5G ACIA
5G Alliance for Connected Industries and Automation

White Paper

Exposure of 5G Capabilities for Connected Industries and Automation Applications

5G Alliance for Connected Industries and Automation

Exposure of 5G Capabilities for Connected Industries and Automation Applications

Contact:
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
Lyoner Strasse 9
60528 Frankfurt am Main, Germany

www.zvei.org

May 2020

Graphics: ZVEI

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 use cases, in particular those use cases related to the management of communication services for devices.
- The second group focuses on network management use cases, 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 customized discrete manufacturing, for instance, 5G enables reliable wireless connectivity which will support e.g. flexible restructuring of production lines. More details on 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 which can address the connectivity needs of virtually any application imaginable in the consumer, enterprise and industrial IoT spaces. To this end, 3GPP has specified 5G to support enhanced mobile broadband, massive-scale IoT, and ultra-reliable and low-latency communications. 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 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 Structure and scope of the document

The current version of this white paper addresses requirements identified by 5G-ACIA and requirements described in relevant documents of 3GPP Release 16 and ongoing specification work for Release 17 (see [5] and [6]). Data models, which are commonly part of the interface specification work, are therefore beyond the scope of this document.

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

Section 4 introduces service exposure requirements for various operational use cases. A summary and future 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 while Section 8 describes architecture concepts for 5G exposure interfaces, and Section 9 describes related operational use cases.

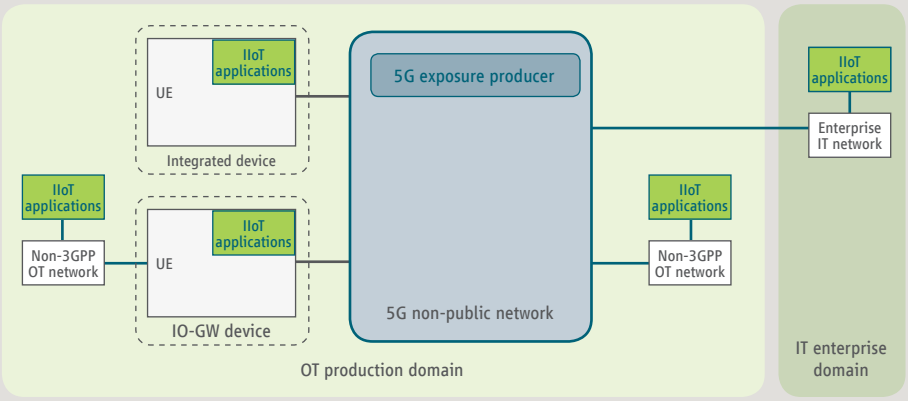
3 Essential assumptions

The focus of this white paper is on how to expose the capabilities of 5G non-public networks (NPN) to connected industries and in particular automation applications. Some essential solution assumptions are defined in this section in order to make the specified requirements easier to understand for the reader. 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 wired data networks. The prime role of exposure interfaces is to manage the user plane of a 5G NPN employed for transmission of application data in layers 2 or 3. Figure 1 depicts how devices can be connected wirelessly to the 5G NPN. It also depicts non-3GPP 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 different domains, such as the OT production domain and the IT enterprise domain. These domains are defined and explained in reference [10].

Fig. 1: User plane view of devices and networks connected via a 5G NPN



Source: 5G-ACIA

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] and [10])
- sensors/actuators or controllers/managers integrated into the device and/or an input-output gateway function (IO-GW), which enables connection of external (to the device) 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

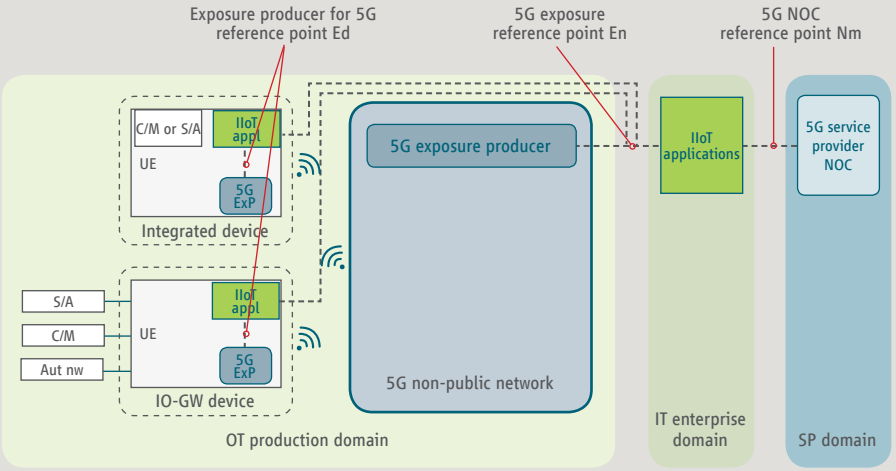
It should be noted that a 5G NPN can connect to non-3GPP networks, for instance TSN networks.

