presents key 5G performance metrics that have been optimized for IIoT use cases calling for sub-ms URLLC performance. gNB is the base station and UE (user equipment) is the device modem. When discussing the performance of an entire 5G system, it's also important to consider delays that can be introduced by the transport network and core network processing. When core network functions for the user plane are deployed locally (for example, in factories), they add less latency than delays associated with the radio interface. When the URLLC features and capabilities are enabled and properly configured, the 5G system can achieve an E2E latency of one or two milliseconds and a reliability of 99.999%. System capacity and performance also depend on the spectrum used as well as various other parameters (e.g. the TDD pattern). There is always a tradeoff between system capacity and achievable performance (latency and reliability). However, 5G can also accommodate more relaxed requirements.

Figure 2: Key performance metrics of a 5G system optimized for sub-millisecond URLLC performance in IIoT use cases, separately showing the contributions of radio and 5G system metrics.



5.2 Capacity, Reliability, and Latency

5G supports URLLC services, which is a major advance for accommodating new IIoT use cases with wireless connectivity. URLLC enables wireless support for service flows in which the greatest tolerable packet latency across the air interface is less than one millisecond, with a packet reliability greater than 99.999% and in specialized deployments greater than 99.9999%. 5G ensures this at a level that meets or exceeds the packet reliability requirement. 5G URLLC is based on a large set of 5G features that have been introduced since Release 15 to address the requirements of ITU-R M.2083. (see references [2] and [3]).

URLLC is one of the pillars of the 5G system. 3GPP has developed several new features for radio access and core networks that enable communication services of this kind throughout the 5G system. They include advanced multi-antenna technologies and a flexible framework for dynamically scheduling user traffic over radio access networks (RANs) to achieve extremely low latency and high reliability.

To maximize reliability and availability, 5G routes user traffic via multiple transmission and reception points (multi-TRPs). In factories full of machines, spatial diversity can be accommodated by packet duplication functionality over radio access and core networks. A simulation-based evaluation of IIoT use cases defined by 5G-ACIA (see [4]) found that advanced semi-static or dynamic 5G RAN resource coordination mechanisms significantly boost the achievable capacity in terms of the number of UEs that meet performance requirements and use resources efficiently. Especially for deterministic traffic in automated industrial environments, semi-static schemes for coordinating resource use among neighboring RAN nodes can greatly increase performance.

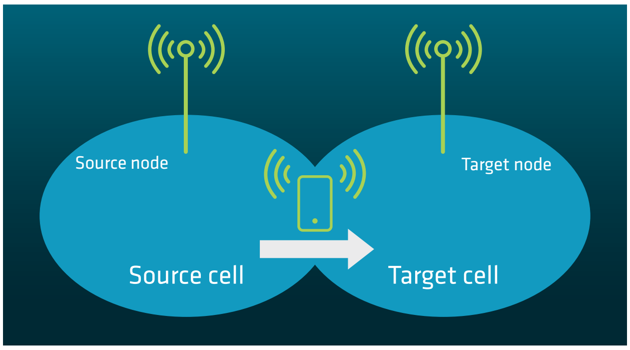
Trials have shown that 5G systems can enable ultra-low-latency communications in real-world scenarios (see [5]). The performance of 5G in a specific 5G-ACIA IIoT scenario with a data packet size of 48 bytes and a strict one-millisecond URLLC performance target was also analyzed in a simulation (see [4]), confirming that a properly configured 5G system is able to meet requirements. Additional tweaks and optimized configurations can improve performance further to 0.5 ms with 99.999% packet reliability over the air interface (see [6]). To achieve very fast speeds in the uplink (from device to network), radio resources must be reserved in advance; this is possible when the network knows the time properties of deterministic traffic, among other things. This in turn is enabled by the time-sensitive communications (TSC) framework introduced by 5G Release 16. Performance per MHz of available spectrum can be improved even further in absolute terms by taking advantage of 5G features such as advanced MIMO (multiple-input/multiple-output) radio antenna technology, beamforming, greater transmission power and so on.

Another important feature of 5G is its elaborate support for Quality of Service (QoS) flows, in which traffic with lower QoS requirements can coexist with traffic with more demanding requirements (such as URLLC) to maximize resource utilization. In order for this to work without compromising URLLC, 5G deploys preemptive scheduling (see [7]). This improves downlink multiplexing of enhanced mobile broadband (MBB) and latency-critical traffic; the gNB (short for gNodeB, referring to a 3GPP-compliant implementation of the 5G NR base station) may partly overwrite (i.e. preempt) an ongoing lower-priority transmission with shorter but more urgent URLLC data packets. Generally speaking, a large volume of traffic with demanding ultra-low latencies tends to reduce the radio network’s overall capacity.

5.3 Mobility and Coverage

Support for mobility is a requirement for many IIoT applications. Two situations can be distinguished: freedom of movement while remaining connected to the same gNB on the one hand, and mobility with support for seamless handover between gNBs or different cells of the same gNB while services continue without interruption on the other. Mobility support is essential whenever coverage limitations or capacity requirements make it necessary to deploy multiple gNBs within the coverage area. It should be noted that handovers can also be triggered by significant scattering within the deployment environment (for example, caused by moving machines or vehicles), and not only by wireless devices physically moving between cells. As shown in figure 3, a seamless handover takes place when a device switches an ongoing transmission from a source node (gNB) to a target node (gNB). The handover must be fast and efficient to prevent the QoS from degrading unacceptably.

Figure 3: Handover of a mobile terminal from a source cell to a target cell



In 5G, the network controls handovers to ensure fast, robust mobility. This must naturally also be supported by the device. The device transmits measurement reports that the network evaluates for deciding when to hand the device from the serving cell over to a neighboring cell. 5G includes several features that have improved handovers compared to 4G. For example, conditional handovers have been introduced to achieve more robust mobility while avoiding unnecessary handovers (see [8]). Another feature is based on dual-active protocol stacks (DAPS): the UE retains its connection to the source cell until it has successfully connected to the target cell. This seamless connectivity prevents the handover from causing a momentary glitch (see [9]). The use of spatial diversity with multi-TRP transmission strategies is another important enhancement in 5G; it prevents device connections from being interrupted by movements or moving objects. Overall, 5G ensures seamless mobility, including support for URLLC during handover, both when switching beams or carriers on the same gNB and between gNBs operating on the same frequency carrier (see references [19] and [11]). NR-U has inherited the same seamless handover functions that are available for NR, with the main difference concerning the reduced reliability of channel access that comes with operating in an unlicensed band.

