5G-ACIA White Paper

Exposure of 5G Capabilities for Connected Industries and Automation Applications

5G Alliance for Connected Industries and Automation

Table of Contents

1 Abstract

This white paper describes the functional requirements for exposing the capabilities of non-public 5G systems to connected industries and automation applications.

Via exposure interfaces, industrial applications can access 5G capabilities for factory and process automation, production IT, and logistics and warehousing. Industrial applications also have access to communication service monitoring and network management capabilities. Due to the generic nature of the exposed capabilities, it is also possible to support other use cases that share the requirements of factory applications. Examples include control applications for rail transportation, electrical power distribution, and central power generation.

Exposed capabilities comprise two major groups:

- The first group focuses on device management, in particular use cases related to the management of communication services for devices.
- The second group focuses on network management, in particular operations and maintenance tasks for the 5G non-public network (NPN).

2 Introduction

2.1 Motivations for using 5G in industry

One of the main differences between 5G and previous generations of cellular networks is 5G's strong focus on machine-type communication and the Internet of Things (IoT). The capabilities of 5G therefore extend far beyond mobile broadband.

5G supports highly reliable communication with very low latency. 5G also supports massive connectivity for IoT applications. These new capabilities enable new use cases in many vertical domains, including the automotive industry, healthcare, agriculture, energy, and other manufacturing sectors. For discrete manufacturing, for instance, 5G enables reliable wireless connectivity, which will support flexible restructuring of production lines and assets. More details on pertinent use cases and 5G network capabilities are provided in reference [11].

2.2 The role of 5G as a multi-service network

The 5G vision is one of a true multi-service network that can address the connectivity needs of virtually any application imaginable in the consumer, enterprise and industrial IoT space. To this end, 3GPP has specified 5G to support enhanced mobile broadband, massive-scale IoT, and ultra-reliable and low-latency communication. 5G networks are also expected to provide unprecedented levels of flexibility compared to previous technology generations, enabling the cost-effective delivery of new services thanks to virtualization, network slicing, and edge-computing capabilities.

For connected industries and automation applications, these services will be provided both by 5G non-public networks (NPNs) deployed in stand-alone mode (stand-alone NPNs, SNPNs), as well as by NPNs deployed and operated by mobile network providers (public network-integrated NPNs, PNI-NPNs) on behalf of an enterprise. These deployment scenarios are described in more detail in reference [2].

2.3 Changes compared to version 1.0

The changes compared to version 1.0 of this white paper, which was published in June 2020, are as follows.

- All requirements described in this white paper are now enumerated.
- Network management use cases were added to the annex (see Section 9.2) and the implications for 5G systems are discussed in Section 4.3.2.
- 3GPP TSG WG1 requirements of Release 17 were analysed in [5] and [6]; this present white paper identifies the corresponding requirements related to exposure interfaces and presents a gap analysis compared to version 1.0 of this white paper. For 3GPP TSG WG1 requirements not covered in version 1.0, service exposure requirements were formulated and added to the pertinent sections.
- Typical parameters for QoS monitoring were added to the annex (see Section 10).

2.4 Structure and scope

The current white paper addresses requirements identified by 5G-ACIA and requirements described in relevant documents of 3GPP Release 17 (see references [5] and [6]). This paper identifies requirements outlined in respective 3GPP specifications that are needed to describe and explain operational use cases. However, readers are encouraged to study references [5] and [6] for a complete overview.

This white paper focuses on use cases and exposure interface implementation but does not address aspects such as data models and protocols – which are commonly part of interface specification work.

The next section presents essential assumptions, without which the requirements described in this white paper cannot be properly understood.

Section 4 introduces service exposure requirements for various operational use cases.

A summary and outlook are presented in Section 5. Definitions of terms and abbreviations used in this white paper are provided in Section 6.

Section 7 lists references given in this white paper.

There are three annexes, A (Section 8), B (Section 9), C (Section 10). Section 8 describes architecture concepts for 5G exposure interfaces, Section 9 describes operational use cases in more detail, and Section 10 identifies typical parameters for QoS monitoring and 5G system key performance indicators (KPIs).

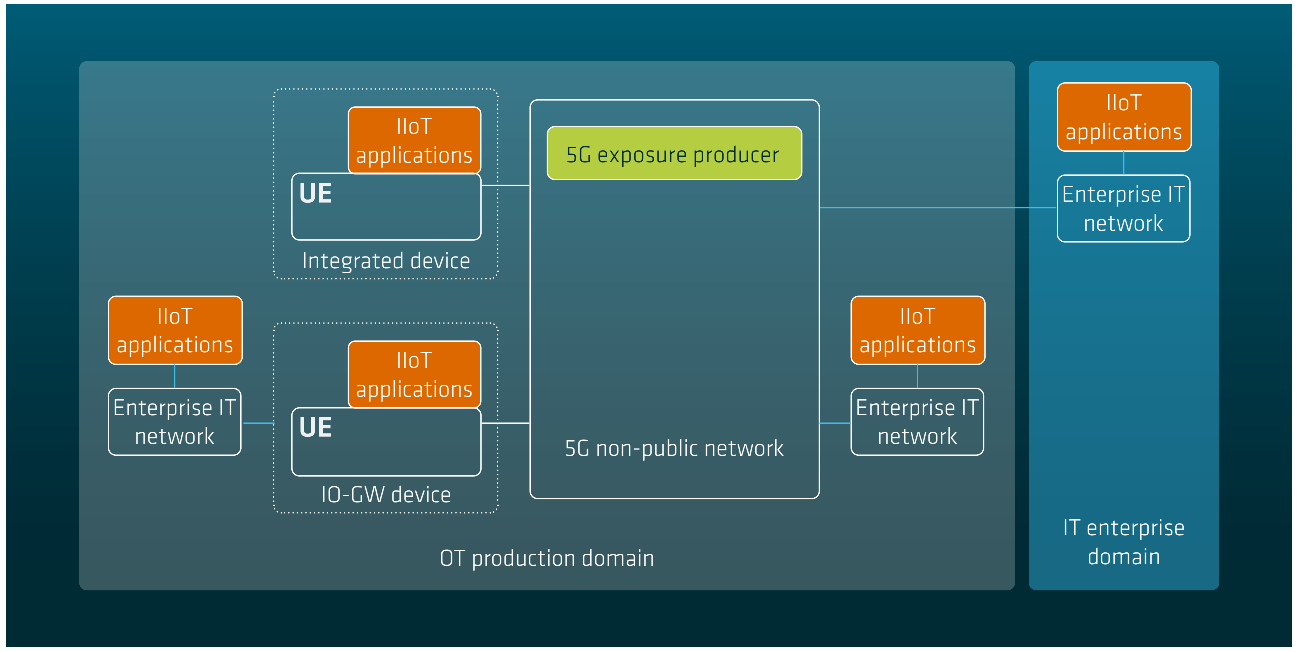
3 Essential assumptions

This white paper focuses on how to expose the capabilities of 5G non-public networks (NPN) to connected industries and in particular automation applications. These applications are referred to in this document as Industrial Internet of Things (IIoT) applications.

Some essential solution assumptions are defined in this section in order to make the specified requirements easier to understand. These assumptions do not preclude any specific exposure interface implementation.

One such basic assumption is that the 5G NPN provides communication services between wireless devices, and between wireless devices and wired data networks. The primary role of exposure interfaces is to manage the user plane of the 5G NPN. The user plane supports the transmission of application

Fig. 1: User plane view of devices and networks connected via a 5G non-public network.



Source: 5G-ACIA

data at layers two and/or three of the OSI model of networking.

Figure 1 shows how devices can be connected wirelessly to the 5G NPN. It also depicts non-3GPP operational technology (OT) networks and enterprise IT networks. IIoT applications are deployed in the enterprise IT domain, in non-3GPP OT networks, and in devices. The IIoT applications are software entities that consume the services of the 5G exposure interfaces as outlined in, for instance, reference [3].

Devices and non-3GPP networks may belong to multiple domains, such as the OT production domain and the IT enterprise domain. These domains are defined and explained in reference [10].

A device in this context is assumed to consist of the following components that are essential for 5G exposure:

- an item of user equipment (UE), providing the connectivity function (see reference [9])
- sensors/actuators or controllers/managers integrated into the device and/or an input-output gateway function (IO-GW), which enables connection of device-external sensors/actuators, controllers/managers or other non-3GPP OT networks
- a local IIoT application function that consumes services of the exposure interfaces
- a compute and store platform on which the IIoT application is deployed

The 5G-ACIA white paper *Integration of Industrial Ethernet Networks with 5G Networks* [10] describes the various communication scenarios, with diverse devices, sensors, actuators and controllers.

It should be noted that a 5G NPN can connect to non-3GPP networks, for instance TSN networks; this option is not explicitly shown in Figure 2.