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.

The requirements listed 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 over two reference points, Ed and En. 5G services exposed over the Ed reference point are accessible only to local IIoT applications, i.e. an IIoT application running on a device. The respective reference point is situated between the IIoT application and the 5G system (see, for instance, Figure D.1-1 in reference [12]). 5G services exposed via the En reference point are accessible to 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 being established, monitored, changed, terminated, etc.) via the services exposed over En and Ed.
- Network management and configuration services required by IIoT applications (see Section 4.3.2), are made available by the service provider via the 5G network operation center (NOC) reference point Nm. These services include all corresponding stages in the 5G network life cycle, e.g. network installation, initial configuration, software management, and network decommissioning. These services and the reference point Nm are not in the scope of this white paper. They are depicted here for completeness; they are specific to NOC implementation and a matter of agreement between the service provider and an enterprise (e.g. the factory operator).
- Services may be provided by, e.g. the factory operator or by a third-party service provider, for instance a mobile network operator. In the latter case, the service provider's (SP) NOC is located within the SP domain. This is a public network from a factory operator's perspective.

Fig. 2: Deployment of reference points



Source: 5G-ACIA

More information is provided in Annex A.

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 [3], other relevant industry standards and documents, as well as the use cases provided in Annex B. Relevant use cases and the primary functions to be provided by 5G systems are summarized in reference [1], while 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 the right level of abstraction.
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 the future in a backward-compatible manner.
3. Service-based interfaces implemented in a service-oriented way, e.g. by means of open RESTful APIs.

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

Device management:
- device identity management
- device provisioning and onboarding
- device connectivity management
- device connectivity monitoring
- device group management
- device location information

Network management:
- network monitoring
- network configuration and maintenance

Security

4.2 Device management

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

Some requirements have also been identified directly by 5G-ACIA members in the OT domain. For related use cases, 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 to address and authenticate communication entities and to manage 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). Mapping of application identifiers to communication layer identifiers is generally performed in 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
- communication technology independency (5G, Ethernet, WLAN, Bluetooth, etc.)
- privacy and security (the OT data is sensitive and should not be accessible to third parties, for instance a mobile network operator)
- the convenience of managing OT device data from a central point of administration

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

Consequently, the requirements in relation to 5G exposure reference points are:

- A communication layer identifier, e.g. the generic public subscription identifier (GPSI) defined by 3GPP must be used at 5G exposure reference points for uniquely identifying a UE.
- OT application identifiers must not be used at 5G exposure reference points (see Annex A).

4.2.2 Device provisioning and onboarding

The 5G exposure reference points must support integration and configuration of a device into a 5G system by provisioning the relevant UE information (e.g. UE IDs, network access authentication keys, subscriptions) to the 5G core network to accept device connection when the device is activated.

The 5G exposure reference point En must support provisioning and onboarding of individual devices and groups of devices.

The 5G exposure reference point En must notify subscribers, for instance the device management server, when a device has connected to the network.

4.2.3 Device connectivity management

The 5G exposure reference point En must support the provisioning of:

- on-demand UE-to-UE and UE-to-data-network connections with defined quality of service (QoS), e.g. minimum service bit rate, minimum communication service reliability, maximum end-to-end latency, etc.
- multiple communication services per device, e.g. both Ethernet-based and IP-based communication services

For a list of QoS parameters see Sub-section C.2.2 in reference [6].

The 5G exposure reference point En must be able to acknowledge a communication service request within 100 ms [5].

For 5G-TSN integration, the 5G exposure reference point En must provide the 5G virtual bridge and port information to the IIoT application (e.g. a TSN centralized network controller, CNC). This information includes IEEE 802.1Q [15] traffic classes, bridge delay per port pair and per traffic class of the 5G system (5GS), and propagation delay per port.

The 5G exposure reference point En must enable the IIoT application, such as the CNC, to configure the 5GS bridge, including port configuration (e.g. IEEE 802.1Qbv traffic scheduling parameters [16]), TSN QoS, and traffic forwarding information.