Assuming full, seamless mobility for meeting service requirements, a wireless system's maximum overall coverage is equal to the combined coverage areas of all gNBs. Extending this idea, 5G could theoretically be scaled up for virtually unlimited coverage. For some applications, however, the greatest coverage achievable with a single gNB can also be relevant – for instance, because it is more straightforward to design the system for the minimum required capacity and latency at the edges of the defined coverage zone. This can help reduce the cost of installation, because less infrastructure is needed. The maximum supported range (or path loss) between a device and the access point antenna is limited by the transmission power level and receiver sensitivity, both of which depend on the spectrum rules and the capabilities of the equipment used. The coverage of 5G networks can be improved further by leveraging sectorization of the gNB, using advanced antenna schemes on both the gNB and the device, increasing the height of antennas, and/or integrating various link adaptation mechanisms.

5.4 UE Synchronization with 5G System Time

Absolute time synchronization over the air interface has been supported by 5G since Release 16. Besides being a key component for supporting IEEE Time Sensitive networking (TSN) and IEEE 802.1AS as described in section 7.3, it can also be used for synchronizing standalone 5G devices with the 5G system's time domain, which is usually Universal Coordinated Time (UTC).

How accurately UE time can be synchronized with 5G system time depends on several factors, which include the channel environment, cell size, and mobility. For IIoT environments, which typically have cells less than a hundred meters wide, the currently achievable performance is better than 540 ns over a single air interface (while compensating for propagation delays; see [12]). Manufacturers of Release 16 devices are currently free to implement proprietary solutions to compensate for propagation delays, but Release 17 will introduce standardized support for larger cells up to several kilometers across. Until the envisaged 3GPP solution for supporting propagation delay compensation becomes available, a synchronization accuracy of typically less than five microseconds is achievable in large macro cells.

6. Exposure Capabilities

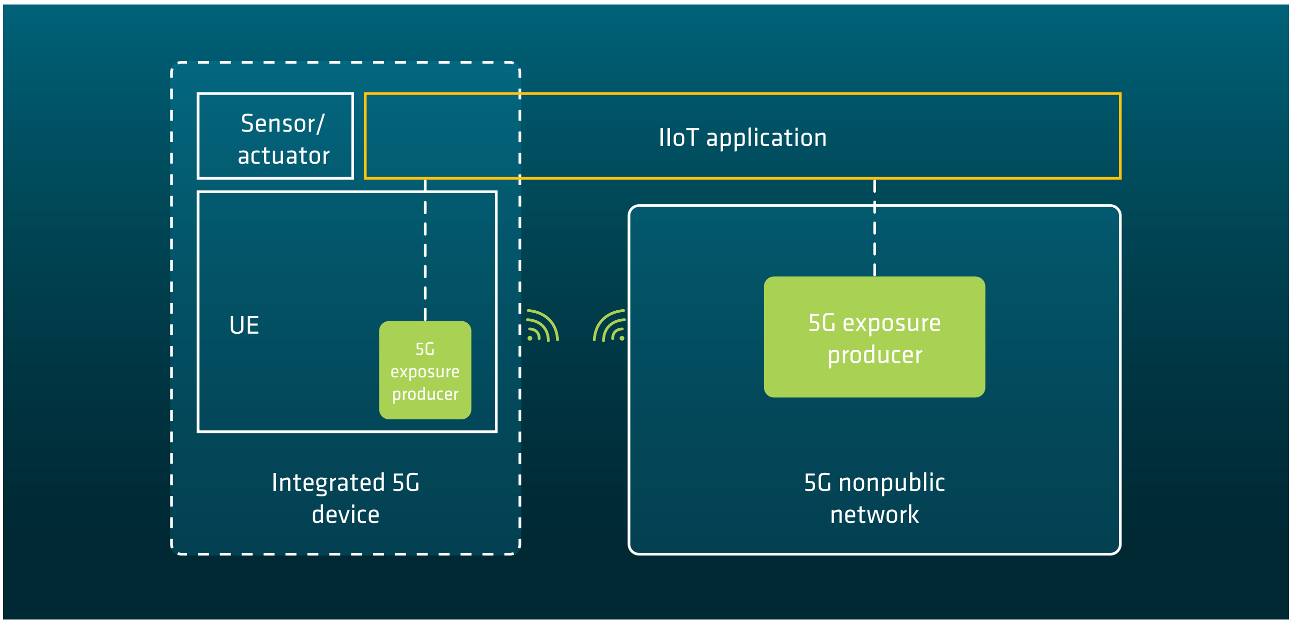
Industrial applications can access 5G network capabilities via so-called exposure interfaces. Examples of network capabilities that are "exposed" by the 5G system include communication service monitoring and network management capabilities. Another 5G-ACIA white paper (see [13] for details) provides a summary of exposure requirements from the standpoint of industrial applications. 5G exposure capabilities can be divided into two groups:

1. Management of end device communication services
2. Network monitoring

The 5G system provides so-called northbound APIs (application programmable interfaces) that allow integration with an OT application as shown in figure 4. These capabilities can be directly implemented using network exposure functions (NEFs) that are natively built into the 5G network. While interacting with other 5G core network functions, they securely expose 5G capabilities and events to third-party application functions. They also make it possible for third-party application functions to exchange information with the internal 5G network. In Release 16, 3GPP introduced the Service Enablement Architecture Layer (SEAL), which provides RESTful APIs. These APIs mask the complexity of 5G to permit quick and easy integration of a 5G network and 5G devices. The main capabilities provided by the SEAL include:

1. Group management service
2. Configuration management service for UE configuration and user profiles
3. Location management service for cells, service areas, and geographical coordinates
4. Identity and key management service for user authentication and authorization
5. Network resource management service for connectivity and QoS monitoring

Figure 4: : Exposure of 5G capabilities (source: [13])