The requirements given in Section 4 are based on the assumptions listed below and illustrated in Figure 2:

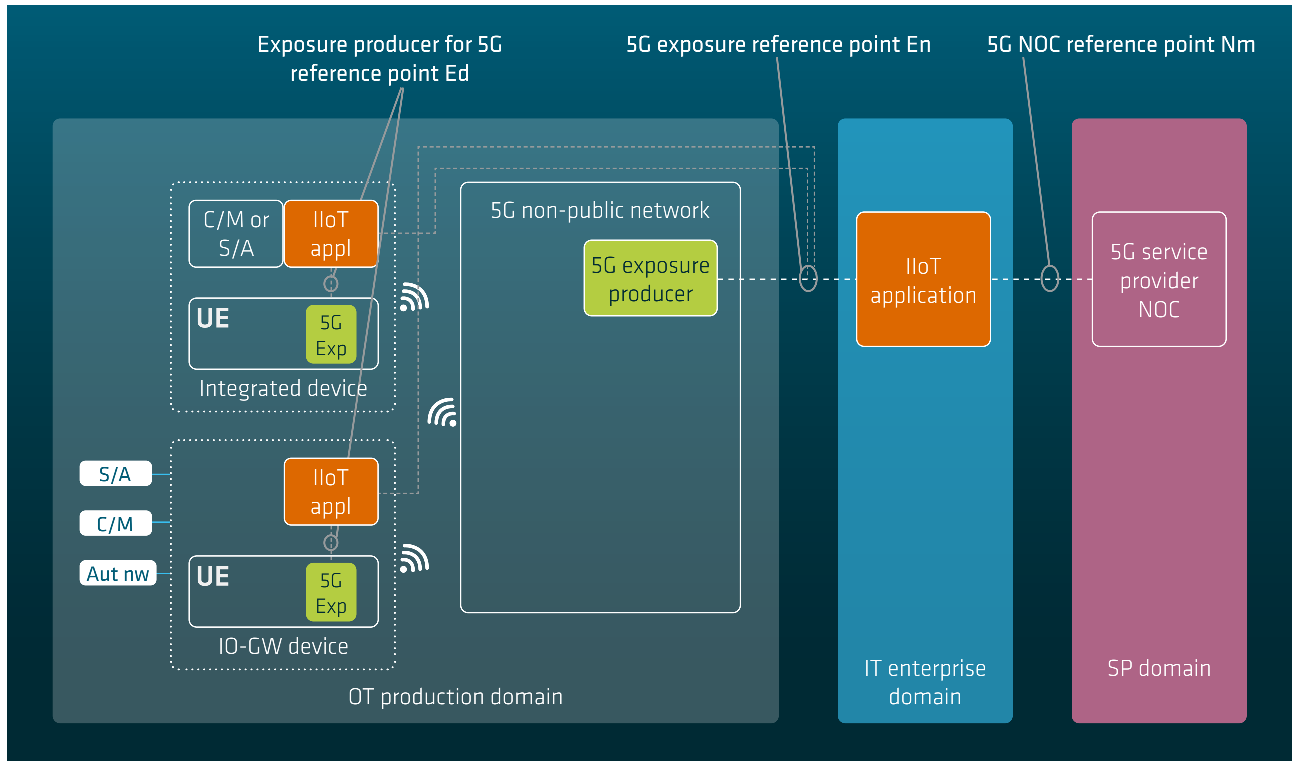
- The exposed 5G services are integrated with the IIoT applications via industry-compliant reference points.
- The 5G exposure services are available via two reference points, Ed and En. These reference points are situated between the IIoT application and the 5G system. Ed is the reference point between a UE and an IIoT application, and En is the reference point between the 5G NPN and an IIoT application. 5G services exposed via the En reference point are accessible via IIoT applications running on any compute node, i. e. applications deployed on a device or on a network node in both the OT production and IT enterprise domains.
- The 5G NPN user plane is managed (e. g. connections established, monitored, changed, terminated, etc.) by the services exposed via the reference points.
- Network management and configuration services required by IIoT applications are made available by the 5G service provider via the 5G network operation center (NOC) reference point Nm (see Section 4.3.2). These services apply to all corresponding stages in the 5G network life cycle, e. g. network installation, initial configuration, software management, and network decommissioning.

The corresponding services are specific to NOC implementation and are a matter of agreement between the service provider and the enterprise (e. g. the factory operator). A detailed description of services exposed via the reference point Nm are beyond the scope of this white paper. Nm is included here for completeness only.

- Services may be provided by, e. g. the factory operator or by a third-party provider, for instance a mobile network operator. In the latter case, the service provider's NOC is located within the service provider (SP) domain, which is a public network from the factory operator's perspective.

More information is provided in Annex A.

Fig. 2: Deployment of reference points



Source: 5G-ACIA

4 Requirements for 5G exposure reference points

4.1 Overview

This section describes the requirements for 5G exposure reference points. The requirements are based on the use cases documented in the 3GPP technical report TR 22.804 [3], other relevant industry standards and documents, as well as the use cases given in Annex B. Other relevant use cases and the primary functions to be provided by 5G systems are summarized in reference [1], while pertinent 3GPP requirements are documented in technical specifications [5] and [6].

Implementation of 5G exposure reference points should reflect the following design philosophy:

1. Usability and simplicity, i. e. the reference points must provide a level of abstraction suitable for IT and OT professionals who do not possess in-depth knowledge of 5G systems.
2. Modularity and extensibility, i. e. it must be possible to make certain reference point functions optional and to enrich the reference points with new functions in a backward-compatible manner.
3. Service-based interfaces implemented in a service-oriented way, e. g. by means of open RESTful APIs.
4. A common time base at the reference point must be applied, so that the IIoT application can correlate exposed events correctly, e. g. connectivity monitoring events.

Requirements for 5G exposure reference points are structured into the following subsections:

Device management (Section 4.2):
- device identity management
- device provisioning and onboarding
- device connectivity management
- device connectivity monitoring
- device group management
- device location information

Network management (Section 4.3):
- network monitoring
- network configuration and maintenance

Security (Section 4.4)

4.2 Device management

The requirements described in this section, and detailed procedures for device provisioning and onboarding, are based on references [3] and [4], while references [4], [5] and [6] are the main sources for operational use cases.

Some requirements described in this document have been identified directly by OT member companies of 5G-ACIA.

For detailed use case descriptions, see Annex B.

4.2.1 Device identity management

Multiple identifier types are used across the communication and application layers. Communication layer identifiers are employed for addressing and authenticating communication entities and for managing secure connections between them. These identifiers are typically specific to the communication technology in use.

Application layer identifiers are employed to identify devices in the enterprise network (independently of the communication technology). Application identifiers are generally mapped to communication layer identifiers at the application layer.

It is advisable to avoid the use of application layer OT device identifiers in a 5G system.

The reasons are:

- the complexity and the variety of OT devices
- the need for backward compatibility with currently deployed device identifiers and current authentication procedures
- the need for communication technology independency (5G, Ethernet, WLAN, Bluetooth, etc.)
- the need for privacy and security (OT data is sensitive and should not be accessible to third parties, for instance to a mobile network operator)
- the convenience of managing OT device configuration data from a central point of administration

More information on communication and application authentication can be found in Annex A.

The requirements in relation to 5G exposure reference points are:

[R-4.2.1-01] A unique identifier must be used at 5G exposure reference points to identify each UE. 3GPP has defined the generic public subscription identifier (GPSI) for this purpose.

> **Note 1:** This requirement is applicable in public and non-public networks.

An industrial 5G NPN can be part of an IP- or Ethernet-based network environment. In these cases, two alternative identifiers can be used instead of the GPSI, namely the IP or Ethernet address of the UE. The prerequisite for use of these two identifiers is that both are unique in the context of the 5G NPN and IIoT application.

[R-4.2.1-02]: In a non-public stand-alone network, the 5G NPN and the IIoT application shall be able to use the UE static IP address for identifying a UE.

> **Note 2:** The static IP address of the UE is assigned by the IIoT application. This IP address can then be employed to identify the UE via the exposure reference points En and Ed.

> **Note 3:** The static IP address can be re-assigned at any time by the IIoT application. Via the reference points En and Ed, the IIoT application prompts the UE to re-establish its connection with the 5G NPN to perform address re-assignment. Address re-assignment will cause an interruption to the device connection.

[R-4.2.1-03] Both static IPv6 and IPv4 shall be supported as alternative identifiers.

[R-4.2.1-04] In a non-public stand-alone network, the 5G system shall support the identification of devices hosting UEs by means of their media access control (MAC) address.

[R-4.2.1-05] OT application layer device identifiers must not be used at 5G exposure reference points.

For more information on communication and application identifiers see Annex A, Section 8.3.

4.2.2 Device provisioning and onboarding

[R-4.2.2-01] The 5G exposure reference points must support integration into and configuration of a device within a 5G system by provisioning the relevant UE information (e. g. UE IDs, network access authentication keys, subscriptions) to the 5G network so it will accept device connection when the device is activated.

> **Note 1:** This requirement enables 5G network plug-and-play connectivity for devices.

[R-4.2.2-02] The 5G exposure reference points must support provisioning and onboarding of individual devices and groups of devices.

[R-4.2.2-03] The 5G exposure reference points must notify the IIoT application when a device has connected to the network.

4.2.3 Device connectivity management

[R-4.2.3-01] The 5G exposure reference points must support:

- on-demand UE-to-UE (UNU) or UE-to-data-network (UN) connections with a defined quality of service (QoS)

  Note 1: A UNU connection is only applicable when both UEs are attached to the same 5G NPN. A UNU connection between two UEs always involves one or more 5G NPN RAN and CN nodes, i.e. UNU is not a direct device-to-device connection. For UNU connections, the QoS parameters used at the exposure reference points apply to the complete communication path from one UE via the network to the second UE. The IIoT application must specify two UE identities (for instance their GPSIs) to establish a UNU connection. For UN connections, only one UE identity is required, and the QoS parameters apply to the communication path from the UE to the point where the 5G NPN connects to the data network.

