D5.5

REPORT DESCRIBING THE FRAMEWORK FOR 5G SYSTEM AND NETWORK MANAGEMENT FUNCTIONS

The 5G-SMART project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 857008.

Report describing the framework for 5G system and network management functions

Grant agreement number: Project title: Project acronym: Project website: Programme:	857008 5G Smart Manufacturing 5G-SMART www.5gsmart.eu H2020-ICT-2018-3
Deliverable type: Deliverable reference number: Contributing workpackages: Dissemination level: Due date: Actual submission date:	public report D19 WP5 Public 30th November 2021 30th November 2021
Responsible organization: Editor(s): Version number: Status:	ERI-DE, CUMU Dhruvin Patel, Jose-Costa Requena V1.0 Final
Short abstract:	This deliverable introduces a new industrial-centric 5G network management framework that is tailored for industrial applications. Furthermore, the document provides details on the prototyped industrial network slice management tool.
Keywords:	5G network management, Service Enabler Architecture Layer for Verticals (SEAL), Time Sensitive Network (TSN), Network Slicing

Contributor(s):	Dhruvin Patel (Ericsson) Géza Szabó (Ericsson) Hubert Przybysz (Ericsson) Jose-Costa Requena (Cumucore) Marilet De Andrade (Ericsson)

Disclaimer

This work has been performed in the framework of the H2020 project 5G-SMART co-funded by the EU. This information reflects the consortium's view, but the consortium is not liable for any use that may be made of any of the information contained therein.

This deliverable has been submitted to the EU commission, but it has not been reviewed and it has not been accepted by the EU commission yet.

Executive summary

Successful integration of smart manufacturing applications and industrial communication technologies with 5G system requires an aligned configuration of the network management as well as the configuration of a whole end-to-end (E2E) system. The 3rd Generation Partnership Project (3GPP) has introduced several enhancements for 5G System (5GS) ensuring such a seamless integration on the north-bound interface towards industrial applications which use the system. This report investigates, how such enhancements come together and interwork with existing and upcoming industrial communication technologies (e.g., Time Sensitive Networking) and industrial applications. The report provides a detailed view of the existing 5G network management approaches from the various standardization development organization (SDOs). Industrial network slicing, as a part of the overall network management, is seen as one of the mechanisms within 5GS to allocate specific network resources for certain demanding industrial applications. The report also provides highlights on the prototyped industrial network slice management tool (INSM). The INSM allows the creation of network slices and groups of industrial end devices i.e., 5GLAN groups that can be registered with the slice. With INSM the slice can be associated with a set of dedicated end-to-end network resources from radio, core and transport networks. A conceptual network management framework is proposed which builds upon the 3GPP defined Service Enabler Layer for Verticals (SEAL) architecture and Common API Framework (CAPIF). The framework is designed with the aim to hide slice management complexity from industrial applications as much as possible, thus simplifying interaction and implementation of the industrial applications and 5GS over the north-bound interface. The analysis shows how different configurations can be enabled for plug and produce use cases with such a network management framework.

Contents

1 Introduction

A successful integration of a 5G deployment in the smart manufacturing domain should consider network management as an important dimension. Today in the smart manufacturing domain, a wide range of network management solutions are available for the existing wired industrial communication technologies (e.g., ABB NeCo[1]). Such solutions are commonly used to manage the layer 2 and 3, Ethernet-based wired networks by implementing the mechanisms and protocols defined by IETF (e.g., SNMP) and/or IEEE 802.1 Bridges network management aspects (e.g., Link Layer Discovery management) standards. In current industrial deployment settings, often the applications and network configurations are done separately (shown in Figure 1). Taking an example of industrial real-time Ethernet variants, specialized tools (e.g., SIMATIC S7 for PROFINET) are available today which allow manual or automatic configuration from an industrial application. Lately, with the introduction of the Time Sensitive Network (TSN) and standardized Industry 4.0 architecture (RAMI model), there is now ongoing effort observed within SDOs and Industry fora to define specific network management aspects for TSN-based industrial networks (IEC/IEEE 60802 TSN profile for industrial network management[2]). From the 5G technology perspective, several new features are introduced which enable simplified integration of vertical applications (such as smart manufacturing) since Release 15.

It is foreseen that the 5G system will co-exist with other industrial communication network technologies such as Ethernet-based industrial networks (e.g., Time Sensitive Networking). Considering 5G system co-existence with existing industrial wired network technologies, the following points are important to consider when defining a network management platform:

- 5G system network framework should interwork with both:
  a. Ethernet-based industrial network management system.
  b. existing or advanced available industrial applications platforms such as Robot Operating System (ROS), where 5GS supports native connectivity solution.
- Existing industrial applications and network management platforms shall not require in-depth knowledge of 5G system functionality and mechanism to enable network configuration.
- There is a need for a simplified solution by which existing industrial network technologies can leverage 5G infrastructure functionality (e.g., group management, location, time synchronization) with very little efforts.
- Finally, there should be standardized interfaces which allow ease of negotiation between 5G system deployment and an existing networking infrastructure.

1 https://library.e.abb.com/public/995bfb356f614dcc944768301015034f/3BSE080639_C_en_800xA_Networks_-_NE840_user_manual.pdf
2 https://1.ieee802.org/tsn/iec-ieee-60802/

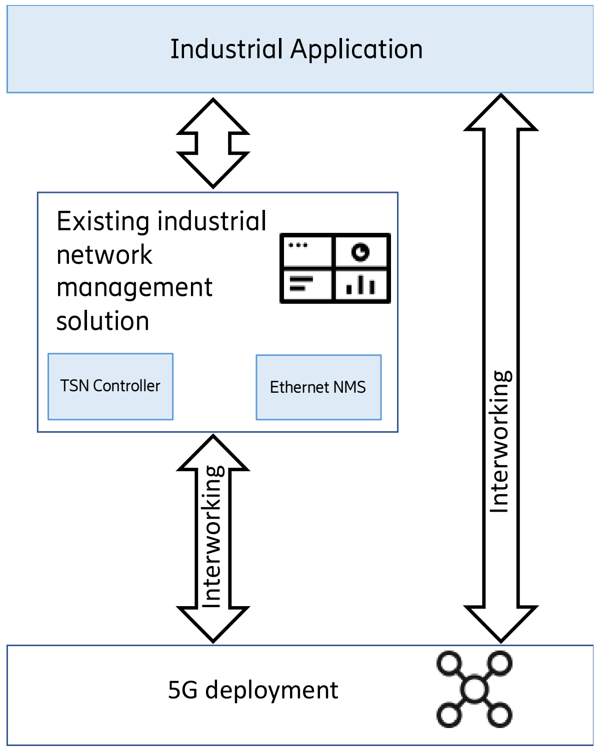

Figure 1 5G interworking with an existing industrial infrastructure

To summarize, there is a need for a simplified 5G network management framework that hides the implementation details of the 5G system and provides a simple integration with an existing industrial network management system (NMS) and industrial applications (or OT applications). Figure 1 provides a view on the interworking aspects to be considered for a 5G integrated network scenario. With this above motivation, 5G-SMART aims to develop such a 5G conceptual network framework. Furthermore, 5G-SMART has prototyped an industrial-centric network slice management tool considering the requirements summarized in section 4.

1.1 Relation to other work packages

In 5G-SMART, work package five (WP5) focuses on the technical aspects going beyond the trial work packages (WP2, 3, and 4). It investigates 5G features, its enhancements, and their integration within the manufacturing ecosystem.

Figure 2 shows the overall workflow of WP5 and the three key focus areas of WP5. WP5 takes input from use case requirements defined in 5G-SMART Deliverable D1.1 [5GS20-D11] and provides input to dissemination activities in WP6. Network management aspects of integrated 5G network are one of the main target areas of WP5 and are elaborated in this document.