4.2.4 Device connectivity monitoring

The 5G exposure reference points must support monitoring of device connectivity.

The 5G exposure reference points must support monitoring of individual devices (via Ed and En) and groups of devices (via En only).

The 5G exposure reference points must support on-demand, periodic, and event-triggered device connectivity monitoring. For event-triggered monitoring, it must be possible to define a list of triggering events, e.g. connection status change, device movements across mobile network radio cells, etc.

The 5G exposure reference point En must provide a history of communication events. These events include, for example, instances where there was a failure to meet the required QoS. This history may include timestamps of events and location-related information (e.g. the location of UEs and radio base stations associated with events).

The 5G exposure reference points must respond to a request to provide real-time QoS monitoring information within a specified time (e.g. within 5 s). This time is subject to negotiation between the communication service consumer and the 5G system.

4.2.5 Device group management

The 5G exposure reference point En must enable creation, modification, and removal of device groups, including definition of group communication services, and other group attributes (for instance the service area).

The 5G exposure reference point En must support the addition/removal of an individual device to/from a group.

It should be noted that a device may belong to multiple groups concurrently. A device may join/leave a group in accordance with, for instance, device location.

The 5G exposure reference point En 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]).

The 5G exposure reference point En must allow IIoT applications to obtain device location information with:

- location data of varying 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 (specified time intervals)

4.3 Network management

The requirements given in this sub-section are based on input from OT companies that are already or will in the future be operating 5G NPNs. As outlined in Annex B, the 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

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

The 5G exposure reference point En must support monitoring to verify that the network components, including component inventory information and network element capabilities, are configured and connected correctly.

The 5G exposure reference point En must support monitoring to verify that the (end-to-end) logical network(s) is/are configured correctly in the 5G system.

Reporting on the logical network(s) a device is (currently) connected to is enabled by the device connectivity monitoring requirements given above.

The 5G exposure reference point En must support monitoring to verify that a logical network is operating according to the prescribed service level specification (SLS). The SLS is the technical part of a service level agreement (SLA).

It must be possible to monitor high-level logical network metrics and KPIs through the aggregation of lower-level metrics and KPIs at the level of physical/logical network components. Access to lower-level metrics and KPIs at the level of physical/logical network components

must be permissible, subject to specific authorizations (e.g. when the NPN is operated as a stand-alone network by the enterprise).

The 5G exposure reference point En must allow monitoring of errors and other alarms from physical/logical network components and connections.

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

The 5G exposure reference point En must support these network monitoring capabilities when

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

4.3.2 Network configuration and maintenance

The information in this section is included for the sake of completeness only. It provides valuable background information for 5G network operators and 5G network equipment manufacturers with regard to the capabilities enterprises need to configure and maintain a 5G NPN.

The 5G NOC reference point Nm provides the means to:

- restart the 5G system fully or partially (i.e. specific network nodes or functions), for instance after a failure, to reestablish device connections without further manual interaction
- backup and restore the 5G system fully or partially, including firmware, software and configuration of network elements
- add, remove and modify existing RAN equipment (e.g. radio heads, base stations, with respect to spectrum management, etc.), and support changes to its operational status: i.e. enable / disable / temporarily disable
- add, modify and remove logical networks, and to add, modify, remove and relocate core functions per logical network
- manage IP/Ethernet network configurations (e.g. address ranges) in the 5G network to allow integration of 5G with non-3GPP OT networks (see Annex A)

Any change to the 5G network must be made in a controlled manner to prevent/minimize faults and service disruptions, and to minimize risks to compliance with the service level specification (SLS).

The above list of capabilities is not exhaustive. The capabilities required will vary and depend on the specific agreement between the service provider and the enterprise (e.g. factory operator).

4.4 Security requirements

The 5G exposure reference points must support means for:

- mutual authentication between the exposure producer (the 5G NPN) and the exposure consumer (an IIoT application)
- confidentiality and integrity of communication between the exposure producer and the exposure consumer
- authorization of the exposure consumer to use exposed capabilities in full, or limited to a subset of the capabilities, based on
  - the functional role of the IIoT application, e.g. network maintenance, network monitoring, or application data exchange
  - network location (e.g. indoor network or outdoor network)
  - logical network purpose (e.g. network configuration or application data exchange)

The 5G exposure reference point En must make the security logging information of UEs available to IIoT applications. An example for such information is 3GPP security mechanisms used in a device connection (e.g. data privacy, authentication, integrity protection).