- multiple connections per device, each characterized by QoS parameters

  Note 2: Connections can be Ethernet-based and/or IP-based.

  Note 3: Examples of QoS parameters that can be defined for each connection are: service bit rate, minimum communication service reliability, and maximum end-to-end latency. For detailed performance requirements see section 5 in reference [6]. See also annex C in reference [6] for a description of the communication model and of characteristic parameters.

  Note 4: IIoT applications may specify – in addition to the requested QoS parameters – a set of secondary QoS parameters. The 5G NPN applies the requested QoS with highest priority and indicates via the exposure reference points which parameters have been applied to the connection in question (see Annex C).

- Modification of an established UNU or UN connection (e.g. new QoS parameters) and termination of a connection.

[R-4.2.3-02] The 5G exposure reference points must be capable of acknowledging a communication service request within 100 ms.

[R-4.2.3-03] For 5G-TSN integration, the 5G exposure reference points must provide the 5G virtual-bridge and port information to the IIoT application.

Note 5: An example of an IIoT application is a TSN centralized network configuration (CNC) entity.

Note 6: This information includes IEEE 802.1Q [13] traffic classes, bridge delay per port pair and per traffic class of the 5G system (5GS), as well as propagation delay per port.

[R-4.2.3-04] The 5G exposure reference points must enable the IIoT application (e.g. the centralized network configuration) to configure the 5GS bridge, including port configuration (e.g. IEEE 802.1Qbv traffic scheduling parameters [14]), TSN QoS, and traffic forwarding information.

[R-4.2.3-05] The 5G exposure reference points must enable the IIoT application to request information on the time synchronization methods supported by the 5G NPN and to activate or deactivate time synchronization for a device or a group of devices by applying one of the methods supported by 5G.

[R-4.2.3-06] The exposure reference points must enable the IIoT application to provide a traffic profile applicable to a single connection, to all connections of a device, or to all connections of a group of devices. The 5G NPN may use that information to assess its resource capacity and to optimize resource allocation. The traffic profile may be provided when a new connection is requested, or when an existing connection is modified.

Note 7: Examples of parameters included in traffic profiles are:

- transfer interval and the data volume per cycle time, or
- average and peak data rates
- Silence time intervals may also be included to indicate when an established connection will not carry any user payload (e.g. at night or on weekends).

4.2.4 Device connectivity monitoring

[R-4.2.4-01] The 5G exposure reference points must support monitoring of device connectivity, including the connection's QoS.

Note 1: Examples for monitoring parameters are provided in Annex C, Section 10.

Note 2: Monitoring must be supported for individual QoS flows and for a set of flows.

[R-4.2.4-02] The 5G exposure reference point must support connectivity monitoring for individual devices or for a group of devices.

[R-4.2.4-03] The 5G exposure reference point must support on-demand, periodic, and event-triggered connectivity monitoring for a device or a group of devices.

[R-4.2.4-04] For event-triggered monitoring, it must be possible to define a list of triggering events.

Note 3: Examples of triggering events include connection status change and device movements across mobile network radio cells.

[R-4.2.4-05] The 5G exposure reference point must be able to provide a history of communication events.

Note 4: These events include, for example, instances when the required QoS could not be met.

Note 5: The communication history may include timestamps of events and location-related information. Examples of such information include the locations of UEs and of radio base stations associated with events.

[R-4.2.4-06] The 5G exposure reference point must respond to a request to provide real-time QoS monitoring information within a specified time.

Note 6: An example of a typical response time is 5 s.

Note 7: This time is subject to negotiation between the communication service consumer and the 5G system.

[R-4.2.4-07] The 5G exposure reference points shall enable the periodic updating of QoS monitoring information.

Note 8: An example of a typical update frequency is once per 10 seconds.

[R-4.2.4-08] The 5G exposure reference point shall enable the provision of statistical information on device connection parameters and error types of a monitored device. The time span for collection and evaluation of statistical values can be specified by the IIoT application.

4.2.5 Device group management

[R-4.2.5-01] The 5G exposure reference point must enable creation, modification, and removal of groups of devices, including definition of group communication services and other group attributes. A unique external group identifier is allocated by the 5G NPN for each group of devices.

Note 1: An example group attribute is the service area.

[R-4.2.5-02] The 5G exposure reference point must support the addition/removal of individual devices to/from a group.

Note 2: A device can belong to multiple groups concurrently. A device may also join/leave a group in accordance with, for instance, device location.

[R-4.2.5-03] The 5G exposure reference point must allow IIoT applications to subscribe to notifications of group status events.

4.2.6 Device location information

5G systems support precise location services for tracking mobile assets (e. g. automated guided vehicles, mobile robots, moveable assembly platforms, portable assembly tools, mobile control panels; see reference [6]).

[R-4.2.6-01] The 5G exposure reference points must allow IIoT applications to capture device location information of the following types:

- Location data with requested granularity.
- One-time delivery of device location information upon request.
- Reporting of device location information triggered by events such as movements (e. g. a device entering or exiting a defined area or moving a defined distance) and time events (e. g. specified time intervals).

4.3 Network management

The requirements given in this sub-section are based on input from OT companies that already or will in the future operate 5G NPNs. As outlined in Annex B, the operational use cases discussed in this white paper only relate to the operational phase of the 5G network management life cycle.

4.3.1 Network monitoring

[R-4.3.1-01] The 5G exposure reference points must provide means of monitoring network status, including integration points with other networks, both at network set-up and during operation.

[R-4.3.1-02] The 5G exposure reference point must support monitoring to verify that network components, (including component inventory information and network element capabilities) are configured and connected correctly.

[R-4.3.1-03] The 5G exposure reference points must support monitoring to verify that the (end-to-end) logical network(s) is/are configured correctly in the 5G system.

> **Note 1:** Reporting on which logical network(s) a device is (currently) connected to is enabled through [R-4.2.4-01].

[R-4.3.1-04] The 5G exposure reference points must support monitoring to verify that a logical network is operating according to the prescribed service level specification (SLS).

> **Note 2:** The SLS is the technical part of a service level agreement (SLA).

[R-4.3.1-05] It must be possible to monitor high-level logical network metrics and KPIs through the aggregation of lower-level metrics and KPIs, i. e. at the level of physical/logical network components.

[R-4.3.1-06] Access to lower-level metrics and KPIs at the level of physical/logical network components must be permitted, subject to specific authorization.

> **Note 3:** Specific authorization is needed to access certain information when the 5G network is not operated by the factory operator but by a service provider. Disclosure of certain information (e. g. physical network components) needs mutual agreement between the service provider and the enterprise (e. g. the factory operator).

[R-4.3.1-07] The 5G exposure reference points must allow monitoring of errors and other alarms from physical/logical network components and connections.

[R-4.3.1-08] The 5G exposure reference points must provide the monitoring information in such a way that it can be effectively used for error detection, localization, root-cause analysis, and error resolution.

[R-4.3.1-09] The 5G exposure reference points must support these network monitoring capabilities when

1. the network is deployed as a stand-alone NPN and operated by the factory operator;
2. the network is deployed as a PNI-NPN, i. e. operated by the mobile network operator, and provided as a service to the factory operator.

[R-4.3.1-10] The 5G exposure reference points shall enable the exposure of network resource utilization.

[R-4.3.1-11] The 5G exposure reference points shall enable the provision of information on the availability of a specific communication service in a particular area.

> **Note 4:** An example of such an area is a specific radio cell.

[R-4.3.1-12] The 5G exposure reference points shall provide time synchronization methods supported by the 5G NPN with a minimum time synchronization accuracy.

4.3.2 Network configuration and maintenance

The operational use cases described in this section are included for the sake of completeness only. They provide valuable background information for e. g. 5G network operators and 5G network equipment manufacturers with regard to the capabilities factory operators expect for the configuration, operation and maintenance of a 5G NPN. Details of these operational use cases are beyond the scope of this white paper – they are subject to mutual agreement between the 5G network operators and the factory operator.

The 5G NOC reference point Nm provides the means to support the following operational use cases:

5G system repair:

- Restarting individual 5G core network functions or 5G radio access nodes
- Re-instantiating virtualised resources used by a network function
- Healing of NFV network service instances mappable to a 5G network slice

Backup/restore of 5G network functions:

- Backup/restore of individual 5G network functions
- Backup/restore of 5G network slices

Provision/deprovision of 5G network components:

- Provision/deprovision of 5G network functions
- Provision/deprovision of a 5G logical network (e. g. network slice or 5G LAN virtual network)
- Provision/deprovision of a 5G radio access node
- Enabling and disabling 5G radio access nodes

Any configuration changes to 5G network functions must be executed in a controlled manner to prevent faults and service disruptions, and to minimize the risk of violating the SLS.

The above list of operational use cases is not exhaustive. They will vary depending on the specific agreement between the 5G network operator and the enterprise (e. g. the factory operator).

4.4 Security requirements

[R-4.4-01] The 5G exposure reference points must support means of mutual authentication and authorization between the exposure producer (the 5G NPN) and the exposure consumer (an IIoT application).