7. Support for Ethernet-Based Industrial Networking

7.1 The 5G System as a Logical Ethernet Bridge

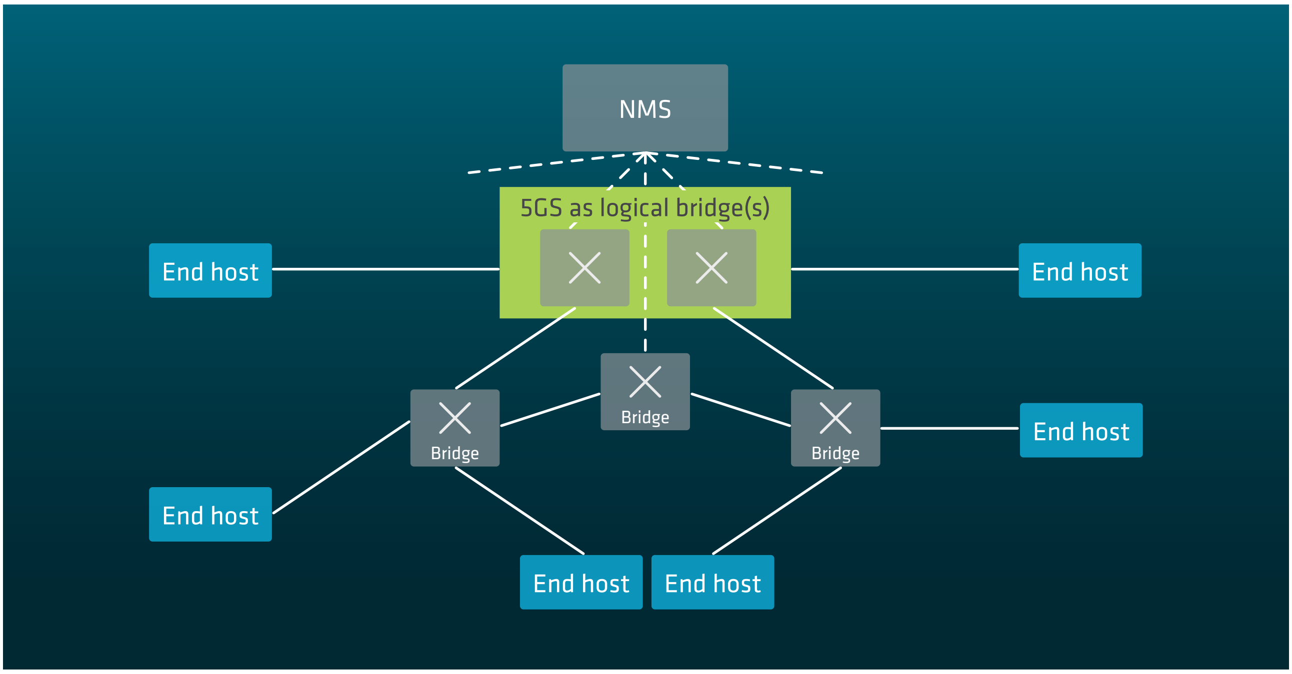
Ethernet is a family of computer networking technologies that are widely used in industry and elsewhere. In field-level applications, it is complemented by a number of fieldbus communication technologies (see reference [14]). It continues to spawn new, widely adopted variants that deviate to some extent from standard Ethernet depending on the real-time communication requirements in each case (see [15]).

The support that 5G technology provides for Ethernet is compatible with features of IEEE standards that are relevant to industrial automation. This allows seamless integration with existing Ethernet deployments such as local area networks (LANs) and time-sensitive networking (TSN) for industrial automation.

5G supports transport of standard IEEE 802.3 Ethernet traffic. For this purpose, the 5G system presents itself as a virtual bridge ready to integrate with existing network management systems (NMSs). These typically use network management protocols for this, like the Simple Network Management Protocol (SNMP) and management information bases (MIBs) as shown in figure 5. A 5G system deployed in an integrated Ethernet network architecture can have multiple 5G logical Ethernet bridges (see [16]). 5G also supports default Ethernet forwarding mechanisms such as flooding and MAC address learning.

A 5G logical bridge can expose its capabilities, including bridge and port management information like the Link Layer Discovery Protocol (LLDP) and VLAN (Virtual LAN), to obtain configuration information from the NMS and particularly that covered by IEEE 802.1Q. A 5G system generates Ethernet PDU (Protocol Data Unit) sessions for routing Ethernet traffic. These sessions also support real-time Ethernet communication systems by transporting their Ethernet frames and interconnecting real-time Ethernet devices.

Figure 5: 5G-integrated Ethernet network architecture



Since the 5G system is modeled as a logical Ethernet bridge, it can integrate with existing Ethernet network management systems. 5G supports TSN on the basis of the IEC/IEEE 60802 TSN Profile for Industrial Automation. This enables it to also support industrial protocols in higher layers, including OPC UA (the OPC Unified Architecture).

7.2 QoS and Support for TSN

7.2.1 Quality of Service

In many industrial use cases, a guaranteed level of service quality is desired for prioritized traffic. TSN- and Ethernet-based industrial networks use several techniques to ensure this. Similarly, the 5G system includes a QoS framework for setting up QoS flows. A QoS flow with the finest possible granularity makes it possible to very finely differentiate QoS levels in the 5G system. A QoS flow can be established for IP or Ethernet communication flows in such a way that each packet of a given flow is forwarded across the 5G system in the same way (e.g. for scheduling and admission control). These flows can be associated with different priority levels, packet delay budgets, and tolerable packet error rates.