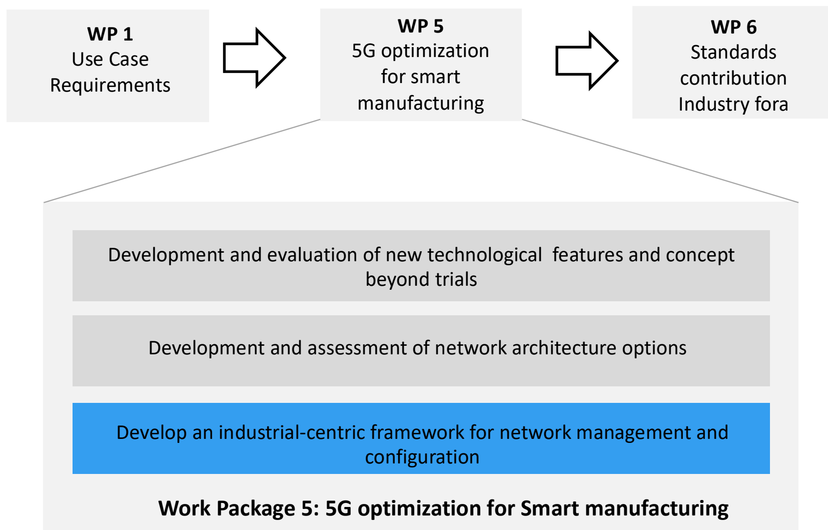

Figure 2 Workflow of WP5

1.2 Objective of the document

The objective of this document is to investigate existing technical enablers for the 5G network management framework and further propose the industrial-centric network management framework. The framework is tailored for the 5G-SMART use case requirements proposed in the D1.1 Deliverable [5GS20-D11]. The main highlights of the document can be summarized in below points:

1. Conceptual 5G industrial-centric network management framework
2. Prototyped industrial-centric network slice management tool

1.3 Structure of the document

Figure 3 shows the overall structure of the document showing the methodology chosen to achieve expected results. The deliverable starts with listing down functional requirements of the 5G-SMART use cases from the network management perspective. Furthermore, based on the requirements, existing 5G network management and OT technical enablers are investigated. Section 4 provides details on the prototyped industrial-centric network slice management tool. Section 5 proposes a new industrial-centric network management framework. Based on the proposed framework, a use case of plug and produce is analyzed for various types of the industrial application configurations.

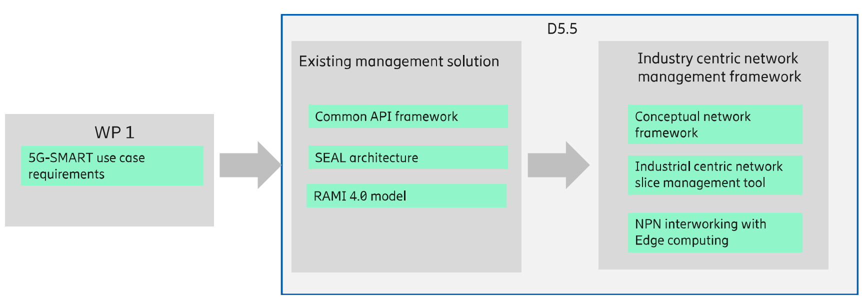

Figure 3 Structure of the document

2 Industrial requirements on the network management framework

5G-SMART explores a wide range of smart manufacturing use cases (Table 1). A comprehensive description of the use-cases can be found in Deliverable D1.1 [5GS20-D11]. This section provides an overview of the functional requirements (as shown in Table 2 below). Requirements from the use cases indicate that 5GS network management and configuration functionality should interwork with existing industrial network management system (e.g., Ethernet network management system), else it would create more complexity to manage such a heterogenous network (5GS interworking with existing industrial network). The requirements imposed on the 5G system clearly show the need for the simplified network management and configuration functionalities.

Table 1 5G-SMART Use cases [5GS20-D11]

No.	5G-SMART use case
UC 1	5G-Connected Robot and Remotely Supported Collaboration
UC 2	Machine Vision Assisted Real-time Human-Robot Interaction over 5G
UC 3	5G-Aided Visualization of the Factory Floor
UC 4	5G for wireless acoustic workpiece monitoring
UC 5	5G Versatile Multi-Sensor Platform for Digital Twin
UC 6	Cloud-based Mobile Robotics
UC 7	TSN/Industrial LAN over 5G

Table 2 Functional requirements from 5G-SMART use cases

Functional requirements	Characteristics/Details	Related 5G-SMART use case
Network status, capability exposure, and interface towards Operation & Management (O&M)	For an efficient integration of 5G system with the infrastructure of the factories of the future as well as with applications, some use cases require an exposure of the 5G communication status and configuration concerning device connectivity management (e.g., for configuring QoS or network slices).	UC1, UC2, UC3, UC5, UC7
Ensuring diverse QoS requirement for industrial applications is satisfied	5G network slicing is one of the possible solutions to realize several use cases having various QoS requirements on top of the same network infrastructure in a flexible, resource-efficient, and secure manner.	UC5 and UC7

Time synchronization management	5G network management framework should provide functionality allowing to dynamically manage time synchronization methods to OT management application.	UC 4 and UC 7
Layer 2 switching/TSN management in integrated industrial based network with 5G system	Transporting TSN and industry LAN (I-LAN) traffic over 5G requires appropriate data-plane features (encapsulation / decapsulation) of TSN/I-LAN frames at the communication end points. The 5G network management framework needs to take care of the configuration of the control-plane features and its interaction with industrial network management system (e.g., TSN's Central Network Configuration (CNC))	UC7

3 Existing network management solutions

Today, existing network management solutions for 5G system infrastructure and industrial wired communication technologies are separate entities and the interworking between them is not clearly defined. This section dives into efforts of the 5G system to expose its capabilities which can be leveraged by the industrial network management solutions. These exposure capabilities are essential for such integration. Following section 3, section 4 provides details on how such interworking can be realized with the proposed industrial network management framework, that also includes the industrial network slicing management tool. This section provides details on the existing and emerging solutions for the network management. Considering requirements from section 2, the section provides an overview on the relevant features of the 5G technology standards to support integration with the smart manufacturing applications. This section forms a baseline for the proposed conceptual network framework (described in section 4).

3.1 5G management and exposure function

3GPP starting from Release 15 has developed features that enable seamless integration of the vertical application on the northbound interface of the 5G System (5GS). According to 3GPP, a Northbound API is an interface between an Application Server (either in a mobile operator's network or external to it - operated by a third party) and the 3GPP system via specified Functions in a mobile operator's network[3]. The evolution of the 5G standards in the same direction can be seen in 4. In Release 15, the focus of the 3GPP was to provide a simplified Application programming interface (API) framework which can be used to leverage 5G functionality. The result was a Common Application Programmable Interface (API) framework (CAPIF) [3GPP20-23222]. CAPIF was defined with an aim to provide a unified northbound API framework. This framework allows harmonization of API development and exposure across 3GPP network functions. Further, Releases 16 and 17 brought vertical specific features with the aim to simplify the implementation and deployment of 5GS in large scale vertical systems. Below more details on the 3GPP specified functionality to support north bound integration with industrial applications and network management system are provided.

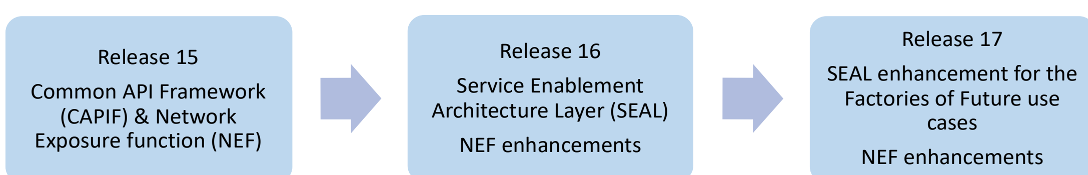

Figure 4 Evolution of 3GPP standard to enable seamless integration on northbound interface

3.1.1 Common API Framework (CAPIF)

CAPIF offers a unified framework to expose securely APIs from 5GS towards industrial applications. CAPIF provides all the essential functionalities for consumers and providers of APIs, such as onboarding, discovery, secure communications, authentication, and authorization for hosting APIs. CAPIF key functional entities include CAPIF core functions, API exposing function and API invoker.