[R-4.4-02] All 5G service requests via the reference points must be authenticated and authorized.

> **Note 1:** This requirement ensures that unauthorized IIoT applications cannot request services and that the 5G system can authenticate IIoT applications (for instance the device management server) before interacting with them.

[R-4.4-03] The 5G exposure reference points must support means of ensuring confidentiality and integrity of communication between the exposure producer and the exposure consumer.

[R-4.4-04] The 5G exposure reference points must support means of authorizing the exposure consumer to use exposed capabilities in full – or limited to a subset of the capabilities – based on the role of the exposure consumer and on context (e. g. location, time, type, etc.) of the device hosting the exposure consumer.

> **Note 2:** Examples of roles are users in the IIoT application domain tasked with e. g. provisioning new devices and managing connectivity. Other users may be tasked solely with e. g. monitoring device connectivity and requesting their location but may not make any modifications to connectivity. Further roles may be assigned for network monitoring and for making network configuration changes.

> **Note 3:** The location of the device is based on the position of the UE as determined by the 5G network.

[R-4.4-05] The 5G exposure reference points must make security logging information from UEs available to IIoT applications.

> **Note 4:** An example of security logging is information on 3GPP security mechanisms applied for IP and Ethernet device connections to ensure e. g. data privacy, authenticity, and integrity protection.

5 Summary and outlook

This white paper describes the capabilities that a 5G non-public network (5G NPN) must expose towards IIoT applications to enable a range of operational use cases. Operational use cases are divided into device management and network management.

To help the reader to better understand how 5G services exposed via the reference points can be consumed by IIoT applications, essential deployment and interconnection assumptions are described in Section 3 and expanded on in Annex A (Section 8).

This white paper focuses on operational use cases that allow factory operators to perform frequent (daily) tasks without the need to involve the network operator. These tasks, as described in Section 4.2, are onboarding of devices to the 5G NPN, and managing and monitoring device connectivity. Section 4.3.1 describes monitoring of 5G NPN performance and operational state.

Other tasks, such as network configuration and maintenance, are not in the focus of this white paper, as these are performed less frequently and may often impact the 5G NPN infrastructure and network functions. Therefore, these tasks will be executed using network operator and network component vendor-specific support systems. For the sake of completeness, however, the use cases for network maintenance and configuration most important to factory operators are given in Section 4.3.2.

It should be noted that the capabilities described here can be exposed both by 5G NPNs deployed in a stand-alone mode and by 5G NPNs deployed and operated by a mobile network operator on behalf of an enterprise.

6 Definitions and abbreviations

6.1 Definitions

5G exposure interface is an interface that exposes a set of capabilities of the 5G system.

5GLAN group, as per reference [7], is a set of UEs using private communication for 5G LAN-type services.

5G LAN-type service, as per reference [7], is a service over the 5G system offering private communications using IP and/or non-IP communications.

5G network is a 3GPP-compliant network consisting of a 5G access network and a 5G core network.

5G system is, as per reference [7], a 3GPP-compliant system consisting of a 5G access network, a 5G core network, and a UE.

5G LAN virtual network is, as per reference [7], a 5G virtual network, capable of supporting 5G-LAN-type services.

Data network is a non-3GPP-compliant OT network or an enterprise IT network.

Device is a physical entity that combines a 5G UE with automation functions, such as sensing and actuation.

Device connection is, in 3GPP terms, an active connection between the UE and data network (via the 5G core network). This connection is established by means of protocol data unit (PDU) session and packet flow descriptions (PFDs).

Exposure consumer is an IIoT application function that uses a service exposed by the exposure producer.

Exposure producer is a 5G function that implements a service that is exposed to IIoT applications as users of the 5G system.

IIoT application is a set of application functions needed to manage industrial processes. IIoT applications can be deployed and executed on any compute entity that has connectivity to the 5G network exposure interface.

IT enterprise domain is a communication infrastructure on the enterprise premises used by enterprise-level, non-real-time resource planning and supervision IIoT applications.

Logical network is a representation of a network that appears to the user as a separate and self-contained network, even though it might be only a subset of physical network resources. For instance, it can be a complete 5G network, a 5G network slice, or a 5G LAN virtual network.

Observation time interval is a time interval during which a series of measurements is conducted [15].

OT production domain is a communications infrastructure on the enterprise premises used by real-time and non-real-time control systems of automation IIoT applications.

Reference point is, as per ITU-T I.112, a conceptual point at the conjunction of two non-overlapping functional groups. A reference point consists of one or more interfaces.

Service provider is a legal entity that owns the 5G NPN and provides services to NPN users based on mutually agreed SLSs. A service provider is responsible for the entire life cycle of the network.

Service provider domain is the communication infrastructure used for the purposes of 5G network configuration, commissioning and management, which is under control of a service provider or under control of an enterprise (e. g. the factory operator).

User equipment (UE) is, according to 3GPP, a device that allows access to 5G network services. According to 3GPP specifications, the interface between the UE and the network is the radio interface.

UE-to-UE connection (UNU) is a connection type offered via the reference points to the IIoT application. A communication path (PDU session or data flow within a PDU session) is established from one UE via various 5G network nodes to a second UE, which is attached to the same 5G NPN.

UE-to-network connection (UN) is a connection type offered via the reference point to the IIoT application. A communication path (PDU session or data flow within a PDU session) is established from the UE to the 5G network integration point to the external data network.

6.2 Abbreviations

3GPP	Third Generation Partnership Project
5G	Fifth generation
5GS	5G system
API	Application programming interface
Ed	5G exposure reference point on the device side
En	5G exposure reference point in the core network
eUICC	embedded UICC (also known as an eSIM)
GPSI	Generic public subscription identifier
IIoT	Industrial Internet of Things
iUICC	integrated UICC (also known as an iSIM)
IT	Information technology
KPI	Key performance indicator
MAC	Media access control
MNO	Mobile network operator
NFV	Network function virtualization
Nm	5G NOC reference point of the NOC for 5G network configuration and management
NOC	Network operations center
5G NPN	5G non-public network
OPC UA	Open platform communication (OPC) unified architecture
OSI	Open Systems Interconnection
OT	Operational technology
RAN	Radio access network
RFC	Request for comment
SLA	Service level agreement
SLS	Service level specification
QoS	Quality of service
TSN	Time-sensitive networking
UE	User equipment
UICC	Universal integrated circuit card (also known as a SIM card)
UN	UE-to-data network connection via a 5G NPN
UNU	UE-to-UE connection within a 5G NPN
UPF	User plane function
VLAN	Virtual local area network

7 References

[1] 5G-ACIA, white paper, *5G for Automation in Industry*

[2] 5G-ACIA, white paper, *5G Non-Public Networks for Industrial Scenarios*, July 2019

[3] 3GPP TR 22.804, *Study on Communication for Automation in Vertical Domains*

[4] Platform Industrie 4.0, *Industrie 4.0 Plug-and-Produce for Adaptable Factories: Example Use Case Definition, Models, and Implementation*

[5] 3GPP TS 22.261, *Service requirements for the 5G system*

[6] 3GPP TS 22.104, *Service requirements for cyber-physical control applications in vertical domains*

[7] 3GPP TS 23.501, *System Architecture for the 5G system*

[8] 3GPP TR 23.734, *Study on enhancements of 5G system (5GS) for vertical and Local Area Network (LAN) services*

[9] 5G-ACIA, white paper, *A 5G Traffic Model for Industrial Use Cases*, November 2019

[10] 5G-ACIA, white paper, *Integration of Industrial Ethernet Networks with 5G Networks*, November 2019

[11] 5G-ACIA, white paper, *5G for Connected Industries and Automation*, 2nd edition

[12] 3GPP TS 23.273, *5G system (5GS) Location Services (LCS)*

[13] IEEE 802.1Q, *IEEE Standard for Local and Metropolitan Area Networks – Bridges and Bridged Networks*

[14] IEEE 802.1Qbv, *IEEE Standard for Local and Metropolitan Area Networks – Bridges and Bridged Networks Amendment 25: Enhancements for Scheduled Traffic*

[15] ISO 1996-2, *Acoustics – Description, measurement and assessment of environmental noise – Part 2: Determination of sound pressure levels.*

[16] 3GPP TS 23.502, *Procedures for the 5G System*

[17] 3GPP TS 23.522, *5G System; Network Exposure Function Northbound APIs*

[18] 3GPP TS 23.222, *Functional architecture and information flows to support Common API Framework for 3GPP Northbound APIs*

[19] 3GPP TS 23.434, *Service Enabler Architecture Layer for Verticals*

8 Annex A: Solution concepts

8.1 Architecture concepts for 5G exposure reference points

While some assumptions for 5G exposure capability requirements are provided in Section 3, this annex provides further details on those assumptions, and guidance on the implementation and integration of exposure interfaces.

A 5G NPN may coexist and require integration with a non-5G OT network. To this end, the transmission of non-IP traffic via the 5G system, e. g. Ethernet traffic, is required. The 5G-ACIA white paper *Integration of Industrial Ethernet Networks with 5G Networks* [10] describes various communication scenarios for integration-related use cases, i. e. line controller to controller, controller to controller, controller to device, and device to compute.