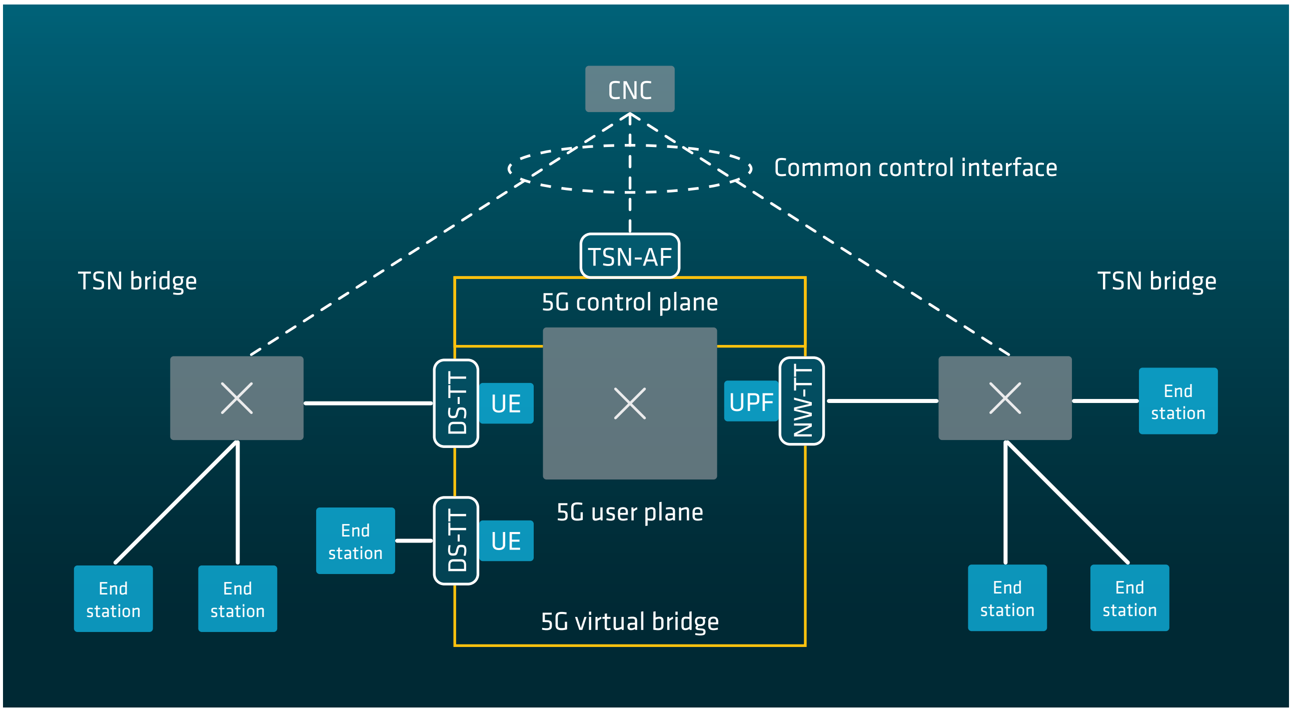
7.2.2 Support for Time-Sensitive Networking

Time-Sensitive Networking (TSN) is a set of open IEEE standards that define mechanisms for reliable, deterministic low-latency networking with IEEE 802.1Q LANs. 3GPP has introduced initial support for integration with wired TSN in Release 16, with further additions planned for Release 17. In other words, real-time TSN capabilities over standard Ethernet have been added to 5G. The 5G system is modeled as a TSN-capable Ethernet bridge, thus making it possible to integrate 5G with TSN to address use cases that are relevant to industrial automation, as validated in a 5G-ACIA white paper on TSN integration with 5G (see [17]).

The 5G system presents itself to an Ethernet network as a set of logical TSN-capable Ethernet bridges that provide Ethernet ports on the mobile device side (at the UE) and the network side (at the User Plane Function (UPF)) as shown in figure 6. Ethernet and TSN communication is possible between any of these Ethernet ports on the mobile device and network sides of the 5G system. Support for TSN communication between different mobile devices will be one of the additions in Release 17. 5G has a control plane function, namely the TSN Application Function (TSN AF), that interacts with the central TSN control plane function as defined in IEEE 802.1Qcc: the TSN Centralized Network Configuration (CNC).

5G bridge properties and 5G TSN functions are configured via the TSN AF. Ethernet/TSN traffic streams are mapped to 5G-specific QoS flows using the Priority Code Point defined by IEEE 802.1Q. 5G can configure service-specific treatments for different QoS flows. For time-critical traffic, for example, QoS flows for ultrareliable transmission with ultralow latency can be configured with the URLLC capabilities specified for 5G. The relevant TSN features supported by 5G are per-stream filtering and policing (defined in IEEE 802.1Qci), which can be used to guard against misbehaving traffic, and time scheduling (defined in IEEE 802.1Qbv) for differentiated treatment of critical traffic flows. These require both the core network and the devices to support 3GPP time-sensitive communications (TSC) features, which in turn makes it necessary, among other things, to include Network-Side TSN Translator (NW-TT) and Device-Side TSN Translator (DS-TT) functionality for interpreting TSN traffic in 5G, as shown in figure 6. The TSN AF also provides topology information as specified by the IEEE 802.1AB Link Layer Discovery Protocol (LLDP), thus making it possible to obtain, via a standardized interface, information on devices and bridges connected to the 5G system. Configuration of redundant transmissions through the 5G system is also supported.

Figure 6: 5G TSN integration



7.3 Support for Time Synchronization

Time synchronization is a fundamental TSN capability; TSN-enabled applications depend on it to unlock other TSN functionality such as time-aware scheduling. Release 16 of 5G supports synchronization between a grandmaster clock and any other node via the 5G system over Ethernet, applying the Generalized Precision Time Protocol (gPTP) specified by IEEE 802.1AS. This makes the 5G system behave like a time-aware system as defined in IEEE 802.1AS.

The 5G system relays gPTP timing information, with its residence time being calculated (see [18]) by its own internal process for synchronizing 5G devices, 5G base stations, and 5G user plane function (UPF) gateways using a shared 5G clock. In Release 16, the gPTP grandmaster clock must be located on the network side of the 5G system. Release 17 will also let it be connected to a 5G device for synchronizing other mobile devices or destinations on the network side. The maximum time error in the 5G system will be limited to 900 ns. Release 17 also extends time synchronization to support the Precision Time Protocol (PTP) over UDP/IP.