5 Summary and outlook

This white paper describes the capabilities that a 5G non-public network (5G NPN) needs to expose to IIoT applications.

In order for the reader to better understand how the 5G services exposed via the reference points can be consumed by IIoT applications, the essential assumptions are described in Section 3 and expanded on in Annex A. For completeness, network configuration and management aspects that are outside the scope of this white paper are also mentioned (see Section 4.3.2).

Operational use cases related to the exposure requirements are grouped into device management and network management. The emphasis of the current version of this white paper is on device management operational use cases, which are further detailed in Annex B.

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

In a next version of this white paper, network monitoring use cases will be included and further detailed.

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	is, as per reference [7], a set of UEs using private communication for 5G LAN-type services.
5G LAN-type service	is, as per reference [7], a service over the 5G system offering private communication using IP and/or non-IP type 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 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. Examples for the latter are 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 users of the 5G system.
Interface	defines a set of interactions between functions needed to achieve a specific purpose.

IT enterprise domain	is a communications 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 portion of physical network resources. For instance, it can be a complete 5G network, a 5G network slice or a 5G LAN virtual network.
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 (SP)	is a legal entity that owns the 5G NPN and provides services to NPN users based on mutually agreed service level specifications (SLS). A service provider is responsible for the entire life cycle of the network.
SP domain	is the communication infrastructure used for the purposes of network configuration, management and commissioning, which is under control of a service provider or under control of an enterprise (e.g. factory operator).
User equipment (UE)	is, according to 3GPP, as defined in TS 21.905, a device that allows access to network services. According to 3GPP specifications, the interface between the UE and the network is the radio interface.

6.2 Abbreviations

3GPP	Third Generation Partnership Project
5G	Fifth generation
5GExRP	5G exposure reference point
5GS	5G system
AF	Application function
CNC	Centralized network controller
CP	Control plane
Ed	5GExRP for exposure on the device side
En	5GExRP for exposure in the core network
eUICC	embedded UICC (a.k.a. eSIM)
IIoT	Industrial Internet of Things
ICT	Information and communications technology
iUICC	integrated UICC (a.k.a. iSIM)
IT	Information technology
KPI	Key performance indicator
MNO	Mobile network operator
Nm	5G NOC reference point of the NOC for 5G network configuration and management
NOC	Network operations center
NPN	Non-public network
NW	Network
OPC UA	Open platform communication (OPC) unified architecture
OT	Operational technology
RAN	Radio access network
RFC	Request for comment
SLA	Service level agreement
SLS	Service level specification
QoS	Quality of service
SP	Service provider
TSN	Time-sensitive networking
UE	User equipment
UICC	Universal integrated circuit card (a.k.a. SIM card)
UP	User plane
UPF	User plane function
VLAN	Virtual local area network

7 References

[1] 5G-ACIA, White Paper, 5G for Automation in Industry, July 2019
[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, June 2017
[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, February 2019
[12] 3GPP TR 22.832, Study on enhancements for cyber-physical control applications in vertical domains
[13] Olaya, Santiago Soler Perez, et al. Communication abstraction supports network resource virtualization in automation, 2018 IEEE 27th International Symposium on Industrial Electronics (ISIE), IEEE, 2018.
[14] 3GPP TS 23.273, 5G system (5GS) Location Services (LCS)
[15] IEEE 802.1Q, IEEE Standard for Local and Metropolitan Area Networks - Bridges and Bridged Networks
[16] IEEE 802.1Qbv, IEEE Standard for Local and Metropolitan Area Networks - Bridges and Bridged Networks Amendment 25: Enhancements for Scheduled Traffic