[3] https://www.3gpp.org/news-events/1854-common_api

API invoker is the application that requests service from the 5G system via CAPIF framework. It interacts with CAPIF core functions to discover available APIs and will consume the services provided by the API exposure functions. In the smart manufacturing domain, an API invoker can be implemented in the existing network management solution or industrial application which can invoke services from the 5G system. For example, OPC server and Ethernet NMS can be realized as API invoker.

CAPIF core functions include all the related functionalities of API handling from authorization to monitoring the service API invocation. Figure 5 shows the interfaces through which an API invoker can communicate with CAPIF core function and API exposing function. API exposing function (AEF) wraps around the existing 3GPP functions and are called by the API invokers. API invoker in our case can be industrial applications. Here, 3GPP functions can be Network Exposure Function (discussed later in section 3.1.3 or Service Enabler Architecture Layer Server (SEAL) (discussed in section 3.1.2). API exposing main functionality includes authentication of API invoker (industrial application) based on the information provided by the CAPIF core function, validating the authorization provided by the CAPIF core function and logging service API invocation at the CAPIF core function.

To summarize, CAPIF is a standardized framework which acts as gateway for exposing the 5G capabilities to industrial applications or network management applications. From a deployment perspective, industrial applications and network management systems must implement necessary functionalities defined by CAPIF standards to interact with CAPIF core and exposing function.

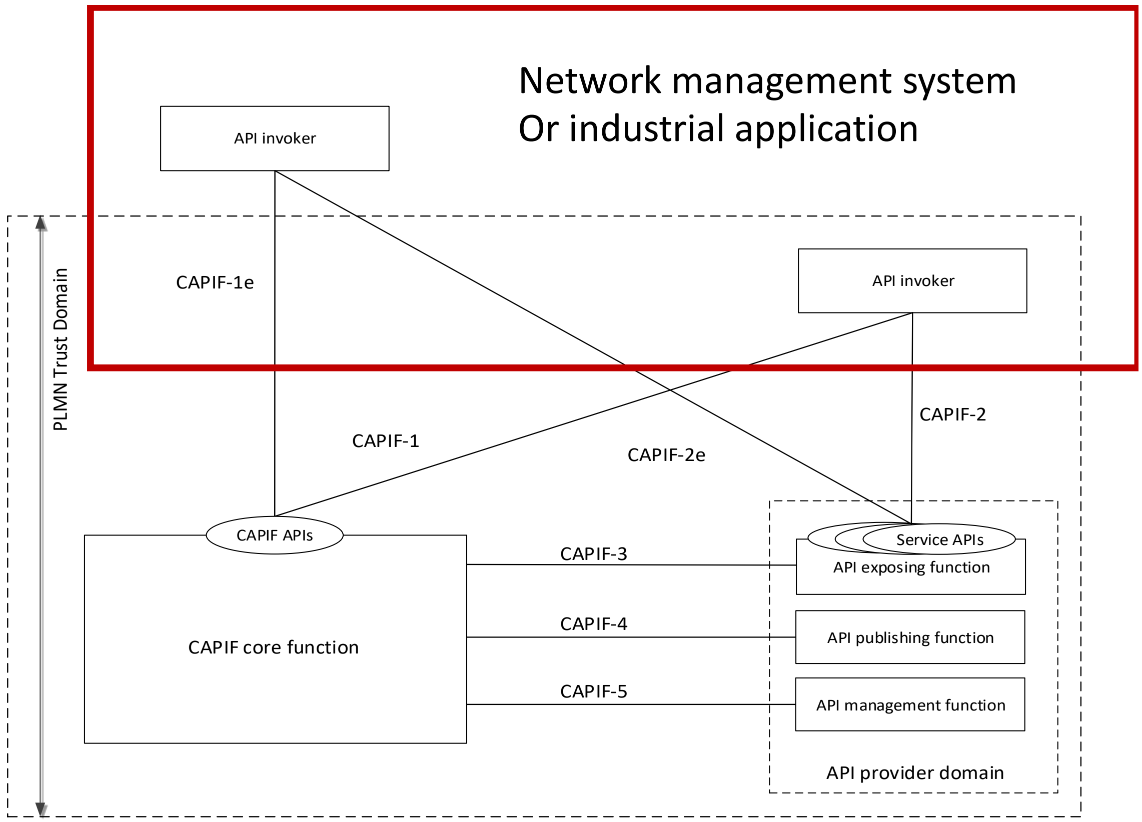

Figure 5 Functional model for the CAPIF from [3GPP20-23222]

3.1.2 Service enabler architecture layer (SEAL)

SEAL architecture defined by 3GPP aims to provides flexible APIs dedicated for the industrial application integration, thus simplifying the interaction of the industrial application with 5G system on northbound interface. Starting from Release 16, SA6 working group within 3GPP has defined Service Enablement Architecture Layer (SEAL), which provides Representational State Transfer (REST)ful application programmable interface (APIs) for flexible integration of the OT application. A high-level architecture of the 5G system with the SEAL functionality for integration with existing OT application and system is shown in Figure 6. The SEAL client interacts with the device end of the manufacturing application (also called vertical application client) for configuration and exposure aspects. The SEAL server on one end communicates with 5GS to a relevant 3GPP function and on the other end interacts with the manufacturing application or network management system.

In the context of the CAPIF framework, the SEAL server acts as CAPIF's API exposing function and the manufacturing application (vertical application layer) acts as API invoker. Application enablement layer includes components of the SEAL architecture which exposes northbound APIs. SEAL provides main capabilities including

1. Group management service,
2. Configuration management service for UE configuration, user profile

3. Location management service for cell, service area and geo coordinates,
4. Identity management and key management service for user authentication and authorization, and
5. Network resource management service for establishment of the connectivity with QoS
6. Network slice capability management.

Additionally, to support seamless integration with smart manufacturing applications, 3GPP is currently finalizing the enhancement of the SEAL APIs functionality. This enhancement includes support of configuring and remapping of networking slicing based on changing requirement, geographic location and positioning information, time synchronization management, TSN integration support, QoS monitoring and 5G LAN group management. The exact solution on how 5G SEAL APIs will be exposed towards manufacturing application and existing OT technologies will be documented in Release 17 specification. 3GPP technical specification (TS) 23.434 [3GPP20-23434] will provide further details on the solution. Release 17 enhancements to SEAL also include the setup of the TSC flows in the 5GS deployment without industrial TSN integration. The solution provides a mechanism for 5GS to directly interact with industrial application (Centralized User Configuration) and enabling configuration of the 5GS-end Ethernet ports (DS-TTs and NW-TTs) to fulfil the QoS requirements. To enable such mechanism, Network Resource Management (NRM) application function within SEAL server is further enhanced with functionalities like TSN-AF and Time Sensitive Communication Time Synchronization Function (TSCTSF). The solution is illustrated with use case in section 6.4