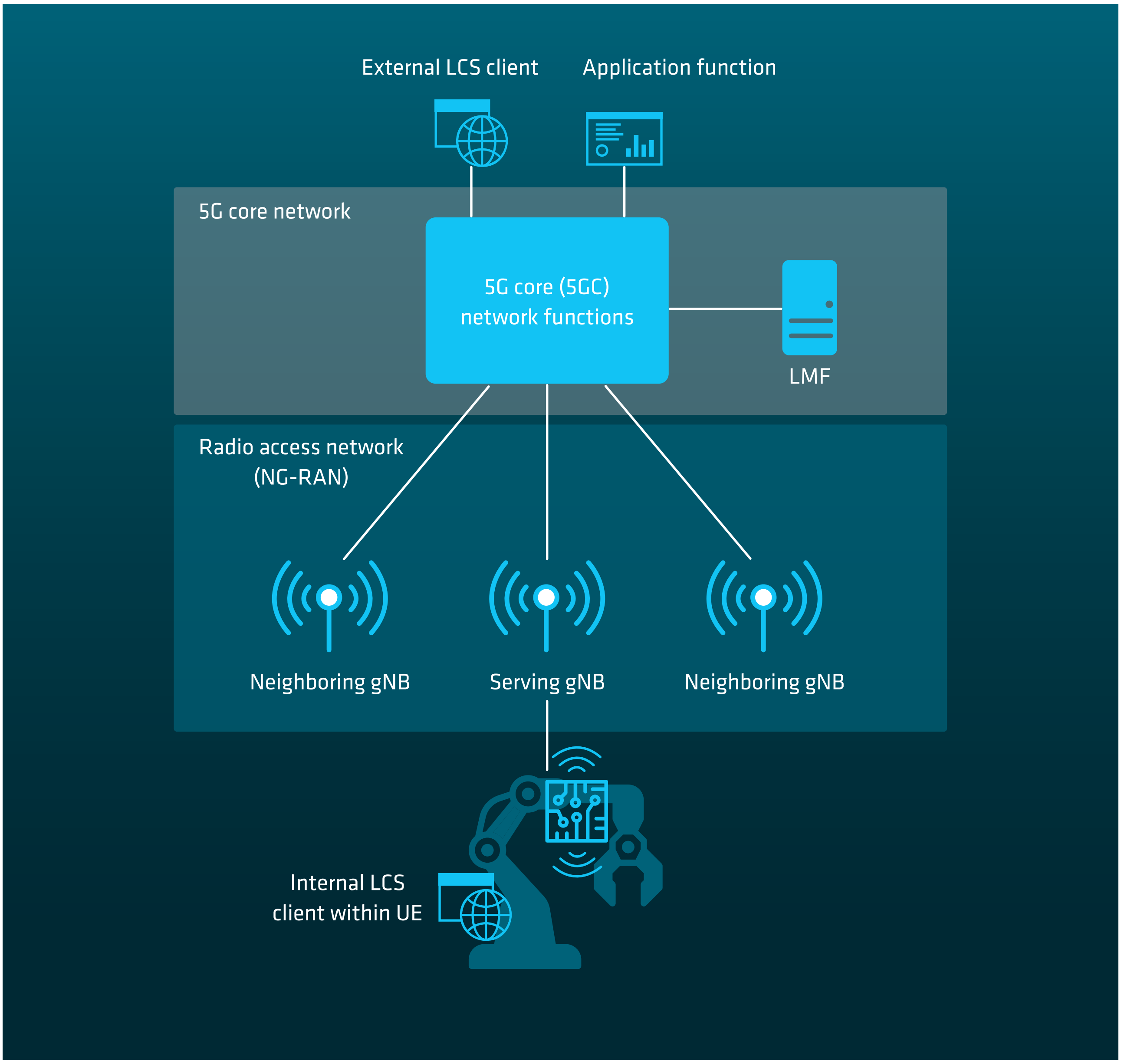
5G supports synchronization across a wide range of domains. They include network sharing scenarios such as two separate nonpublic 5G networks sharing the same 5G radio access network (see [18]). An essential aspect here is secure protection of synchronization messages sent over the 5G system from the grandmaster clock to equipment, similarly to other private data transmitted over the network. PTP messages are encrypted and can only be read by authorized devices.

8. Positioning

Three-dimensional positioning is an important capability in many industrial sectors. It is a prerequisite for quite a few things, including tracking personnel and assets, ensuring safety, locating tools in manufacturing and assembly facilities, optimizing supply chains, and controlling automatic guided vehicles. The required level of accuracy (see reference [19] for details) and the environmental and radio conditions under which positioning needs to be done can vary significantly.

The basic principles of 5G NR positioning are specified in 3GPP Release 16, and Dwivedi et. al. (in [20]) have provided an overview of the major improvements that have been made to it since 4G (also called LTE). Figure 7 contains an overview of the 5G location services (LCS) architecture, which can be broken down into core network (CN) and 5G RAN (NG-RAN) functions.

Figure 7: Simplified 5G LCS Architecture



An LCS client function or application function can initiate a location request with a set of QoS positioning parameters. LCS clients can reside in either the 5G CN or the mobile device (UE). An entity called the location management function (LMF) plays a key role. It interacts with serving and neighboring gNBs and UE to receive and process uplink (UL) and downlink (DL) positioning measurements for computing the UE's position. On the side of the next-generation radio access network (NG-RAN), some positioning techniques require multi-cell measurements, for example a downlink time difference of arrival (DL-TDOA), while others, like downlink angle of departure (DL-AoD), require a single serving cell to perform a positioning fix on the UE. The LMF may also provide the UE with data to support positioning (see [21] for details).

A key enabler for precise positioning in 5G is the use of mmWave frequency bands (ranging from 24 to 40 GHz) for wideband signals, beamforming, and precise estimation of angles using multiple antennas. The wideband signals can enable excellent time resolution and positioning accuracy on the order of decimeters with perfect synchronization of base stations (gNBs), in other words with a maximum sync error of less than 1 ns. Precise estimation of angles doesn't require base stations to be synchronized and therefore excellently complements solutions based on time difference of arrival (TDoA) measurements.

Performance simulations (see [20]) have shown that the current 5G standard can potentially achieve positioning accuracies of a few meters outdoors and several decimeters indoors, but falls short of the reliability required for industrial applications. Simulation results obtained during the study item phase of the positioning work carried out for Release 16 (see [22]) showed that the Release 16 target of a horizontal positioning error of less than 3 m for 80% of the UEs in commercial indoor use cases can be met under ideal conditions, which include perfect synchronization between base stations. This makes 5G positioning suitable for many use cases. However, it should be noted that 5G positioning techniques mainly rely on having a line of sight (LoS) between at least one base station and the UE. Depending on the amount of clutter present, such as machines, metallic objects, shelves, etc., an industrial environment may require dense deployment of gNBs to ensure LoS for enough of them to achieve highly reliable decimeter-level positioning accuracy.

In highly cluttered environments, positioning accuracy can be improved by using devices with integrated sensors instead of increasing the density of the gNBs. For example, an inertial measurement unit (IMU) provides an accelerometer, gyroscope, and sometimes magnetometer measurements that can be used to track a device's movements.

Many manufacturing use cases are indoors, implying that solutions based on the global navigation satellite system (GNSS) will face challenges due to the very low signal levels and resulting poor or nonexistent coverage there. For outdoor use cases that more readily allow the use of GNSS, 5G includes broadcasting of positioning assistance data like those used for GNSS-Real Time Kinematics (GNSS-RTK), thus potentially achieving a positioning accuracy on the order of centimeters (see [23]). Even without the use of GNSS-RTK, however, the current 5G Release 16 standard can potentially provide positioning accuracy on the order of 10 m in outdoor networks, including those deployed for national or regional coverage. The 5G standard also supports other non-3GPP positioning technologies involving signaling, such as Terrestrial Beacon Systems (TBS), sensors (e.g., barometer, IMU), and WLAN/Bluetooth-based positioning (see [24]). The 5G system also supports a combination of high-precision positioning with local indoor deployment and less accurate positioning with outdoor macro deployment, which can be useful when moving between buildings in an industrial campus area or for logistics use cases, to cite two examples. Non-3GPP positioning technologies can also be coupled with radio-based 3GPP 5G hybrid positioning methods for enhanced accuracy.