8 Annex A: Solution concepts

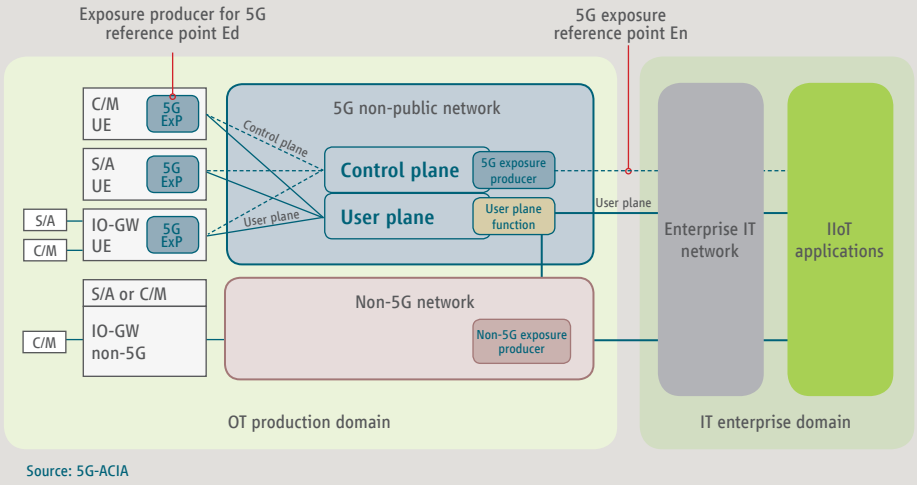
8.1 Architecture concepts for 5G exposure reference points

While some assumptions are given in Section 3, this annex further details those assumptions and provides guidance on implementation and integration of exposure interfaces.

A 5G NPN deployment may coexist with and require integration with a non-5G OT network. To this end, the transmission of e.g. Ethernet traffic via 5G 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: line controller-to-controller, controller-to-controller, controller-to-device, and device-to-compute.

Fig. 3: High-level reference point deployment

A: actuator; C: controller; M: manager; S: sensor



Source: 5G-ACIA

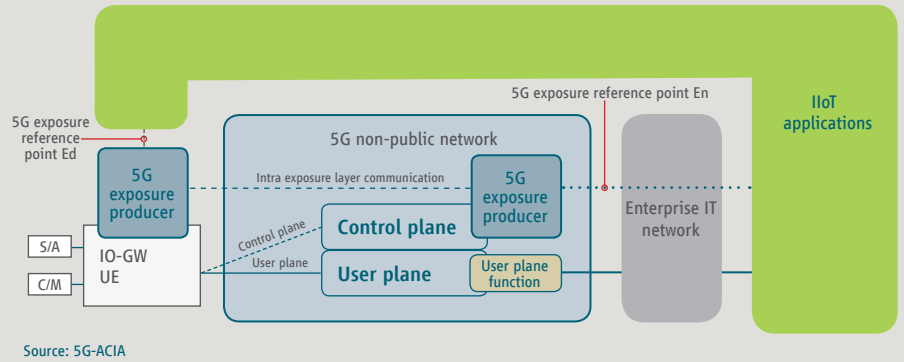
Figure 3 depicts the 5G exposure reference points in relation to the control and user planes of the 5G NPN and in relation to IIoT applications.

Figure 4 depicts the communication layer architecture of the overall system, including device-side and network-side perspectives. The control plane (CP) is employed to dynamically manage the user plane data connections with required transmission characteristics. These connections are used for transferring data between devices and IIoT applications via the 5G NPN.

The IIoT application may be a distributed application with its components communicating in the application layer using these data connections. They exchange application-specific information by means of application-specific protocols such as OPC UA.

5G capabilities are exposed to IIoT applications via the network-side 5G exposure reference point (denoted En) and via the device-side 5G exposure reference point (denoted Ed), so that the communication services of the underlying 5G system can be used in a simple, transparent, and efficient manner. The reference point Ed consists of local interfaces accessible only to IIoT applications executing in the device. On the other hand, the reference point En contains interfaces that are accessible remotely and used for exposing the capabilities of the entire 5G system subject to authorization policy. An IIoT application executing on the device or within the network may use reference point En if it has the required authorization.

Fig. 4: High-level communication-layer architecture



Source: 5G-ACIA

The intra 5G exposure layer communication shown in Figure 4 is used to enable exposure of device-side capabilities via reference point En. This provides, for instance, device-made measurements of the radio signal strength to an application. This intra exposure layer is internal to the 5G system and is, therefore, not visible at the 5G reference points.

The detailed description of the operational use cases in Annex B indicates whether reference point Ed or En is used.

When it comes to 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 for handling traffic, and for onboarding of devices and terminals. These stages typically include radio resource planning, configuration of the 5G network, comprising the radio access network (RAN), the core network (CN), 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, performance and report handling. Network management processes include tasks such as adding more capacity or reconfiguring parts of the network. Onboarding and offboarding of devices/terminals and managing device connectivity (e.g. QoS) are also performed during this phase.
3. The "retirement and upgrade" phase handles the big 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	

Source: 5G-ACIA

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 service provider's network operations center (NOC). The NOC is used for operating and maintaining the 5G NPN (see Figure 2). The service provider may be an MNO or an enterprise (e.g. factory operator). The NOC may manage one or many NPNs. The interfaces to the NOC are part of the 5G reference point Nm. They are not part of 5G reference point En and are, therefore, not addressed in this white paper (but mentioned here for completeness).