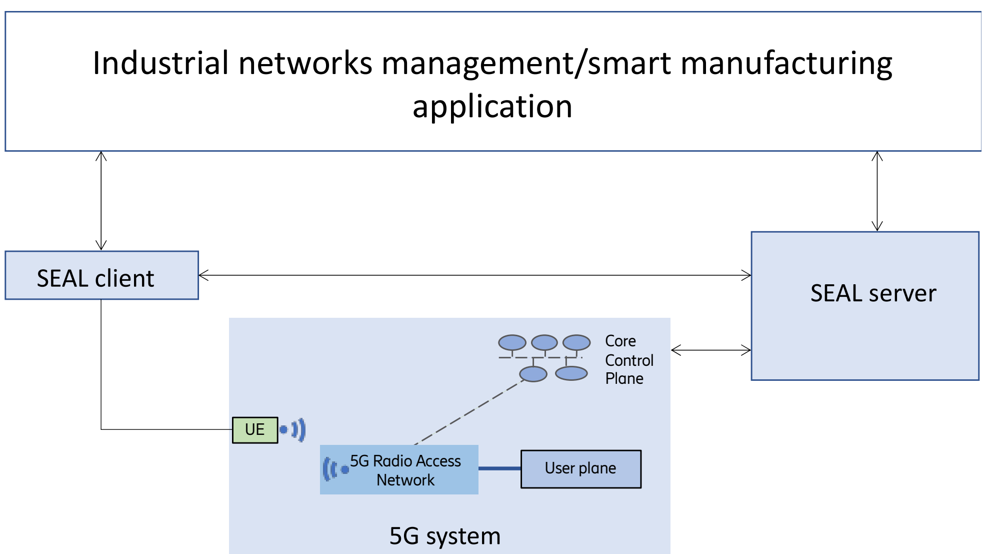

Figure 6 SEAL architecture

3.1.3 Network Exposure Function (NEF)

Compared to SEAL which is more focused on enabling enterprise friendly APIs for integration, NEF is network function defined by 3GPP with a purpose of providing high granularity detailed telecommunications APIs. Some of SEAL enablers defined above uses NEF functionality to consume 5GS capabilities. NEF is another 3GPP function which allows the API invokers (industrial application or Network Management application) to access 5G function capabilities via standardized APIs. NEF also translates information coming from the industrial application to 3GPP network function. NEF supports secure provision of the information from industrial application to 3GPP network functions. External applications can provide information about the expected behavior from the end user equipment (UE).

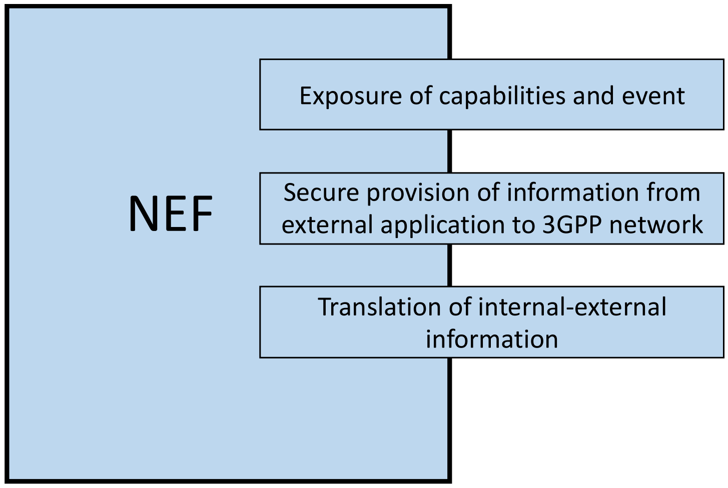

Figure 7 NEF functionality

3.2 IEEE 802.1 TSN management models

Time Sensitive Networking is a set of open standards defined by the IEEE 802.1 Time Sensitive Networking task group. TSN TG specifies new functionalities as an extension on IEEE 802.1Q standards with an aim of enabling deterministic communication services. TSN technical introduction can be found in a 5G-SMART report [5GS20-D51]. Resource management in the TSN enabled IEEE 802.1 Ethernet networks, following relevant extension of the IEEE 802.1Q

1. Stream Reservation protocol [802.1Qat][4]
2. TSN configuration [802.1Qcc][5]
3. Basic YANG [802.1cp][6]
4. YANG for LLDP [7]
5. YANG & MIB for FRER [8]

The IEEE 802.1 Qcc extension support the configuration of the TSN network's components in runtime. The concept of User to Network interface (UNI) is introduced, which allows end users to specify TSN stream requirements without knowledge of the network, thereby making the networking configuration transparent to the user.

There are three basic configuration models (Figure 8,Figure 9 and Figure 10) defined by the extension. The fully distributed model considers TSN stream requirement propagated through the network

[4] http://www.ieee802.org/1/pages/802.1at.html
[5] https://1.ieee802.org/tsn/802-1qcc/
[6] https://standards.ieee.org/standard/802_1Qcp-2018.html
[7] https://1.ieee802.org/tsn/802-1abcu/
[8] https://1.ieee802.org/tsn/802-1cbcv/

originating from the talker till the listener. Therein the UNI is between an end station and its access switch as represented in Figure 8 (solid arrow).

The centralized network/distributed user model (shown in Figure 9) considers a new network configuration entity called Centralized Network Configuration (CNC). CNC has complete knowledge of the TSN network, and it acts as the brain of the network responsible for configuring features in TSN bridges and end stations. In this model, UNI is between the end station and the TSN bridge. User/network configuration is further dissipated from neared TSN switch to CNC via the remote management protocol.

The fully centralized model (Figure 9) allows the central user configurator (CUC) entity to interact directly with the CNC via UNI interface. CUC retrieves the capabilities from the end station and configures the TSN features in the end station. Figure 11 shows the interaction between CUC and CNC. Request to joint contain talker and listener group parameters as defined in [IEEE18-8021QCC]. Response from CNC contain status group parameters. These group parameters are the collection of the TSN configuration information.

Talker group per end device contain information such Stream ID, StreamRank, End station interface, DataFrame Specification, Traffic specification, User to network requirements and interface capabilities of the end station. Lister group contains stream ID, end station interface, user to network requirement and interface capabilities of the listener end station. Further details on specific definition and attribute unit are detailed in IEEE 802.1Qcc [IEEE18-8021QCC].

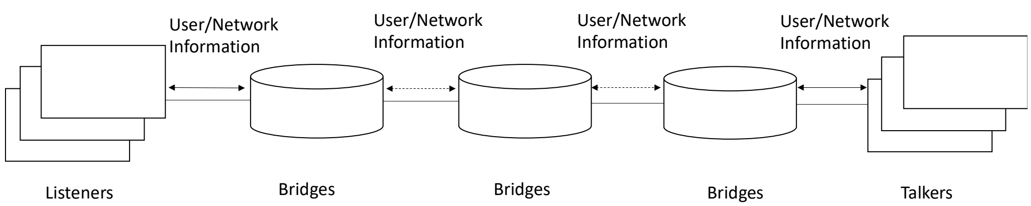

Figure 8 Fully distributed model based on IEEE 802.1Qcc[5]

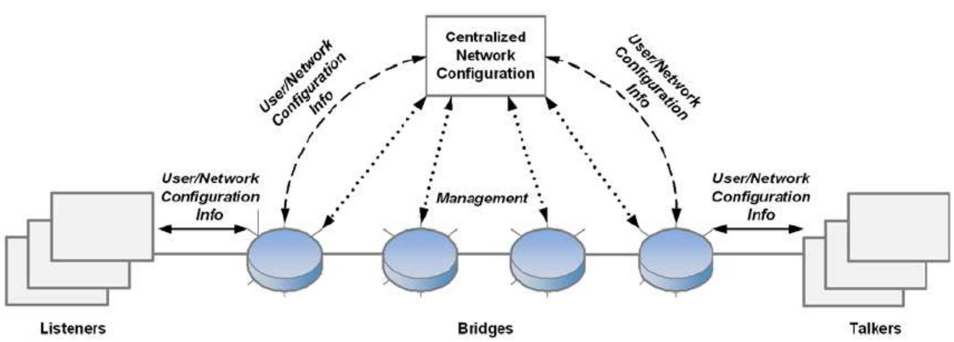

Figure 9 Centralized network/distributed user model based on IEEE 802.1Qcc[5]