Work to standardize positioning in Release 17 is still in progress and expected to be finalized in 2022. The declared objectives specifically emphasize IIoT use cases. The goal pursued by the improvements currently being made to the 5G standard is to achieve an indoor positioning accuracy of fewer than 20 centimeters for 90% of UEs (see [25]). Another enhancement now being discussed involves reducing the end-to-end positioning latency to less than 100 ms in order to minimize the overall "time to first fix" (TTFF), a measure of the time required to acquire relevant data and calculate a position. The Release 17 improvements are listed in in the 3GPP Study on NR Positioning Enhancements (reference [25]) and include reductions in UE Rx/Tx (reception/transmission) and/or gNB Rx/Tx timing delays as well as more accurate UL AoA (angle of arrival) and DL AoD (angle of departure) measurements and reporting.

The 5G positioning framework also has potential for integrating new scenarios to achieve greater energy efficiency and identify the positions of equipment relative to other devices in the network. Future enhancements of 5G may also add support for low-power, high-accuracy absolute and relative positioning applications such as tool tracking with extended battery lifetime requirements, which are essential for IIoT use cases.

9. Security

When wires are no longer used for connections, measures to secure communications shouldn't rely exclusively on physical safeguards. 5G integrates security features for securing communications across the radio interface and throughout the 5G system.

5G provides mutual authentication between an industrial 5G device's modem and the 5G network via the radio interface. This blocks unauthorized devices from accessing the network while also preventing legitimate devices from connecting to a fake or wrong network. Mutual authentication is the prerequisite for using the 5G key hierarchy to encrypt all traffic flowing between devices and the network and thus ensuring the wireless link's integrity and confidentiality. These mechanisms securely encrypt traffic passing over the radio interface to obscure content even if it is intercepted. The content is protected from being altered in any way and the identities of the sender and receiver are concealed. Depending on security requirements, protection can be additionally applied at the level of the OT (over-the-top) application using the IPSec (Internet Protocol Security), TLS (Transport Layer Security), DTLS (Datagram Transport Layer Security) or another suitable protocol.

Two methods are available for performing mutual authentication and executing the associated security functions:

- In the case of a PNI-NPN (Public Network Integrated Nonpublic Network) or when directly accessing a public network, it's necessary to use mutual authentication based on a USIM (Universal Subscriber Identity Module). The USIM contains the 5G subscriber's identity and the corresponding long-term secret cryptographic key. The default mechanism for deploying the USIM is a removable UICC, commonly referred to as a "SIM card", but the USIM can also be implemented on an embedded or integrated UICC onto which a profile (eSIM) can be loaded. The advantage of using a UICC is that the long-term key can never leave the UICC, thus effectively preventing any cloning of USIMs.
- In the case of SNPNs (Standalone Nonpublic Networks), it isn't mandatory to use an USIM. This makes it possible to develop and introduce deployment options for the 5G authentication function on the industrial device, which can be optimized for integration with the industrial domain. Non-USIM models of this type can also use hardware-based security, in which an industrial device could use a secure element as an anchor for safeguarding the industrial protocol layer. This can then potentially also be used as a trusted storage and execution environment for 5G authentication.

In addition to mutual authentication and protection of the wireless link, traffic control capabilities are provided and can be used to protect industrial networks. It should be stressed that these capabilities aren't directly bound to the 5G mutual authentication described above and are therefore available regardless of whether USIM/UICC or another authentication mechanism is employed. They are especially useful if security can't be provided at the level of the industrial network protocol. The security of such a (legacy) industrial network is based on physical isolation, which could potentially be breached by adding wireless access capabilities to the network. Fortunately, the 5G system has also been equipped with features for preventing certain devices from interacting with the industrial network, even if they have a valid USIM.

At a high level, this can be achieved by using a 5G network slice and/or closed access groups (CAGs), with access to them being limited to members of the industrial network. The user plane function (UPF) of the 5G core network can also restrict access to certain segments of industrial networks (known as data networks or DNs) and even enforce policies in individual streams, making it possible to filter traffic on the basis of (for example) application, source, and/or destination addresses or VLAN IDs. This gives the industrial network's operator very fine-grained control over traffic flowing within the industrial network in order to meet QoS requirements while isolating traffic to secure the network.

3GPP is continuing to improve 5G security to meet the operational needs of OT use cases, taking approaches similar to Network Slice-Specific Authentication and Authorization (NSSAA) and data-network-specific ("secondary") authentication (introduced in 3GPP Releases 16 and 15, respectively).

10. Standardization, Conformance, and Testing

In order for a communication system like 5G to operate reliably, all of its components need to seamlessly and flawlessly work and interact. 5G continues the legacy of previous cellular system generations that have been successfully doing this for decades. The 5G standards include functional specifications for system components as well as requirements that they must comply with standards and conformance testing specifications. 5G certification programs are extensive and include testing of most of the system's standardized functionality, including its performance. This is intended to make sure that 5G devices from any vendor can be used in any 5G network. Not all Industrial IoT features are currently covered, however.

3GPP radio access network working groups RAN WG1, RAN WG2, RAN WG3, and RAN WG4 are responsible for defining the requirements for standards-compliant radio functionality for base stations and devices (see references [26] and [27]). RAN WG4 defines the conformance testing specifications for base stations, covering radio transmitter and receiver characteristics and radio frequency performance (see references [28] and [29]).

The conformance testing specifications for devices are defined by RAN WG5 and cover radio transmitter and receiver characteristics, RF performance, radio resource management (RRM), and the functionality of all protocol layers for the RAN, the core network, and the IMS (IP Multimedia Services) service layer (see [30]).

Device conformance specifications are used for certification by, for example, the Global Certification Forum (GCF) (see [31]) and the PTCRB (see [32]). On the device side, the requirements for conformance address a variety of UE radio access capabilities that have been standardized in 5G (see [33]).

All this is intended to ensure that certified 5G devices will perform in accordance with their tested specifications and deliver the stated UE capabilities. Manufacturers are responsible for making sure that their devices are tested by an accredited laboratory in order to qualify for certification.