Integration with IIoT applications is expected to require some network-management-related operational use cases to be supported via the 5G reference point En; these requirements are described in Section 4.3.1.

8.2 Integration of 5G with wired networks

8.2.1 Integration of 5G NPN with Industrial Ethernet networks

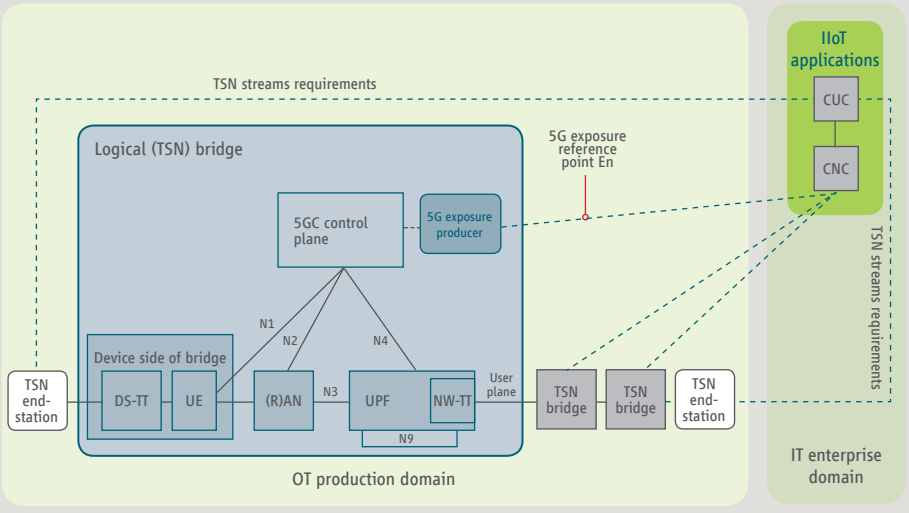
This white paper assumes the 5G network is deployed as a non-public network. 5G systems in compliance with 3GPP Release-16 specifications will offer 5G LAN-type services. One example would be the 5G system operating as an Ethernet bridge. Thanks to this new functionality, 5G systems will be able to support deterministic, time-sensitive layer-two traffic flows. In this context, the device management server can interact over reference point En to establish the 5G LAN-type services, associate them with virtual local area networks (VLANs) and therefore integrate them with legacy enterprise networks.

The integration of 5G with Ethernet networks is analyzed and explained in [10].

8.2.2 Integration of 5G NPN with TSN networks

In addition to supporting Ethernet connectivity, as of Release 16, 3GPP is also specifying integration of 5G with TSN networks. In this context, the 5G system integrates with the TSN network in the form of a TSN bridge within a centralized configuration model. The user plane TSN translators are placed at the egress points of the 5G system, i.e. at the user plane function (UPF) and the UE (see Figure 5). The TSN application function (TSN-AF) interacts with the TSN CNC to configure TSN flows in the 5G system. The 5G exposure reference point En exposes the TSN-AF capabilities.