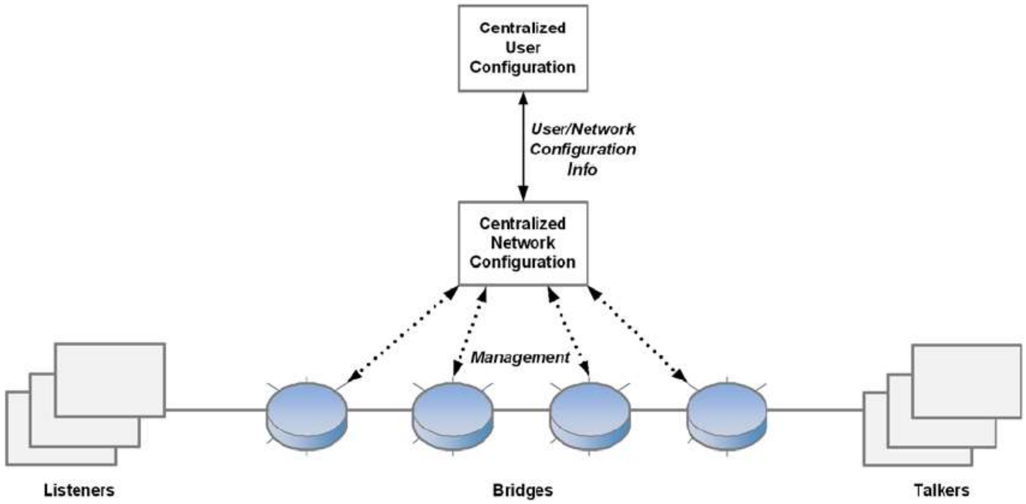

Figure 10 Fully centralized model based on IEEE 802.1Qcc[5]

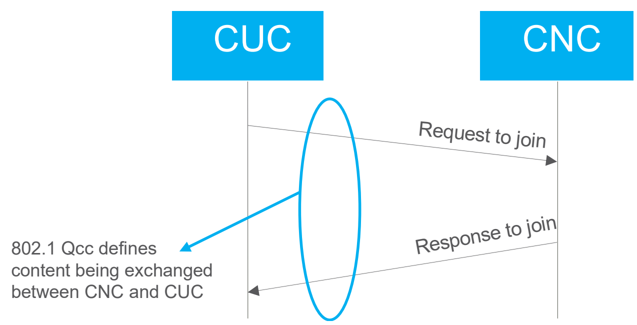

Figure 11 Interaction between CUC and CNC

Out of all the three-configuration models, the fully centralized model is the most suitable for smart manufacturing use cases. The fully centralized model works perfectly where timing and other configuration are determined by the industrial application. In the fully centralized configuration model, the following smart manufacturing relevant TSN features are configured by the CNC

1. Credit based shaper algorithm (IEEE 802.1Qav)[9]
2. Frame preemption (IEEE 802.1CB)[10]
3. Scheduled traffic (IEEE 802.1Qbv)[11]
4. Frame Replication and Elimination for reliability (FRER) (IEEE 802.1AS)[12]
5. Pre-stream Filtering and policing (PSFP)[13]

---

[9] http://www.ieee802.org/1/pages/802.1at.html
[10] https://standards.ieee.org/standard/802_1Qbu-2016.html
[11] http://www.ieee802.org/1/pages/802.1bv.html
[12] http://www.ieee802.org/1/pages/802.1as.html

CUC and CNC are the logical entities defined by the IEEE 802.1Qcc. In a practical deployment, these entities can be implemented on the same computing system. As such, the standard extension does not specify the protocol used for interaction between CUC and CNC.

The International Electrotechnical Committee (IEC) and IEEE are jointly working on the project IEC/IEEE 60802 to define TSN profile for industrial automation use cases. It is an ongoing activity which also considered the configuration and management aspect of TSN networks in industrial deployments.

3.3 5G deployment model in integrated Ethernet-based industrial networks

After the first release of the 5G standard (release 15), 3GPP started working on the 5G integration aspect with Ethernet-based industrial networks. 5GS supports Ethernet and can work with networks that are compatible with IEEE standards relevant for industrial automation (IEEE TSN). This feature of 5GS makes sure that it interworks with existing Ethernet deployment e.g., Local Area Network.

Today 5G system (5GS) supports Ethernet and is compatible with IEEE standards relevant for industrial automation (IEEE TSN). This allows seamless interworking with existing Ethernet deployments e.g., Local Area Network (LAN) integration and TSN deployment in industrial deployments.

Starting from Release 15, 5GS supports transport of the IEEE 802.3 Ethernet user plane traffic. 5GS is modeled as a virtual Ethernet Bridge and is prepared for integration with the existing industrial network management system. From the outside, 5GS can be seen as a virtual Ethernet bridge, and any network management system can interact and configure 5GS similarly as an Ethernet switch to a certain extent. In an industrial deployment, 5GS can have multiple 5G virtual Ethernet bridges, one per user plane function (UPF). 5GS also supports flooding and MAC learning as default forwarding mechanisms.

Figure 12 shows the 5G integrated Ethernet network architecture, where 5G as logical layer 2 Ethernet bridge exposes its capabilities to the existing network management system. These capabilities include bridge and port management information such Link Layer Discovery Protocol (LLDP) and Virtual LAN (VLAN) and other related IEEE 802.1Q configurations.

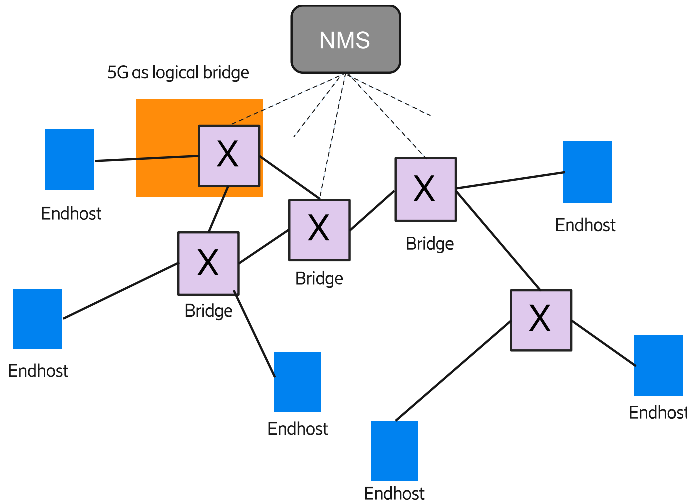

Figure 12 5G-integrated Ethernet network architecture

3.3.1 5GS modelled as virtual TSN bridge

From release 16, 5GS supports interworking with TSN-based networks. 3GPP has specified 5GS interworking through its support of the time-sensitive communication services. 5GS is modeled as TSN capable Ethernet bridge, wherein each 5GS deployment, a virtual 5G bridge can be realized per user plane function (UPF) instance. 5G core network binds the UPF instance ID (defined in TS 23.502) [TS20-23501] with bridge ID. Figure 13 shows the integration of 5GS with the TSN-based Ethernet network. The 5GS provides Ethernet ports on the mobile device sides (Device Side TSN Translator DS-TT) and the network side (Network Side TSN Translator NW-TT) as shown in Figure 13. Ethernet and TSN stream communication are possible between any two ports over 5GS, including DS-TT to DS-TT communication (i.e., UE to UE communication via UPF). 5GS also specifies TSN-AF, a control plane application function that interacts with central TSN CNC. 5G bridge properties and 5G TSN functions are configured via the TSN AF. Ethernet/TSN frames are mapped to 5G specific QoS flows based on the Priority Code Point (PCP) according to IEEE 802.1Q standard. In this way, TSN-AF triggers essential capabilities configuration within 5GS based on the information exchanged with CNC.