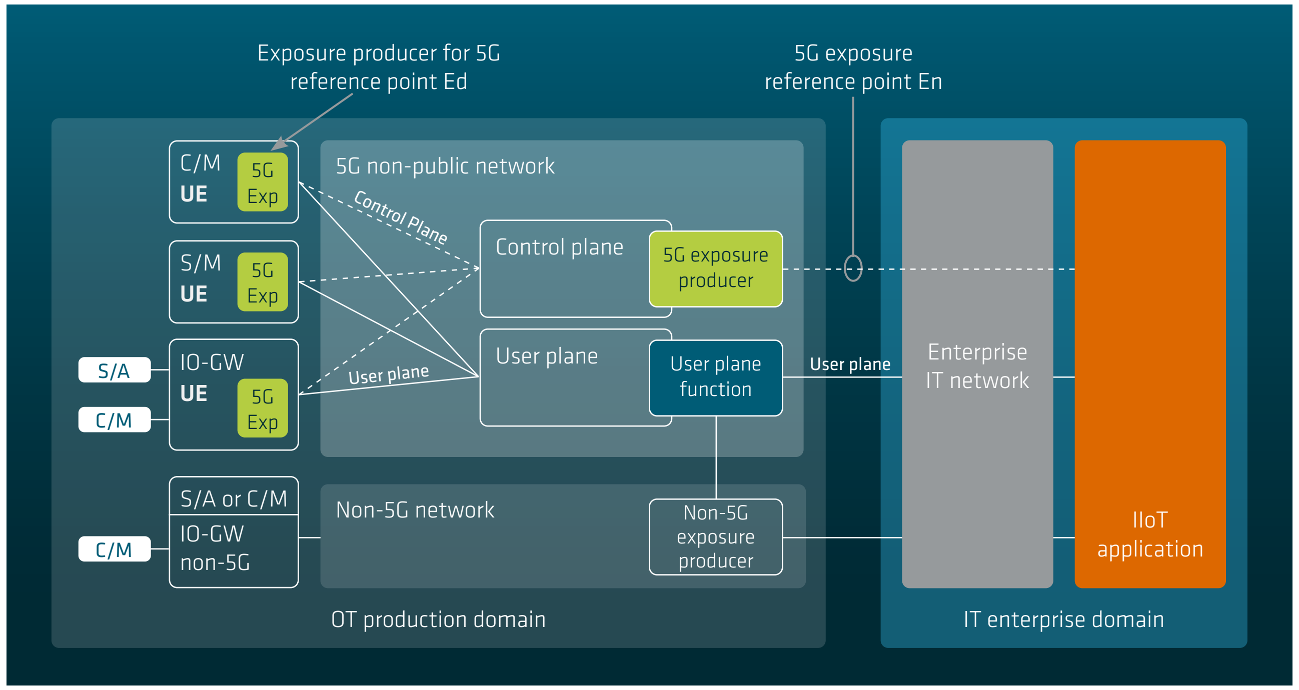
Figure 3 depicts the 5G exposure reference points in relation to the control and user planes of the 5G NPN and in relation to non-5G networks and the IIoT applications.

The control plane of the 5G NPN is employed to dynamically manage the user plane device connections according to required transmission QoS parameters. These device connections are used to transfer data between devices and IIoT applications via the 5G NPN.

The IIoT application may be a distributed application with its components communicating at the application layer by use of these device connections. These application components exchange information by means of application-specific protocols, such as OPC UA.

To allow the IIoT application to use 5G communication services in a simple, transparent and efficient manner, the 5G capabilities are exposed via the network-side 5G exposure reference point En and via the device-side 5G exposure reference point Ed. The reference point Ed consists of local interfaces accessible only to IIoT applications executing on the device. The refence point En, by contrast, possesses interfaces accessible remotely and used to expose the capabilities of the entire 5G system (subject to authorization).

Fig. 3: High-level reference point deployment. A: actuator; C: controller; GW: gateway; IO: input and output; M: manager; S: sensor



Source: 5G-ACIA

The descriptions of operational use cases in Annex B indicate in each case whether reference point Ed or En, or both, are used.

For the management of a 5G network, there are three important phases.

1. The "plan-to-deploy" phase, encompassing the initial stages of planning until the network is ready to handle traffic, and ready to onboard devices and terminals. These stages typically include radio resource planning, configuration of the 5G network (comprising the radio access network, the core network, the transport network, and network slices).
2. The "operational" phase is the period when the network is in service. The network is monitored during this phase. There are processes in place for fault resolution and for performance reporting. Network management tasks include, e. g. adding more network resources or reconfiguring parts of the network. Onboarding and offboarding of devices and managing device connectivity (e. g. QoS) are also performed during this phase.
3. The "retirement and upgrade" phase comprises major transitions of groups of entities in the network. This includes replacing or phasing out hardware and software, and upgrading existing services.

This white paper describes the requirements at 5G exposure reference points for operational-phase use cases, namely use cases that exist during the operational life cycle phase of non-public 5G networks.

The table below clarifies the roles of the management, control and user planes during the various phases of the network life cycle.

Table 1: The management, control and user planes during the life cycle of a 5G system

Plane	Plan-to-deploy phase	Operational phase	Retirement and upgrade phase
Management plane	X	x	X
Control plane		x	
User plane		x	

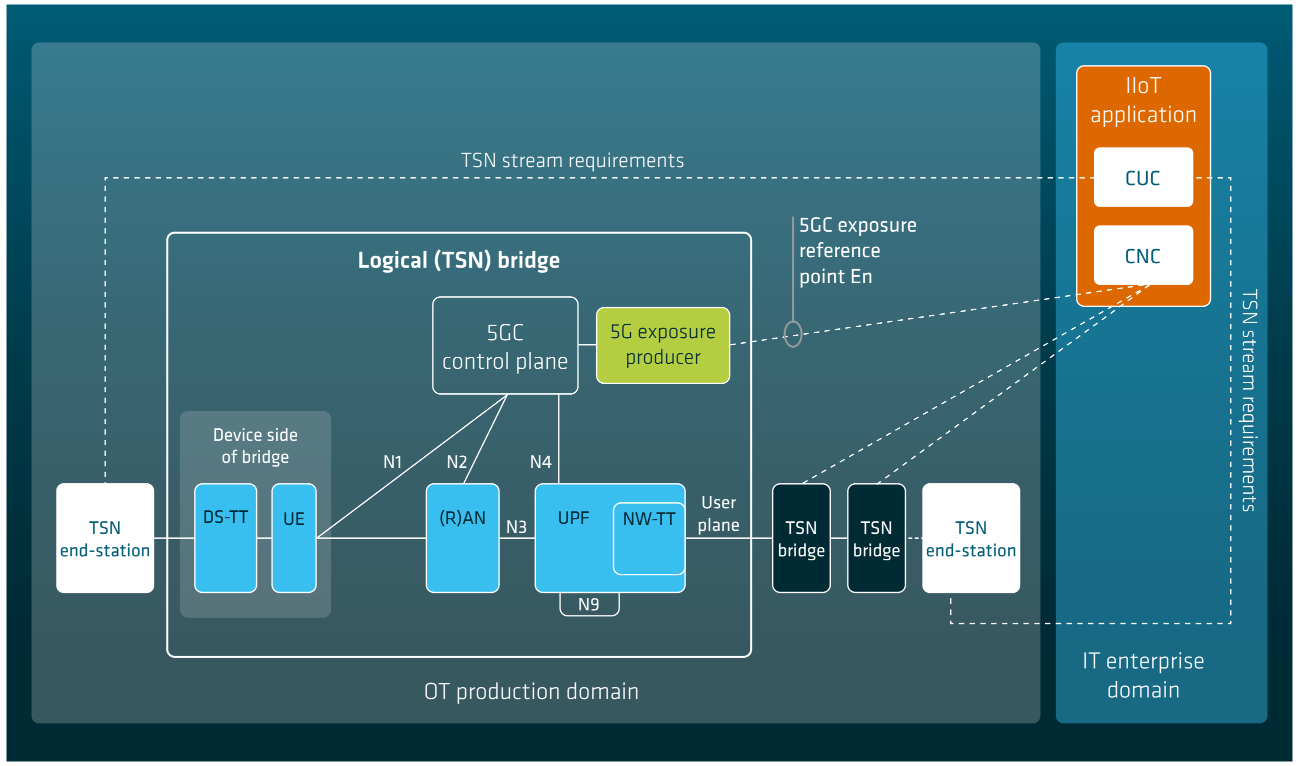
Often the complete set of network management capabilities for all aspects and phases is supported by a network management tool available from the network equipment vendor or integrator. A tool of this kind is typically integrated into the 5G service provider's network operations center (NOC). The NOC is used to operate and maintain the 5G NPN (see Figure 2). The 5G service provider may be an MNO or an enterprise (e. g. the factory operator). The NOC may manage one or multiple NPNs. These operational uses cases, supported via the 5G reference point Nm, are not addressed in detail in this white paper, as mentioned in Section 4.3.

8.2 Integration of 5G with wired networks

8.2.1 Integration of 5G NPNs with Industrial Ethernet networks

This white paper assumes the 5G network is deployed as a stand-alone, non-public network. 5G systems in compliance with 3GPP Release 16 and later specifications will offer 5G LAN-type services. One example would be the 5G system operating as an Ethernet bridge. On account of this new functionality, 5G systems will be able to support deterministic, time-sensitive layer-two traffic flows.