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

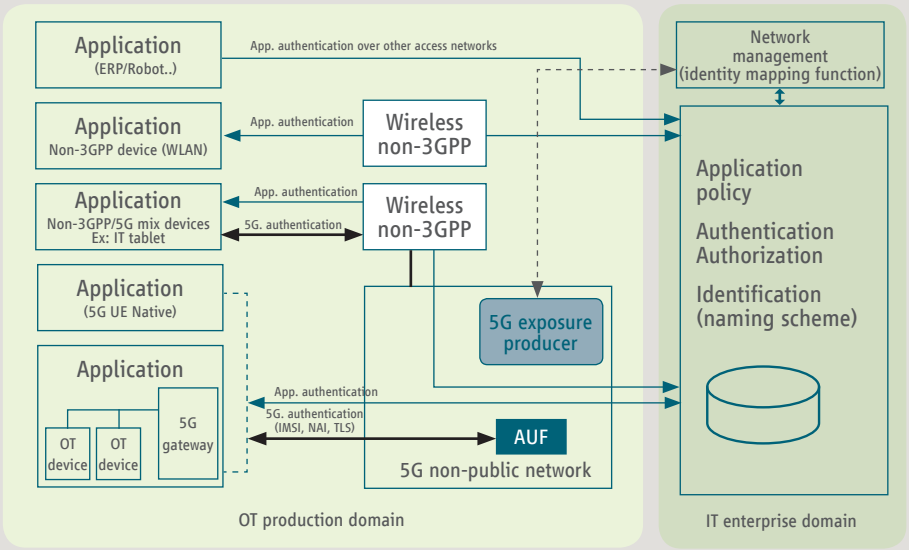


Source: 5G-ACIA

8.3 Device identities, authentication and authorization

A logical view of the authentication of communication devices and IIoT applications that leverage 5G NPNs is shown in Figure 6.

Fig. 6: Authentication and authorization of IIoT applications



Source: 5G-ACIA

The UE authenticates itself to gain access to the 5G network. To this end, the UE employs a subscriber permanent identifier (SUPI), a network access identifier (NAI), a transport layer security (TLS) certificate or another credential. 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 application in the IT enterprise domain and 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.

The network management application maps the IIoT application identifier to the UE identifier. As a result, any application can address the IIoT application (or a device) connected via the 5G network. Note that interactions with the 5G network via the exposure reference point En only make use of the device's 5G generic public subscription identifier (GPSI).

Within the 5G system, each UE is allocated a SUPI, UE connectivity service subscription. The SUPI is in the format of IMSI (international mobile subscriber identity) or NAI (RFC 7542).

For reasons of confidentiality and security, the SUPI is not disclosed "over the air" or to any IIoT applications and is not made available outside of the 5G system and also not via the 5G exposure reference points. Instead, a GPSI is used on the 5G exposure reference points to uniquely identify a UE. The 5G system maintains mapping between GPSI and SUPI. 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.

A non-3GPP device can also access the enterprise IT network via a wired network or a WLAN access point that is 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 case, too, application-level authentication is performed via a data connection and is not divulged to the 5G system.

Note that 3GPP Rel-16 does not include support for non-3GPP access to a 5G NPN.

Note, also, that a device may consist of more than one UE.

9 Annex B: Detailed use case descriptions

The use cases 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 (En consumer; IT enterprise domain) Device provisioning and onboarding service (En producer; 5G NPN) Device connectivity monitoring service (En 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 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 purposes (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) used for application-level device configuration purposes.	
Execution – step 1	How the device is configured to access the 5G NPN depends on the security and provisioning solution. a. In the case of UICC, this implies inserting the card obtained from the 5G NPN operator (the card is provisioned with 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 (as per GSMA procedures). 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 done 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 obtains access credentials and subscriber profile for access to the 5G NPN. Note that as described in Annex A, the identity mapping function is configured with mapping between device identity and the GPSIs for the device(s).	