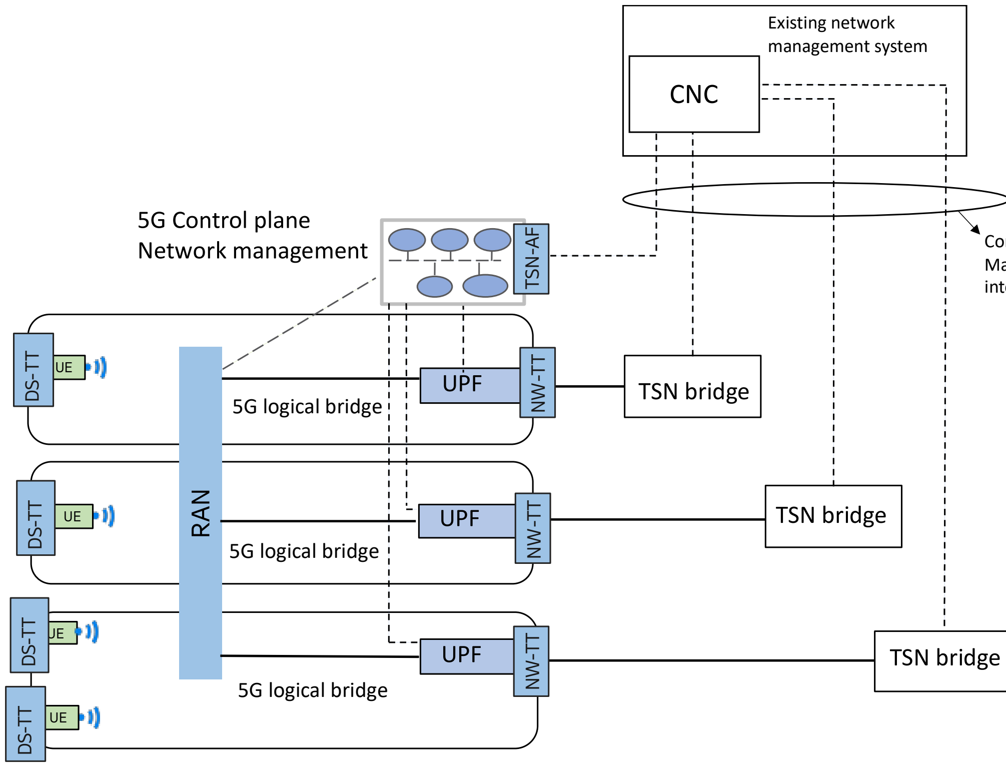

Figure 13 5G-TSN integrated deployment model

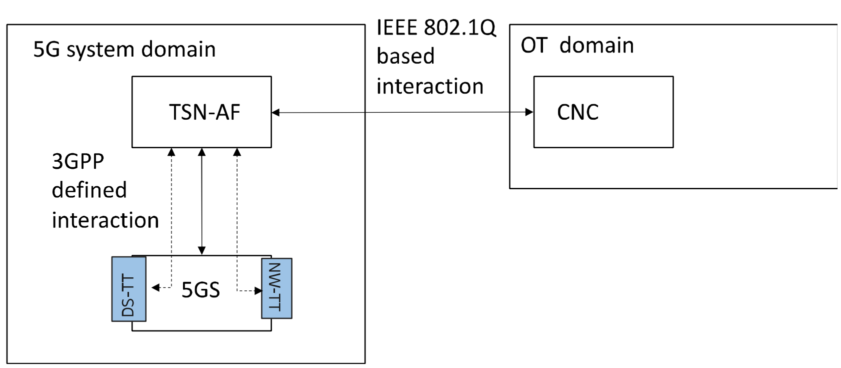

Figure 14 AF interaction with 5GS and OT domain

TSN-AF binds the 5GS bridge ID with the UPF ID, also TSN-AF stores the binding relationship information of the PDU session with related port of the DS-TT/UE side. From the TSN-AF viewpoint, there is only one NW-TT per UPF, but NW-TT can have multiple Ethernet ports used for the traffic forwarding. 5GS bridge information shared with the TSN CNC controller includes following:

1. 5GS bridge ID

2. Number of ports,
3. List of port numbers,
4. Capabilities of 5GS defined according to IEEE 802.1Qcc. These includes 5GS bridge delay per port per traffic class, including 5GS bridge delay (dependent and independent of frame size, and and their maximum and minimum values: independentDelayMax, independentDelayMin, dependentDelayMax, dependentDelayMin), their Min and Max values, ingress port number, egress port number and traffic class
5. Propagation delay per port, including transmission propagation delay, egress port number.
6. VLAN configuration information,
7. Topology of 5GS bridge as per IEEE 802.1AB,
8. Traffic classes and their priorities as per IEEE 802.1Q
9. TSN stream parameters per port as defined in IEEE 802.1Q to support PSFP.

TSN-AF is the main responsible entity in the 5GS to receive all the 5GS information and provide updates towards CNC entity. Between TSN-AF and CNC, all the port management and bridge management information are exchanged for the ports located in DS-TT or NW-TT. TSN-AF supports transfer of standardized port management information towards DS-TT and NW-TT with a port management information container (PMIC) (towards DS-TT) and bridge management information container (BMIC) (towards NW-TT). The details on the PMIC and BMIC are provided in 3GPP TS 23.501 [3GPP20-23501].

3.4 RAMI industry 4.0 AAS model

Engineering associations in Germany started in the last few years to put efforts towards developing the Reference Architecture Model for Industry 4.0 (RAMI 4.0). This effort was to ensure digitization of smart manufacturing happens with common networks and protocols, rules for cyber security, data protection, and semantics. The result was a three-dimensional, layered model of the architecture which ensured connectivity among all the components involved from E2E perspective in the digitized manufacturing eco-system [DT20-5GACIA].

With the aim to digitize all the assets within the smart manufacturing factory (asset can be physical, virtual software, intangible), RAMI 4.0 has defined an Asset Administration Shell (AAS). AAS provides a unified information framework for all the data and function mapping to a particular asset. Each asset in smart manufacturing is envisioned to have AAS as a wrapper through which all the data concerning assets can be accessed. The concept of an AAS is introduced to enable:

- Horizontal integration through value networks,
- Vertical integration, e.g., within a factory/or production shop,
- Life-cycle management, end-to-end engineering,
- Human beings orchestrating the value stream.

AAS provides access to information and functionalities through its standardized northbound interface enabling communication among different assets represented in a unified semantic representation. This information is represented in a hierarchical way using sub models. The sub models aggregate information belonging together and combine different functional aspects of an Industry 4.0 component. Sub models are linked to a use case creating a value.

The 5G system deployed in smart manufacturing can also be considered as physical and logical asset. 5G-ACIA has made the first attempt to model the 5G system AAS in the report [DT20-5GACIA]. According to 5G-ACIA report, 5G-AAS is defined for the UE as a separate physical/virtual asset and one network entity. Below is a summary of 5G-AAS.

3.4.1 5G AAS based on the 5G-ACIA report

5G Network AAS is a hierarchically structured sub model. It has a static part and a dynamic part to enable the timely update of changes of the parameter along the life cycle and to report the actual status. Throughout the lifecycle of the 5G NPN, below are the main properties within 5G network AAS that are not changed.

1. 5G NPN NW identity,
2. Network KPIs,
3. Network topology including a list of deployed network elements,
4. Radio and network capabilities (supported spectrum, transmit power, type of connections, etc.).

The UE 5G AAS sub models also contain both active and passive parts. These sub models can be read and modified by the other industrial application via message interface. The active parts also include the algorithms that enable peer-to-peer communication with other AAS.

Some properties require interactions with a variety of network functions, and other AASs in order to provide a meaningful value. Of vital importance is the list of 5G links that reflects all PDU sessions and data flows with associated QoS profiles for all 5G UE served by the respective 5G network. Via the 5G Network AAS, other AASs or industrial IoT application functions can manage the connectivity of each UE. Therefore, the attributes associated with that list of properties must also be modifiable. Managing connections is a frequent operation that applies to many UEs in the network.

4 Industrial-centric network slice management tool

The section provides details on the prototyped network slice management tool. The industrial network slice management tool (INSM) implementation is based on the 3GPP specification [3GPP20-28531]. The realized architecture supports different types of 5G-SMART use cases. Before getting into the details of the tool, first, let us define the network slicing concept.

Network slicing is the concept of 5G that enables the creation of independent instances of 5G networks within a 5G system sharing the available resources in the Radio Access, Transport, and core network functions. The industrial devices can be grouped and assigned to different network instances or slices and will be allocated different resources to isolate their traffic and might get different QoS levels compared to other slices. The network slicing can be applied to support integration with industrial networks that complies with security zones defined in IEC 62433, thus each security zone can be associated with a different network slice with dedicated network functions.

