

Title: 5G capabilities exposure for factories of the future – identified gaps

Source: 5G Alliance for Connected Industries and Automation (5G-ACIA)

To: 3GPP TSG SA, 3GPP TSG CT

CC: 3GPP TSG SA WG1, 3GPP TSG SA WG2, 3GPP TSG SA WG3, 3GPP TSG SA WG5, 3GPP TSG SA WG6

Date: September 6th 2022

Contacts: Dr. Andreas Mueller, 5G-ACIA Chairman (Andreas.Mueller21@de.bosch.com)
Dr. Afif Osseiran, 5G-ACIA Vice-Chairman (Afif.Osseiran@ericsson.com)
Alexander Bentkus, 5G-ACIA Secretary (bentkus@zvei.org)

1. Overall Description

In 2021, 5G-ACIA published a revised white paper on the exposed 5G capabilities that are needed by factory operators to manage and maintain industrial 5G devices and 5G Non-Public Networks (NPN) in a simple and efficient manner [1]. 5G-ACIA informed 3GPP about this work in SP-210281 and a reply LS was provided in SP-211134. 5G-ACIA wishes to thank 3GPP for their answer and collaborative spirit.

In the meantime, 5G-ACIA mapped these requirements onto Rel-17 specifications and identified the gaps and possible limitations as listed below. Some of these gaps could be relevant for future 3GPP work.

Gap ID	Description	Corresponding requirement in the 5G-ACIA whitepaper mentioned above
G.1	<p>Provisioning of single subscriptions or a bulk of subscriptions by a provisioning server (which is assumed to be an IIoT function outside of the NPN domain) is identified as a requirement from enterprises.</p> <p>This is not seen as a gap in 3GPP specifications, because a provisioning protocol is not currently in the scope of 3GPP.</p> <p>Provisioning via exposure reference points could be considered for future work by 3GPP.</p>	<p>[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</p> <p>[R-4.2.2-02] The 5G exposure reference points must support provisioning and onboarding of individual devices and groups of devices</p>
G.2	<p>The 5G exposure reference point must be capable of acknowledging a service request within 100 ms. The acknowledgement may include the requested information or may be a service request acknowledgement followed by the actual requested information. In the latter case the requested information must be provided within a specified time.</p>	<p>[R-4.2.3-02]* The 5G exposure reference points must be capable of acknowledging a communication service request within 100 ms.</p> <p>[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.</p>
G.3	<p>Provision of security event/logging information is identified as gap in 3GPP specifications.</p>	<p>[R-4.4-5]† The 5G exposure reference point must be able to provide a history of communication events.</p>

* A similar requirement is found in clause 6.10.2 in TS 22.261.

† A similar requirement is found in clause 6.10.2 in TS 22.261.

<i>Gap ID</i>	<i>Description</i>	<i>Corresponding requirement in the 5G-ACIA whitepaper mentioned above</i>
G.4	For providing a traffic profile applicable to the connections of a UE, and for knowing the status, the current specifications do not address the case of a group of devices in a single request.	[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 traffic profile may be provided when a new connection is requested, or when an existing connection is modified.

5G-ACIA also identified the following limitations of 3GPP specifications.

<i>Limitation ID</i>	<i>Description</i>	<i>Corresponding requirement in the 5G-ACIA whitepaper mentioned above (if applicable)</i>
L.1	A solution for VLAN tag assignment that is not dependent on secondary authentication and a corresponding authentication server may be needed. Note: The only standardized way of assigning VLAN tags is by using an authentication server DN-AAA with secondary authentication. This means that an authentication server DN-AAA must be deployed, and authentication credentials for secondary authentication must be managed just for supporting VLAN tag assignment, even in cases where there is no other reason for using secondary authentication.	N/A

<i>Limitation ID</i>	<i>Description</i>	<i>Corresponding requirement in the 5G-ACIA whitepaper mentioned above (if applicable)</i>
L.2	<p>Currently, application-centric QoS profiles such as those in clause 5 in TS 22.104 can only be translated into “5G-native” QoS profiles in a pre-defined manner. For instance, the factory owner describes these QoS profiles in an SLA. Thereafter, the NPN operator translates them into “5G-native” profiles and provides the owner with IDs for each of the profiles.</p> <p>However, it can be foreseen that not all QoS profiles are known, for instance if automation devices intermittently enter the factory premise and request previously undefined QoS communication service. Therefore, a more dynamic solution is needed.</p>	N/A
L.3	<p>Establishment of UE-to-UE QoS bearer with a single API call is considered as a limitation when NEF is used (currently one API call per each UE would be required).</p> <p>Note that SEAL already has support for UE-to-UE QoS bearer establishment with one API call only.</p>	<p>[R-4.2.3-01] The 5G exposure reference points must support:</p> <ul style="list-style-type: none"> • on-demand UE-to-UE (UNU) or UE-to-data-network (UN) connections with a defined quality of service (QoS) • multiple connections per device, each characterized by QoS parameters • modification of an established UNU or UN connection (e. g. new QoS parameters) and termination of a connection

<i>Limitation ID</i>	<i>Description</i>	<i>Corresponding requirement in the 5G-ACIA whitepaper mentioned above (if applicable)</i>
L.4	NEF only supports QoS monitoring for delay. For other QoS parameters, NEF only provides a binary notification about QoS degradation but does not provide additional information. It is considered beneficial to provide an indication about a degraded QoS and in what way it is degraded.	[R-4.2.4-01] The 5G exposure reference points must support monitoring of device connectivity, including the connection's QoS
L.5	IP address assignment is not provided via the exposure interfaces. It is considered beneficial to expose this feature to Application Functions.	[R-4.2.1-02], Note 2 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 point.
L.6	Fine-grained authorization on the level of specific services and resources, e.g. restricting API requests from specific AFs for specific UEs, is not specified in the standards.	N/A

2. Actions

5G-ACIA kindly asks 3GPP to take note of the identified gaps and limitations in Rel-17 specifications for considerations in the ongoing and future activities of 3GPP.

3. Date of Next 5G-ACIA Plenary Meetings

- 5th – 8th December 2022, Plenary Meeting in Frankfurt
- 21st – 22nd February 2023, Plenary Meeting, virtual (tbc.)

4. References

- [1] 5G-ACIA whitepaper, [Exposure of 5G Capabilities for Connected Industries and Automation Applications](#), 2021.