11. Conclusions

5G delivers a number of capabilities that enable advanced industrial use cases (including isochronous real-time motion control, sensor systems for monitoring critical processes, and AR/VR applications) for deployment over a single wireless communication system. They include both stringent communications requirements and integration capabilities to enable 5G to seamlessly blend in or coexist with preexisting and evolving Ethernet technologies. 5G-ACIA has a strong history of adapting 5G specifications to meet demanding use cases in the IIoT sector. In addition to presenting the IIoT capabilities of 5G based on extensive analyses carried out by 5G-ACIA, this white paper discusses various ways to add 5G communications to IIoT scenarios, including options for accessing and using frequency spectrum.

For more information on the capabilities of 5G in the context of IIoT, interested readers are invited to read these other 5G-ACIA white papers:

- Key 5G Use Cases and Requirements
- 5G for Automation in Industry
- 5G for Connected Industries and Automation (Second Edition)
- 5G Non-Public Networks for Industrial Scenarios
- Performance Testing of 5G Systems for Industrial Automation
- Integration of 5G with Time-Sensitive Networking for Industrial Communications
- Integration of Industrial Ethernet Networks with 5G Networks
- Security Aspects of 5G for Industrial Networks
- Exposure of 5G Capabilities for Connected Industries and Automation Applications

5G-ACIA is committed to helping the industrial networks community understand and apply 5G technology. New publications are made available at Publications - 5G-ACIA.

12. Key Terms and Definitions

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

5G-ACIA
5G-ACIA is the globally leading organization for shaping and promoting Industrial 5G.

13. Acronyms

3GPP
3rd Generation Partnership Project

5G-ACIA
5G Alliance for Connected Industries and Automation

AR/VR
Augmented reality/virtual reality

CN
Core network

DS-TT
Device-side TSN translator

gNb
5G base station

IEEE
Institute of Electrical and Electronics Engineers

LAN
Local area network

LCS
Location services

LMF
Location management function

NG-RAN
5G radio access network

NMS
Network management system

NPN
Nonpublic network (private network)

NR
New Radio (5G radio)

NW-TT
Network-side TSN translator

PNI-NPN
Public network integrated nonpublic network

QoS
Quality of service

RAN
Radio access network

SNPN
Standalone NPN

SIM
Subscriber identity module

TSC
Time-sensitive communications

TSN
Time-sensitive networking

UE
User equipment

UICC
Universal integrated circuit card (a physically secure device for storing USIM applications)

UPF
User plane function

URLLC
Ultra-reliable low latency communications

USIM
Universal subscriber identity module

14. References

[1] 5G-ACIA, "5G-ACIA whitepaper: 5G Non-Public Networks for Industrial Scenarios," 2020. [Online]. Available at: https://5g-acia.org/wp-content/uploads/2021/04/WP_5G_NPN_2019_01.pdf.

[2] 3GPP, "TS38.300 - NR and NG-RAN Overall description; Stage-2," 2020. [Online]. Available at: https://www.3gpp.org/ftp//Specs/archive/38_series/38.300/38300-g30.zip.

[3] T.-K. Le, U. Salim and F. Kaltenberger, "An overview of physical layer design for Ultra-Reliable Low-Latency Communications in 3GPP Release 15 and Release 16," February 2020. [Online]. Available at: https://arxiv.org/pdf/2002.03713.pdf.

[4] 3GPP, "RP-210490 - Report on Evaluations for 5G-ACIA," March 2021. [Online]. Available at: https://www.3gpp.org/ftp/tsg_ran/TSG_RAN/TSGR_91e/Docs/RP-210490.zip.

[5] Ericsson, "5G URLLC - Achieving industrial automation," 2021. [Online]. Available at: https://www.ericsson.com/en/cases/2020/accelerate-factory-automation-with-5g-urllc.

[6] 3GPP, "R1-1901470 Reply LS on TSN requirements evaluation," January 2019. [Online]. Available at: ftp://ftp.3gpp.org/tsg_ran/WG1_RL1/TSGR1_AH/NR_AH_1901/Docs/R1-1901470.zip.

[7] K. I. Pedersen, G. Pocovi and J. Steiner, "Preemptive Scheduling of Latency Critical Traffic and Its Impact on Mobile Broadband Performance," in IEEE 87th Vehicular Technology Conference (VTC Spring), Porto, 2018.

[8] I. Leonardo Da Silva, C. Eklöf, J. Muller and R. Zhohov, "This is the key to mobility robustness in 5G networks," Ericsson, May 2020. [Online]. Available at: https://www.ericsson.com/en/blog/2020/5/the-key-to-mobility-robustness-5g-networks.

[9] O. Ohlsson, P. Wallentin and C.-G. Persson, "Reducing mobility interruption time in 5G networks," Ericsson, April 2020. [Online]. Available at: https://www.ericsson.com/en/blog/2020/4/reducing-mobility-interruption-time-5g-networks.

[10] 3GPP, "TR37.910 - Study on self evaluation towards IMT-2020 submission," 2019. [Online]. Available at: https://www.3gpp.org/ftp//Specs/archive/37_series/37.910/37910-g10.zip.

[11] I. Viering, H. Martikainen, A. Lobinger and B. Wegmann, "Zero-Zero Mobility: Intra-Frequency Handovers with Zero Interruption and Zero Failures," IEEE Network Magazine, no. April, 2018.

[12] 3GPP, "TR38.825 - Study on NR industrial Internet of Things (IoT)," 2019. [Online]. Available at: https://www.3gpp.org/ftp//Specs/archive/38_series/38.825/38825-g00.zip.

[13] 5G-ACIA, "Exposure of 5G Capabilities for Connected Industries and Automation Applications," February 2021. [Online]. Available: https://5g-acia.org/5g-acia_exposure_of_5g-capabilities_for_connected_industries_and_automation_applications_single-pages/. [Accessed on 23 June 2021].

[14] IEC, "61784-1:2019 Industrial communication networks - Profiles Part 1: Fieldbus profiles," April 2019. [Online]. Available at: https://webstore.iec.ch/publication/59887.

[15] IEC, "61784-2:2019 Industrial communication networks - Profiles - Part 2: Additional fieldbus profiles for real-time networks based on ISO/IEC/IEEE 8802-3," April 2019. [Online].

[16] Patel et al., "5G-SMART deliverable D5.1, "First Report on 5G network architecture options and its assesements"," November 2020. [Online]. Available at: https://5gsmart.eu/wp-content/uploads/5G-SMART-D5.1.pdf. [Accessed Sept 2021].