INSM is developed based on the principle of hiding the complexity of the 3GPP defined network slice configuration parameters. INSM allows an OT operator to implement network slice functionality without any 5G domain knowledge. This is realized with simplified APIs exposed by the INSM towards the industrial application domain.

Within the 5G-SMART project, INSM has been designed taking into the SEAL architecture where a RESTful interface is provided by a Network Slice Management Capability internally known as 5G Network Slice Management Service (NSMS) to an external Industrial Application Functions that can provide a graphical user interface (GUI) to the OT manager. With this GUI the operator can create groups of devices as part of a 5GLAN and create network slices to be assigned to those groups. The OT manager through that GUI would be able to define the QoS parameters in terms of bandwidth, delay to be assigned to the group of devices assigned to the network slice created. The INSM configures the slice from an E2E perspective, this means that the slice will allocate not only radio and network resources but also core network functions that will connect the selected devices with different fixed networks (existing Ethernet-based industrial networks) available in the industrial infrastructure. The other possibility to realize the interface towards INSM can be of the OT operator implementing the RESTful APIs and integrating it with existing industrial applications.

The INSM design follows the architecture defined in 3GPP TS 28.531 [3GPP20-28531] that consists of an external Application Function (AF) that is provided to the OT manager and will interact with the 5G internal Network slice capability management server (Network Slice Management Service (NSMS)). Internally, the NSMS has to deliver end-to-end resource allocation which would be managed through different vendor-specific functions provided to manage the 5GS. 3GPP has defined in TS 28.531 the concept of slice subnet which is considered a different segment of the end-to-end system e.g., RAN subnet, Transport subnet, Core Network subnet. The NSMS will interact with the different slice subnets to allocate the required resources for creating the end-to-end network slice as shown in Figure 15.

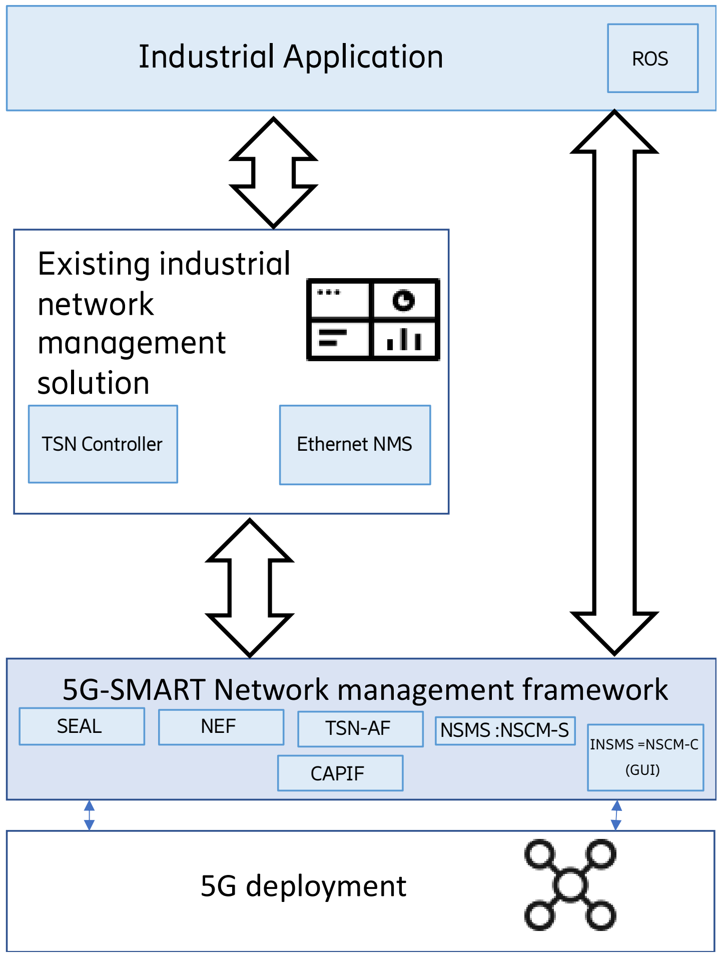

Figure 15 INSM integration with 5G-SMART network management framework

4.1 Network slice subnet modules (Functional blocks)

The network slice management system directly interacts with the industrial application in a simplified manner, i.e., INSMS that includes a GUI that hides the complexity of 5G system and allows the OT manager to easily create and assign network slices to mobile devices as part of industrial infrastructure. In addition to the INSMS the slice management system will provide 5G internal network functions (NF) that provides REST API to the INSMS for creating and managing the slices. The 5GS internal functions consist of independent modules that according to 3GPP TS 28.531 [3GPP20-28531] are subnet components that manage the RAN, Transport and 5G Core resources to be allocated when NSMS creates a new slice. These subnet modules are vendor specific to support multi-vendor 5G system and the NSMS connects to all these functions. Therefore, the NSMS will manage the RAN through the RAN-NSSMS (Network Subnet Slice Management System) to check and reserve radio resources for the network slice. The transport network resources will be managed through the TS-NSSMS (Network Subnet Slice Management System) and the NSMS will allocate core network functions for each slice with the CN-NSSMS. However, all these 5G complexity would be hidden for the OT application with the GUI for easy management of network slices.

4.2 Network slice functionality

The network slice management is available through the GUI part of the INSM shown as NSM in the figure below and includes the creation of groups under the Group section. The first step before creating a slice is to create the group of devices (which can be also mobile devices) that will be connected to the industrial infrastructure. Figure 16 displays the first step where the OT manager can access the “Group” item to visualize all the existing groups in the 5G system that can be edited, deleted or new groups can be created. Figure 17 shows that the OT manager has to select the devices to be part of 5GLAN group, which differ from normal consumer groups since in the 5GLAN group the devices might consist of routers with multiple Ethernet ports and MAC addresses.