Fig. 4: 5G system as a virtual bridge integrated into TSN network



Source: 5G-ACIA

8.2.2 Integration of 5G NPNs with TSN networks

In addition to supporting Ethernet connectivity as of Release 16, 3GPP is also seeking to enable integration of 5G with TSN networks. In this context, the 5G system integrates with the TSN network like a TSN bridge which is configured according to the centralized configuration model. The user plane TSN translators (DS-TT and NW-TT in Figure 4) are placed at the ingress and egress points of the 5G system, i.e. at the user plane function (UPF) and the UE (see Figure 4).

The TSN application function interacts with the TSN centralized network configuration entity to configure TSN flows in the 5G system. The 5G exposure reference point En exposes the TSN application function capabilities.

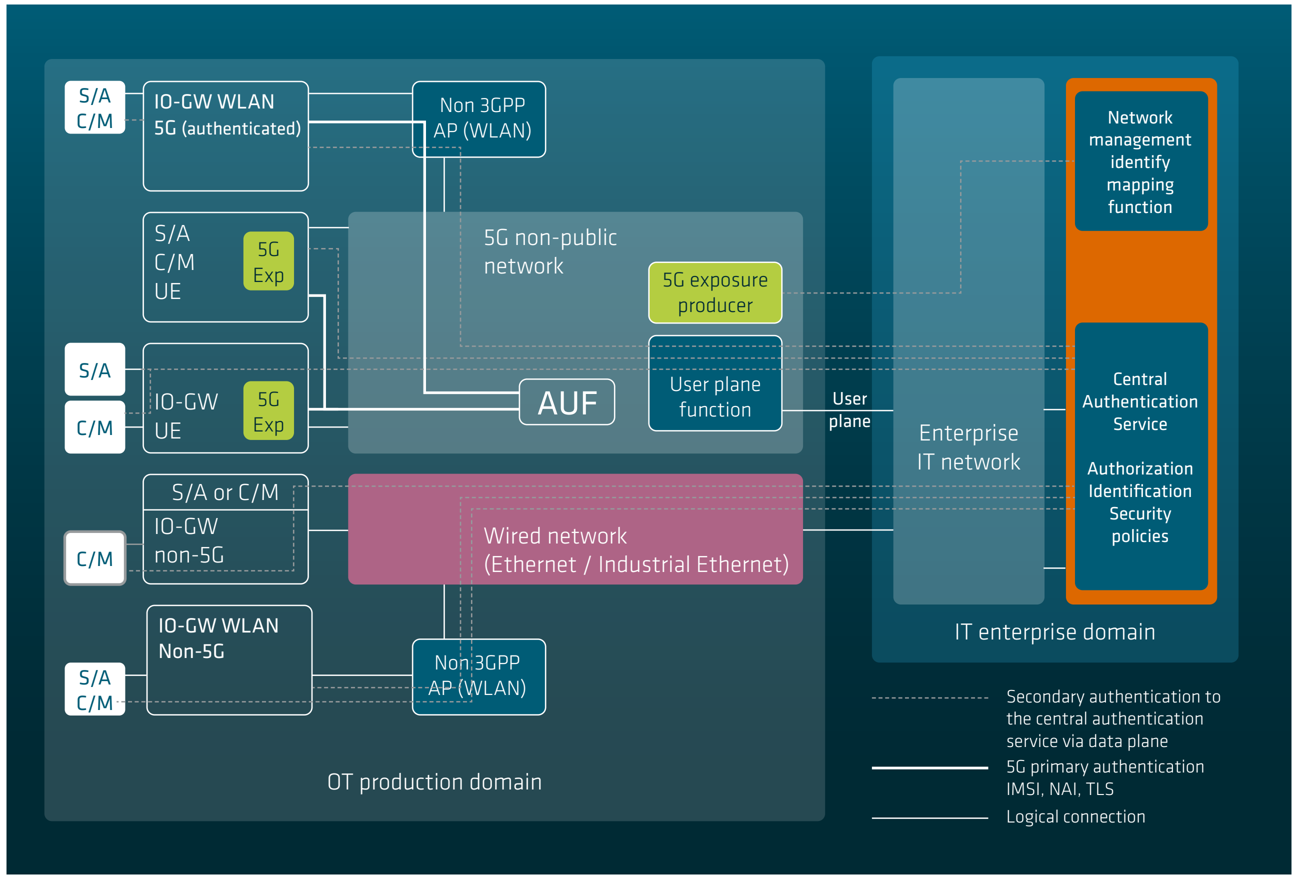
8.3 Device identities, authentication and authorization

A logical view of authentication for communication devices and IIoT applications that leverage 5G NPNs is shown in Figure 5.

The UE and the network mutually authenticate to allow the UE to gain access to the 5G network. Once the UE has been authenticated by the 5G network, the corresponding local application function can connect to the enterprise network and to the device management server in the IT enterprise domain via the user plane and it can perform application authentication.

The application authentication method used is not divulged to the 5G system. Any device or IIoT application that is located "behind" a 5G UE, or that is part of a 5G-enabled device, uses the 5G network to connect to the enterprise network and device management application in the IT enterprise domain without being authenticated by the 5G network.

Figure 5: Authentication and authorization of IIoT applications



Source: 5G-ACIA

The network management server maps the IIoT application identifier to the UE identifier. Note that interactions with the 5G network via the exposure reference points only make use of the device's unique identifier, e.g. the 5G generic public subscription identifier (GPSI) or UE statically allocated network address as described in Section 4.2.1.

For reasons of confidentiality and security, the 5GS internal identifier is not disclosed "over the air" or to any IIoT applications. Furthermore, it is not made available outside of the 5G system or via the 5G exposure reference points. Instead a unique public identifier, e.g. a GPSI, is used on the 5G exposure reference points to uniquely identify a UE. The 5G system maintains mapping between the GPSI and the corresponding internal identifier. The GPSI is either a mobile station international ISDN number (MSISDN) or an external identifier in the form of username@realm according to 3GPP TS 23.003. Alternative identifiers are the static IP address or MAC address of the UE.

A device may consist of more than one UE, in which case each UE is addressed by means of its own unique identifier, e.g. GPSI or network address.

A non-3GPP device can also access the enterprise IT network via a wired network or a WLAN access point connected to the 5G network. In the latter case, 5G access network authentication is managed by the 5G network in a similar way as for a UE. In this scenario, too, application-level authentication is performed via a data connection and is not divulged to the 5G system.

Note that 3GPP Releases 16 and 17 do not include support for non-3GPP access to a 5G NPN.

9 Annex B: Detailed use case descriptions

The use cases given in this section are based on the assumptions in Section 3.

9.1 Device management use cases

9.1.1 Device provisioning and onboarding

Use case	Description	Comments
Title	Provisioning and onboarding of device(s)	
Goal	Provision and onboard device(s) in the 5G NPN	
Actors	5G NPN operator Device with an integrated 5G UE Device manufacturer Device management server (exposure consumer via En; IT enterprise domain) Device provisioning and onboarding service (exposure producer; 5G NPN) Device connectivity monitoring service (exposure producer; 5G system)	An IO-GW with a UE is treated as a device.
Pre-conditions	The device is pre-configured with a device manufacturer/vendor certificate (or other type of credentials) that allows successful identification and authentication of the device by the 5G network. The device is either pre-configured with the NPN identity, or it is capable of selecting the NPN by other means (e. g. manually or by using a trial-and-error method). The 5G NPN is operational and is configured with subscription profiles for various services, including the type of network access authentication (for instance 3GPP AKA, EAP-TLS) and a logical network dedicated to device provisioning tasks (typically with limited connectivity and isolated from the other logical networks for security reasons). The 5G NPN also includes a default logical network (typically for best-effort connectivity) for application-level device configuration.	
Execution – step 1	How the device is configured to access the 5G NPN depends on the security and configuration data provisioning solution. a. In the case of UICC, this implies inserting the card obtained from the 5G NPN operator (the card is provisioned with data such as access credentials and a subscriber profile). b. In the case of eUICC/iUICC, access credentials and the subscriber profile are downloaded from a device-provisioning server c. Otherwise, the device will use pre-configured device manufacturer credentials to connect to the NPN's provisioning logical network and gain access to the provisioning server. Network access authentication for this provisioning step can be performed by the 5G NPN, in which case the initial credentials are provided to the system through the device provisioning and onboarding service. Otherwise, authentication can be delegated by the 5G NPN to an authentication server (for instance in the IT enterprise domain), in which case the address of the authentication server must be provided by the device management server. After successful connection to the provisioning server, the device receives access credentials and a subscriber profile for access to the 5G NPN. Note that – as described in Annex A – the identity mapping function is configured to ensure mapping between the device identity and the GPSIs (or other unique identifiers) for the device(s). As part of this provisioning step, the device management server initiates the device provisioning and onboarding service for one of the following provisioning procedures. 1. Authorization to the NPN of a single device with a given GPSI or another unique identifier. 2. Authorization to the NPN of a set of devices with given GPSIs or other unique identifiers ("bulk authorization"). Note that a device may be assigned multiple unique identifiers if it comprises multiple UEs. In this case, all UEs of that device are authorized by means of a single operation.	
Execution – step 2	The device management server is notified by the device provisioning and onboarding service of the successful or unsuccessful execution of the requested procedure.	
Execution – step 3	When the device is turned on, or when it has successfully completed the provisioning step 1a or 1b, and successfully connects to the default logical network, the device connectivity monitoring service notifies the device management server of the following event: a device with a given GPSI (or other unique identifier) has connected to the default logical network of the 5G NPN. The MAC and/or IP address is also provided so that the device management server can address the device.	
Post-conditions	The device is successfully connected to the default logical network.	