[17] 5G-ACIA, "Integration of 5G with Time-Sensitive Networking for Industrial Communications," 2021. [Online]. Available: https://5g-acia.org/5g-acia_integration_of_5g_with_time-sensitive_networking_for_industrial_communicatins_single-pages/. [Accessed 23 June 2021].

[18] Godor et al., “A Look Inside 5G Standards to Support Time Synchronization for Smart Manufacturing,” IEEE Communications Standards Magazine, vol. 04, no. 03, 2020.

[19] 3GPP, “TS22.261 - Service requirements for the 5G system,” 2021. [Online]. Available: https://www.3gpp.org/ftp/Specs/archive/22_series/22.261/22261-i30.zip. [Accessed 30 June 2021].

[20] Dwivedi et al., “Positioning in 5G networks,” 2021. [Online]. Available: https://arxiv.org/pdf/2102.03361.pdf. [Accessed 23 June 2021].

[21] 3GPP, “TS23.271 - Functional stage 2 description of Location Services (LCS),” 2021. [Online]. Available at: https://www.3gpp.org/ftp//Specs/archive/23_series/23.271/23271-g00.zip.

[22] 3GPP, “TR38.855 - Study on NR positioning support,” 2019. [Online]. Available at: https://www.3gpp.org/ftp//Specs/archive/38_series/38.855/38855-g00.zip. [Accessed 2 July 2021].

[23] Ericsson, “LTE Positioning and RTK: Precision down to the centimeter,” [Online]. Available: https://www.ericsson.com/en/blog/2018/11/lte-positioning-and-rtk-precision-down-to-the-centimeter.

[24] 3GPP, “TS38.305 - Functional stage 2 description of Location Services (LCS),” [Online]. Available: https://www.3gpp.org/ftp/Specs/archive/38_series/38.305/38305-g50.zip. [Accessed 9 Sept 2021].

[25] 3GPP, “TR38.857 - Study on NR Positioning Enhancements,” 2021. [Online]. Available at: https://www.3gpp.org/ftp/Specs/archive/38_series/38.857/38857-h00.zip. [Accessed 23 June 2021].

[26] 3GPP, “List of RAN1 Technical Specifications and Technical Reports,” [Online]. Available: https://www.3gpp.org/DynaReport/TSG-WG--r1.htm.

[27] 3GPP, “List of RAN4 Technical Specifications and Technical Reports,” [Online]. Available at: https://www.3gpp.org/DynaReport/TSG-WG--R4.htm.

[28] 3GPP, “TS38.141-1 - NR; Base Station (BS) conformance testing Part 1: Conducted conformance testing,” 2020. [Online]. Available at: https://www.3gpp.org/ftp/Specs/archive/38_series/38.141-1/.

[29] 3GPP, “TS38.141-2 - NR; Base Station (BS) conformance testing Part 2: Radiated conformance testing,” 2020. [Online]. Available at: https://www.3gpp.org/ftp/Specs/archive/38_series/38.141-2/.

[30] 3GPP, “RAN5 - Mobile terminal conformance testing,” [Online]. Available at: https://www.3gpp.org/Specifications-groups/ran-plenary/49-ran5-mobile-terminal-conformance.

[31] “Global Certification Forum,” [Online]. Available at: https://www.globalcertificationforum.org/.

[32]“PTCRB,” [Online]. Available: https://www.ptcrb.com/.

[33] 3GPP, “TS 38.306 NR; User Equipment (UE) radio access capabilities (Release 16),” 2021. [Online]. Available at: https://www.3gpp.org/ftp/Specs/archive/38_series/38.306/38306-g60.zip

[34] NTT Docomo, “Field Experiments on 5G Ultra-Reliable Low-Latency Communication (URLLC),” July 2018. [Online]. Available at: https://www.nttdocomo.co.jp/english/binary/pdf/corporate/technology/rd/technical_journal/bn/vol20_1/vol20_1_003en.pdf.

[35] Nokia, “5G and Wi-Fi6 radio: options for operational technology,” 2020. [Online]. Available at: https://onestore.nokia.com/asset/207850.

[36] Nokia, “5G New Radio Unlicensed,” 2021. [Online]. Available at: https://onestore.nokia.com/asset/210366?_ga=2.63841071.1842850492.1620807913-36346702.1583570076.

11 5G-ACIA Members

As of November 2021

5G to go

AALBORG UNIVERSITY
DENMARK

ABB

AI-LINK

altran
Part of Capgemini

arm

ASKEY

ASOCS®

ATHONET

aurelis

Baicells

BAYFU

BECKHOFF

BOSCH

Canon

celona

中国移动
China Mobile

cisco

CONGIV

DASSAULT SYSTEMES

DENSO

Deutsche Messe

DFKI

CATAPULT
Digital

NTT
docomo

Druid

EMERSON.

Endress+Hauser

ERICSSON

ETRI

FESTO

flex.

Fraunhofer

GHMT®

HARTING

HIRSCHMANN
A BELDEN BRAND

HMS

HUAWEI

IDLab
INTERNET & DATA LAB

ifak

ifm

III
財團法人資訊工業策進會
INSTITUTE FOR INFORMATION INDUSTRY

Infineon

inIT

intel.

ITRI
Industrial Technology
Research Institute

KETI

KEYSIGHT
TECHNOLOGIES

Lenovo
LS telcom
MAVENIR
MC TECHNOLOGIES

Microsoft
MITSUBISHI ELECTRIC
MOXA
MUGLER TELCO NETWORKS.

Nitto
NOKIA
NXP
orange™

Panasonic
PEPPERL+FUCHS
PHŒNIX CONTACT
Qualcomm

R3 RELIABLE REAL-TIME RADIO
Radisys
ROHDE&SCHWARZ
SAL SILICON AUSTRIA LABS

salzburgresearch
Schneider Electric
SICK
SIEMENS

SINTEF
SoftBank
SONY
ST life.augmented

T · ·
TRUMPF
TZi
ublox

UPLINK
verizon✓
VIAVI
VIAVI Solutions
vodafone

VOLKSWAGEN AKTIENGESELLSCHAFT
WAGO
Weidmüller
XITASO

YOKOGAWA ◆
ZTE

5G-ACIA White Paper
5G for Industrial Internet of Things (IIoT):
Capabilities, Features, and Potential

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

Published by
ZVEI e. V.
5G Alliance for Connected Industries and
Automation (5G-ACIA), a Working Party of ZVEI e. V.
www.zvei.org

November 2021

www.5g-acia.org