	As part of this provisioning step, the device management server invokes 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. 2. Authorization to the NPN of a set of devices with given GPSIs ("bulk authorization"). Note that a device may be assigned multiple GPSIs if it contains 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 about 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 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 (En consumer; IT enterprise domain) Device provisioning and onboarding service (En producer; 5G NPN) Device connectivity monitoring service (En 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) knows the mapping between device identity and GPSI(s) 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 GPSI from the NPN 2. Remove a set of devices (in bulk) with given GPSIs from the NPN Note that a device may be assigned multiple GPSIs, if it contains multiple UEs. In that 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 with regard to 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 GPSI is 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	
Actors	Device (Ed consumer) with an integrated 5G UE (Ed producer) Device management server (En consumer; IT enterprise domain) Device connectivity management service (En producer and Ed producer; 5G NPN)	
Pre-conditions	The device has an established connection to one or more logical networks and the device management server was notified of device connectivity status.	
Execution – step 1	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 the local application function, respectively). 1. Modify the current QoS parameters of an already established connection. 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 network address and the associated 5G NPN resources.	For 5GS integrated with TSN, TSN-defined mechanisms are used. The device management server may be instructed by enterprise resource planning (ERP) or manufacturing execution system (MES) about needed connectivity per device.
Execution – step 2	The device connectivity management service triggers related network procedures and may instruct the device to execute connectivity management procedures. The device management server or the local application function is notified by the device connectivity management service about the successful or unsuccessful execution of the requested procedure. At each QoS modification and each additional connection establishment procedure, the availability of resources in the 5G system is assessed. If the limits of resources are reached, the procedure may fail. Where the device management server made a successful request, the device's local application function is notified (Ed) when the execution was successful. Otherwise, it is notified of its failure.	
Post-conditions	TThe device has established and/or terminated one or more connections with QoS parameters. The connectivity status is known to the device management server, which may present the information in a human-readable format to an OT 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 of a device that is already onboarded	
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.	
Execution – step 1	The device management server or a device's local application function queries the device connectivity monitoring service for the status of a particular device connection or a set of connections. The device connectivity monitoring service replies via En or Ed with, for instance, • connection(s) established and associated connection type(s) (IP or Ethernet); • network address per connection and used logical network; • (optional) logical network(s) used; • the configured QoS parameters per connection; • (optional) permanent equipment identifier (PEI) and, if applicable, other proprietary device attributes; • (optional) certificate status; • (optional) network access restrictions; • (optional) the current RSRP (reference signals received power) value measured at the device's current location. The status information is compiled in a machine-readable format, for instance in XML or JSON.	
Post-conditions	The device has 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 of service query	
Goal	Obtain detailed device status and measured connectivity-related data of a device that is already onboarded	This use case can be applied for 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.	
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 time duration must be specified. For long durations (e.g. weeks), the data granularity level will inadvertently be coarse, e.g. days. For short durations (e.g. days), the granularity can be finer (e.g. hours). The device connectivity monitoring service replies via En or Ed, respectively, with, for instance: • the current latency • the minimum service bit rate over the last hour • current cell ID • historical latencies • historical minimum service bit rate over 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 what attribute is monitored. For instance, concerning communication service reliability, time stamps from the beginning and end of the unavailability of the communication service in question are of interest. For end-to-end latencies it could be the maximum of the end-to-end latencies over a pre-defined period. Additionally, the distribution function of the end-to-end latency could be of interest.
Post-conditions	The device management server and/or the device's local application function knows the device 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 of a device or a device group	This use case can be applied for regular monitoring purposes.
Actors	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.	
Execution – step 1	The device management server or the device's local application function subscribes with the device connectivity monitoring service for events concerning the device connectivity conditions changes. Subscription can be made for e.g. the following events: • maximum latency exceeded; • minimum service bit rate not achieved; • communication service availability dropped below requested value; • connectivity dropped / connectivity re-established; • RSRP values below threshold; • cell change (handover). The device connectivity monitoring service will initiate respective supervision functions in the 5G NPN nodes and will acknowledge the event subscriptions if successful. Otherwise, a failure response is returned.	During normal operations of a well-designed and dimensioned 5G NPN no such events should be triggered.
Execution – step 2	The device connectivity monitoring service will trigger an event notification towards the device management server or the device's local application function, including: • the device ID (GPSI); • the event type as well as the reached/exceeded threshold value; • (optional) multiple event types occurring simultaneously may be grouped into a single notification (e.g. if they are caused by the same source); • (optional) events affecting all devices of a device 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 with the device connectivity monitoring service to events concerning 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 the device's local application function, respectively, 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 (Ed consumer) with an integrated 5G UE (Ed producer) Device management server (En consumer; IT enterprise domain) Device group management service (En 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 its attributes, including network name, communication type (IP or Ethernet), VLAN identifier, and default QoS parameters for device connection to the 5GLAN group. The device group management service provides the 5GLAN group data to the 5G system and replies with an external group identifier for the 5GLAN 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 with success or failure. In case of 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 and, optionally, other devices in the group are notified, too. 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) is/are added or removed from a 5GLAN group.	
Post-conditions	5GLAN groups are provisioned in the 5G NPN and a device is 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 of a device (or a group of devices)	
Actors	Device with an integrated 5G UE Location-aware application (En consumer) Device location management service (En producer; 5G system)	
Pre-conditions	The 5G NPN is operational and the targeted devices are onboarded.	
Execution – step 1	The location-aware application requests the current and/or deferred location of a device or a 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 [14]. The response time includes the time to first fix. The device location management service determines the current location of the device or a group of devices in accordance with the requested location service quality and responds with location information of the device(s). A request for deferred 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 pre-defined area); • periodically reported location, i.e. location information is provided at specified time intervals; • movement (an event where the device moves by more than some predefined distance from a predefined location). When a device location event occurs for a device or a 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 about the device(s).	
Post-conditions	The location of device(s) is available and provided upon request or upon the occurrence of an event.	

Source: 5G-ACIA

10 5G-ACIA members

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

Source of front-cover image: Variante B