Use case	Description	Comments
Title	Deprovisioning and offboarding of device(s)	
Goal	Deprovision and offboard device(s) from the 5G NPN	
Actors	Device with an integrated 5G UE Device management server (exposure consumer via En; IT enterprise domain) Device provisioning and onboarding service (exposure producer; 5G NPN) Device connectivity monitoring service (exposure producer; 5G NPN)	An IO-GW with UE is treated as a device.
Pre-conditions	The 5G NPN is operational and is configured with subscription profiles for various services, including the type of network access authentication (for instance 3GPP AKA, EAP-TLS) and a default logical network. Device(s) are provisioned and onboarded in the 5G NPN. The identity mapping function (device management server) enables the mapping between device identity and GPSI(s) or other suitable unique identifiers for each device.	
Execution – step 1	The device management server requests the device provisioning and onboarding service to execute one of the following procedures. 1. Remove a single device with a given unique identifier from the NPN (see Section 4.2.1). 2. Remove a set of devices (in bulk) with given GPSIs or other suitable unique identifiers from the NPN. Note that a device may be assigned multiple GPSIs (or other suitable unique identifiers) if it comprises multiple UEs. In this case, all UEs of that device are removed by means of a single operation.	
Execution – step 2	The device management server is notified by the device provisioning and onboarding service of the successful or unsuccessful execution of the requested procedure.	
Execution – step 3	The device connectivity monitoring service notifies the device management server of the following event: a device with a given unique identifier has disconnected from the NPN.	
Post-conditions	The device is successfully deprovisioned and disconnected from the NPN.	

9.1.2 Device connectivity management

Use case	Description	Comments
Title	Device connectivity management	
Goal	Change the connectivity parameters of a device that is connected to the default logical network or is already onboarded. Change the connectivity parameters of two devices that have a UNU connection.	
Actors	Device (exposure consumer via Ed) with an integrated 5G UE (exposure producer via Ed) Device management server (exposure consumer via En; IT enterprise domain) Device connectivity management service (exposure producer; 5G NPN)	
Pre-conditions	The device has an established connection to one or more logical networks or to another device attached to the same logical network. The device management server was notified of device connectivity status.	
(optional) Execution – step 1	The device management server may provide a traffic profile to the device connectivity management service for a single connection or for all connections that are intended to be established/modified on that device. The traffic profile may also apply to a group of devices and therefore to all connections of all devices in that group. The device connectivity management service can use the traffic profile(s) to assess network capabilities and optimize resource usage.	The receipt of a traffic profile will not trigger any QoS changes. Changes are executed when the connection establishment or modification is requested by the device management server.
Execution – step 2	The device management server or the device's local application function instructs the device connectivity management service in the 5G NPN to execute one of the following procedures (the pertinent device connection identifier is provided by the device management server or, respectively, by the local application function). 1. Modify the current QoS parameters of an already established connection with the new requested QoS parameters and optionally with secondary QoS parameters. Secondary QoS parameters may contain all or a subset of parameters as in the requested QoS but with different values. A reference to the traffic profile may also be provided. 2. Change the current connection characteristics from IP to Ethernet or vice versa. 3. Provide additional connections to the device (with their own QoS requirements). 4. Terminate a connection and release the associated 5G NPN resources.	For 5GS integrated with TSN, TSN-defined mechanisms are used. The device management server may be instructed by the enterprise resource planning (ERP) or manufacturing execution system (MES) on required connectivity for each device.
Execution – step 3	The device connectivity management service triggers 5G connectivity management procedures in the network and in the device(s). The device management server or the local application function is notified by the device connectivity management service of the successful or unsuccessful execution of the 5G connectivity management procedures. Upon each QoS modification and each additional connection establishment procedure, the availability of resources in the 5G system is assessed. If the 5G NPN cannot support the requested QoS parameter, the secondary parameters (if specified in the request from the IIoT application) may be selected. If resource limits are reached, the procedure may fail. Where the device management server made a successful request, the device's local application function is notified (Ed). Otherwise, it is notified of the request's failure.	
Post-conditions	The devices have established and/or terminated one or more connections with QoS parameters. The connectivity status and the applied QoS parameters are known to the device management server, which may present the information in a human-readable format to an OT stakeholder, for instance an engineer.	

9.1.3 Device connectivity monitoring

Use case	Description	Comments
Title	Device connectivity and status monitoring	
Goal	Obtain detailed device status and connectivity-related data for a device already onboarded	
Actors	Device (exposure consumer via Ed) with an integrated 5G UE (exposure producer via Ed) Device management server (exposure consumer via En; IT enterprise domain) Device connectivity monitoring service (exposure producer; 5G system)	
Pre-conditions	The device or all devices within a group have an established connection to one or more logical networks or to another device attached to the same logical network.	
Execution – step 1	The device management server or a device's local application function queries the device connectivity monitoring service for the status of the connections for a device or group of devices. The device connectivity monitoring service replies via the reference point with status information on: • connection(s) established and associated connection type(s) [IP or Ethernet]; • network address for each connection and used logical network; • the configured QoS parameters for each connection; • permanent equipment identifier (PEI); • the current RSRP (reference signal received power) value measured at the device's current location. • logical network(s) used by the device (optional); • proprietary device attributes (optional); • certificate status (e. g. a X.509 certificate) (optional); • network access restrictions (optional). The status information is compiled in a machine-readable format, for instance in XML or JSON.	Note that some of the listed status information is optional depending on network and device configuration.
Post-conditions	The devices have established one or many connections with network addresses and QoS parameters. The status of the device connections is known to the device management server and/or to the device's local application function, which may present the information in a human-readable format to an OT engineer.	

Use case	Description	Comments
Title	Device connectivity quality for a service query	
Goal	Obtain detailed device status and measured connectivity-related data for a device already onboarded	This use case can be applied to e. g. trouble-shooting activities.
Actors	Device (Ed consumer) with an integrated 5G UE (Ed producer) Device management server (En consumer; IT enterprise domain) Device connectivity monitoring service (En producer and Ed producer; 5G system)	
Pre-conditions	The device has an established connection to one or more logical networks or to another device attached to the same logical network.	
Execution – step 1	The device management server or the device's local application function requests the device connectivity monitoring service for the current and/or historical quality of the device connections. For historical data, the duration must be specified. For long durations (e. g. weeks), data granularity level will necessarily be coarse. For short durations (e. g. days), granularity can be finer. The device connectivity monitoring service replies via the reference point with, for instance • the current end-to-end latency • the minimum service bit rate over the last hour • current cell ID(s) • historical end-to-end latencies • historical minimum service bit rate for one-day intervals • communication service availability over the last day The monitoring information is compiled in a machine-readable format (e. g. XML, JSON, etc.).	The format of current and historical values is contingent on the attribute to be monitored. For instance, for communication service reliability, time stamps from the beginning and end of the non-availability of the communication service in question are of interest. For end-to-end latencies it could be the single highest end-to-end latency value over a pre-defined period. Additionally, the distribution function of the end-to-end latency could be of interest. Example parameters covered by connectivity quality queries are provided in Section 10.
Post-conditions	The device management server and/or the device's local application function is aware of the device's connection quality for a particular period. The device management server or the device's local application function may present the information in a human-readable format to an OT engineer.	

Use case	Description	Comments
Title	Device connectivity monitoring subscription	
Goal	Subscribe to connectivity-related status changes for a device or group of devices	This use case can be applied to monitoring.
Actors	Device management server (En consumer; IT enterprise domain) Device connectivity monitoring service (exposure producer; 5G system)	
Pre-conditions	The device has an established connection to one or more logical networks or to another device attached to the same logical network.	
Execution – step 1	The device management server or the device's local application function subscribes to the device connectivity monitoring service for events related to device connectivity condition changes. Subscriptions can be made for, e. g. the following events: • maximum latency exceeded; • minimum service bit rate not achieved; • communication service availability fell below the requested value; • connectivity lost / connectivity re-established; • RSRP values below threshold; • cell change (handover). The device connectivity monitoring service will initiate corresponding supervision functions in the 5G NPN nodes and will acknowledge the event subscriptions if successful. Otherwise, it will respond by indicating failure.	
Execution – step 2	The device connectivity monitoring service will trigger an event notification to the device management server or the device's local application function, including: • the unique device ID (see Section 4.2.1); • the event type as well as the achieved/exceeded threshold value; • (optional) multiple event types occurring simultaneously may be grouped into a single notification (e. g. if they are from the same source); • (optional) events affecting all devices within a group are sent as a single notification, including the logical network ID. The information can be presented in machine-readable (XML, JSON) and/or human-readable formats.	
Execution – step 3 (optional)	The device management server or the device's local application function cancels subscriptions to the device connectivity monitoring service for events related to the status of a particular communication service. The device connectivity monitoring service will cease corresponding monitoring functions in the 5G NPN nodes and will acknowledge the event subscription cancellation.	
Post-conditions	The device management server or, respectively, the device's local application function receives event notifications when certain connectivity conditions have changed.	

9.1.4 Device group management

Use case	Description	Comments
Title	Device group management	
Goal	Creation/modification of 5GLAN groups in the 5G NPN, each providing 5G LAN-type services	
Actors	Device (consumer via Ed) with an integrated 5G UE (producer via Ed) Device management server (consumer via En; IT enterprise domain) Device group management service (producer; 5G NPN)	
Pre-conditions	The 5G NPN is operational and is configured with communication services, e. g. IP communication or Ethernet-type services.	
Execution – step 1	The device management server requests the device group management service to create a 5GLAN group and set its attributes, including network name, communication type (IP or Ethernet), VLAN identifier, and default QoS parameters for device connection to the 5G LAN group. The device group management service provides the 5G LAN group data to the 5G system and replies with a unique group identifier for the 5G LAN group. The device management server requests the device group management service to modify a group identified with the external group identifier. Modifications may include changes to the group attributes or deleting the group. The device group management service provisions the modification, and replies indicating success or failure. When deleting a group, all device members of the group are first disconnected from the 5GLAN group; the device management server is notified of the device disconnection. The device management server adds or removes one or more devices (each identified with a GPSI) to/from a 5GLAN group identified with the external group identifier. The device group management service provisions the modification, and notifies the devices and the device management server that device(s) has/have been added or removed from a 5GLAN group.	External group identifier is a unique public 3GPP-specified identifier assigned to a group of devices. The individual devices are identified e. g. by the GPSI.
Post-conditions	5GLAN groups are provisioned in the 5G NPN and a device is a member of one or more 5GLAN groups.	

9.1.5 Device location information

Use case	Description	Comments
Title	Device location information	
Goal	Provide location information for a device (or group of devices)	
Actors	Device with an integrated 5G UE Location-aware application (consumer) Device location management service (producer via En; 5G system)	
Pre-conditions	The 5G NPN is operational and the devices are onboarded.	
Execution – step 1	The location-aware application requests the current location of a device or group of devices with a specified location service quality. The location service quality is defined by class (best effort or assured), accuracy and response time. The classes are defined in reference [12]. The response time includes time-to-first-fix. The location-aware application may also request the event-triggered location of a device or group of devices. The device location management service determines the current or event-triggered location of the device or group of devices in accordance with the requested location service quality and responds with location information for the device(s). A request for event-triggered location contains the types of events that trigger the delivery of location information, for instance • connection/disconnection to/from the 5G NPN; • area (an event where the device enters, leaves or remains within a predefined area); • periodically reported location, i. e. location information is provided at specified time intervals; • movement (an event where the device moves by more than a predefined distance from a predefined location). When a device location event occurs for a device or group of devices, the device location management service sends a response to the location-aware application. The response contains the event(s) that triggered the response and the location information on the device(s).	
Post-conditions	The location of device(s) is available and provided upon request or upon the occurrence of an event.	

9.2 Network management use cases

9.2.1 Network monitoring

Use case	Description	Comments
Title	Network monitoring – verifying network configuration and operation in a 5G NPN	
Goal	Verification that the network is configured and is operating according to requirements.	
Actors	Network operator of the enterprise that operates the 5G NPN (consumer). Network management function (provider)	
Pre-conditions	A network model exists. The model comprises an inventory of network nodes and components, and the KPIs and SLS describing the deployed network. The network is deployed, configured and in an operational state.	Before executing network monitoring services, it is recommended that the 5G network is configured and verified according to agreed SLSs.
Execution – step 1	Monitoring 5G network consistency. 1. The network operator requests physical and virtual topology information from the network management function, including configurations, performance counters and integration points for the 5G network. By specifying filter criteria, the topology information can be limited to specific network parts. Topology information includes links and dependencies, e. g. links and dependencies between virtual and physical entities. Filter criteria are, e. g.: • Exact match or a range of network node and component identities • Logical network ID • Physical location of network nodes and components • Node and component type etc. 2. The network operator receives the requested data from the network management function as a single object or as a collection of objects. The retrieved physical and virtual topology information and configurations are compared by the network operator with the designed target network model in order to identify deviations between the target model and the actual network.	Of special interest are the integration points, i. e. the 5G network functions and components that interface with the enterprise IT or non-3GPP OT networks.
Execution – step 2	Notifications of network changes when monitoring the network: 1. The network operator requests a subscription for monitoring network changes from the network management function. The requested updates include topology and configurations according to defined filter criteria, see, for instance, the list in step 1. 2. When the network management function detects network changes, the network operator is notified. That notification contains a limited number of network nodes and component identities where changes were detected. The network operator can retrieve more information on a selected node or component and can also retrieve the complete network topology information. Network changes can be triggered by: a. Alarms from the network. b. Planned network changes, for instance expansions/modifications executed via operation and support systems. c. Direct changes to network elements and components, e. g. via command line interfaces. 3. The network operator receives the requested data from the network management function. 4. The retrieved changed topology and configurations are compared by the network operator with the network model to identify deviations.	This is an optional step for optimization; it is always possible for the consumer to retrieve the topology in step 1.
Post-conditions	The network is verified as configured and operational in accordance with network design and network requirements.	

10 Annex C: Parameters for QoS monitoring

This annex provides examples of parameters and performance indicators of interest to IIoT applications, but it is not intended to be exhaustive, i. e. it does not imply limits to the parameters made available by a 5G NPN. 3GPP has defined the capabilities which can be exposed to IIoT applications, e. g. parameters related to QoS monitoring, parameters influencing 5G traffic, events (e. g. signalling path status, status of QoS), 5GLAN group information, service-specific information, exposure of analytics data, etc. The 5G network can expose these capabilities via network exposure functions (NEF) [7], [16], [17] and via the SEAL framework [19] or CAPIF [18].

10.1 Parameters pertaining to connections

Table 2: Typical device connectivity parameters for QoS monitoring by IIoT applications

Parameter	Comments	Typical dynamicity	Parameter pertaining to the device connection or the 5G network
Communication service availability	In relation to a negotiated observation time interval.	Continuous; selective	Device connection
Communication service reliability	In relation to a negotiated observation time interval.	Continuous; selective	Device connection
End-to-end latency	For each requested 5QI (includes alternative QoS profiles).	Continuous; selective	Device connection
Service bit rate	For uplink or downlink or both.	Continuous	Device connection
Packet error ratio	–	Continuous; selective	5G network

10.2 General key performance indicators

Table 3: Typical general key performance indicators for QoS monitoring by IIoT applications

Parameter	Comments	Dynamicity	Parameter pertaining to the device connection or the 5G network
Success rate of connection requests	Number of successful access attempts to the 5G network divided by the total number of attempts. Background: This parameter indicates if authorized UEs that attempt to connect to the 5G network are rejected.	Continuous; event-based	5G network
Dropped connections	This parameter may be an absolute figure or a ratio/proportion	Continuous; selective	Device connection
Traffic volume for each 5QI and alternative QoS profiles	The time span for measurement of the traffic volume is a configuration parameter	Continuous; selective	Device connection
Cause of device connection termination	–	Event-based	Device connection
Handover success	Ratio of successful handovers of devices from one radio cell to the other cell	Continuous; selective	5G network
Measured SNR	Measured at UE and/or gNB; SNR per beam. The IIoT application specifies when the SNR is to be measured and in what format the result is to be presented.	Continuous, event-based; selective	5G network
Measured signal strength	Measured at UE and/or gNB. The IIoT application specifies when the signal strength is to be measured and in what format the result is to be presented.	Continuous; event-based selective	5G network

10.3 Aggregated parameters

Raw data is collected from an IIoT application, for instance from the device management server. When requested, aggregated figures are presented to the IIoT application.

Aggregation can be performed for each

- Single 5G cell ID or group of cells or an arbitrarily defined geographical area with 5G network coverage
- Device unique identifier, e. g. GPSI or network address of the UE,
- logical network,
- QoS profile.

Typical parameters for aggregation are provided in Sections 10.1 and 10.2.

5G-ACIA White Paper
Exposure of 5G Capabilities for Connected
Industries and Automation Applications

Contact
5G Alliance for Connected Industries and
Automation (5G-ACIA), a Working Party of ZVEI
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 – German Electrical and
Electronic Manufacturers' Association
5G Alliance for Connected Industries and
Automation (5G-ACIA), a Working Party of ZVEI
www.zvei.org

February 2021
Design: COBRAND Berlin

11 5G-ACIA Members

As of February 2021

- ABB
- altran
- arm
- ASKEY
- ASOCS
- ATHONET
- Audi
- aurelis
- BAYFU
- BECKHOFF
- Baicells
- BOSCH
- Canon
- celona
- 中国移动 China Mobile
- cisco
- DASSAULT SYSTEMES
- DENSO
- Deutsche Messe
- DFKI
- docomo
- Endress+Hauser
- EMERSON
- ERICSSON
- ETRI
- FESTO
- Fraunhofer
- GHMT
- HARTING
- HIRSCHMANN A BELDEN BRAND
- HMS
- HUAWEI
- IDLab INTERNET & DATA LAB
- ifak
- ifm
- III
- infineon
- inIT
- intel
- ITRI Industrial Technology Research Institute

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

5GACIA

www.5g-acia.org