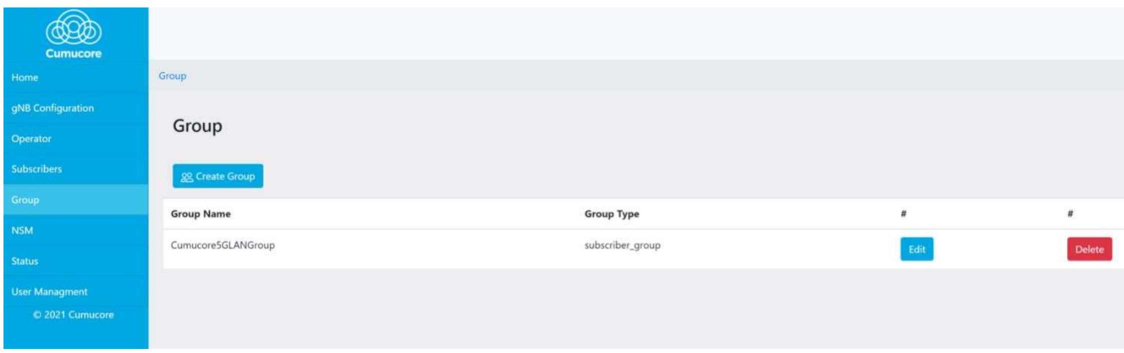

Figure 16 OT application for creating 5GLAN group

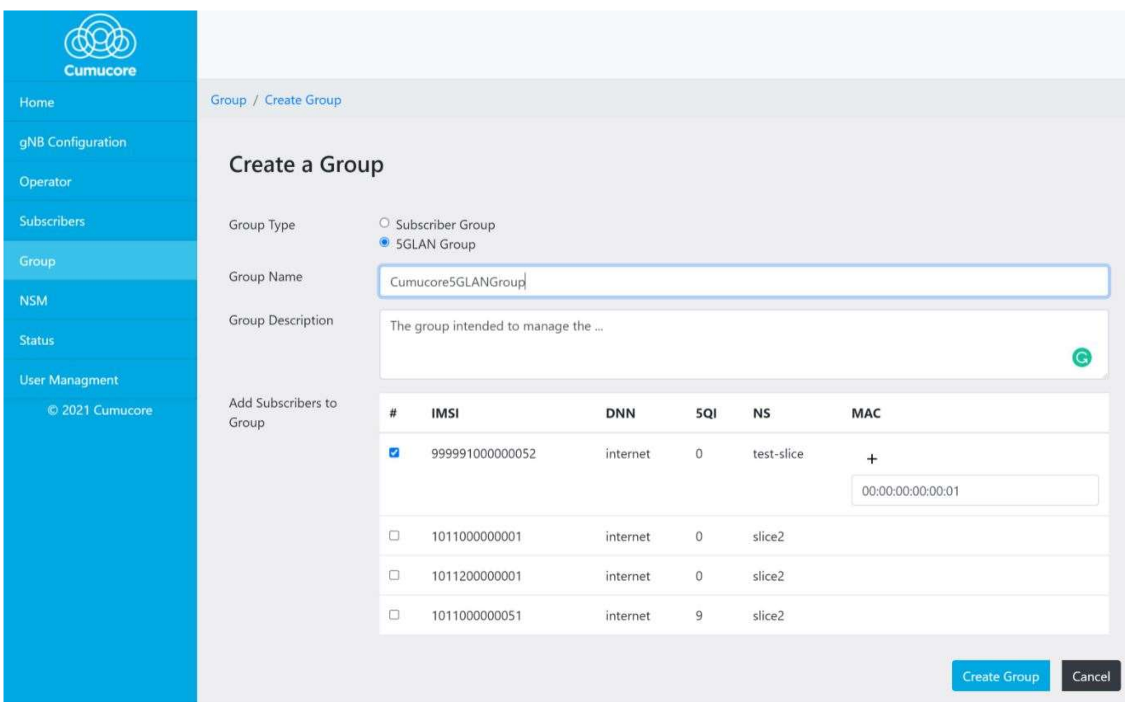

Figure 17 GUI in the OT application to create 5GLAN groups

The creation of 5GLAN group is not mandatory before creating a slice but will facilitate to assign many devices to the slice after it is created. The INSM provides the GUI to easily create network slices with a reduced set of parameters which the INSM will communicate to the NSMS internally through the subnet network functions and allocate the RAN and 5G core resources for the slice.

The OT manager can select NSM item in the GUI to visualize the network slices available or create new one as shown in Figure 18.

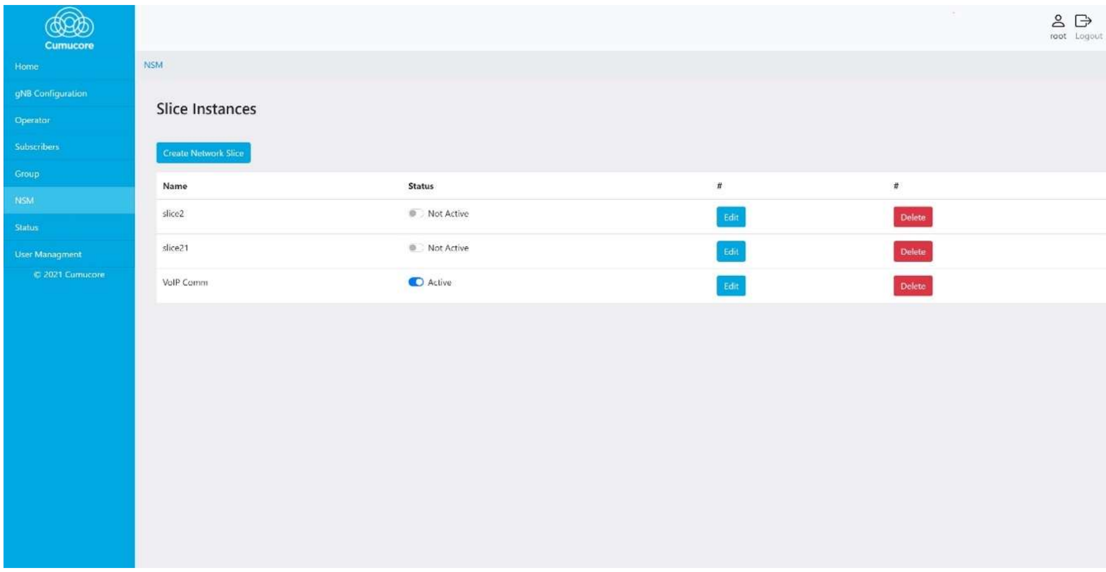

Figure 18 OT application to edit or create network slices

The OT manager selects to create a new slice and has to enter a minimum set of parameters in terms of maximum and minimum data capacity required as well as the QoS, maximum delay required by the slice and data network (i.e. Data Network Name (DNN)) that will be connected to the slice as shown in Figure 18. To support security zones each slice will be associated with different DNN that will connect the slice from the 5GS to the specific security zone in the fixed industrial network.

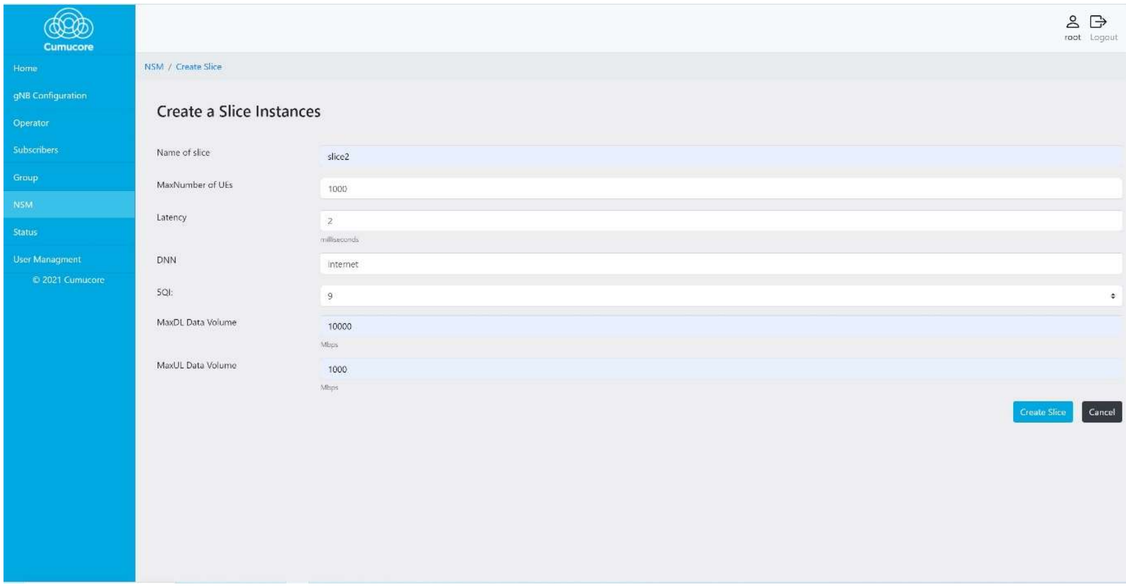

Figure 19 GUI in OT application to enter parameters for creating a slice

After the slice is created the OT manager will have to activate it by going to NSM and selecting the "Create Slice" button shown in Figure 19, which will then open the floor plan shown below for selecting the coverage area of the slice. The OT manager can also select the coverage area by selecting the base stations to be allocated for the slice (shown in Figure 20). The coverage area of selected base station will be deciding factor for coverage of selected slice.

Figure 20 OT application to select the coverage of the slice

After selecting the coverage area, the OT application will show a window where the OT manager has to select the devices to be part of the slice. At this point the devices can be selected individually or using the previously created 5GLAN groups.

4.2.1 Network slice creation and activation use case realization

The proposed architecture for managing network slices consists of the RAN-NSSMS, TS-NSSMS and CN-NSSMS modules which will implement the following functionality.

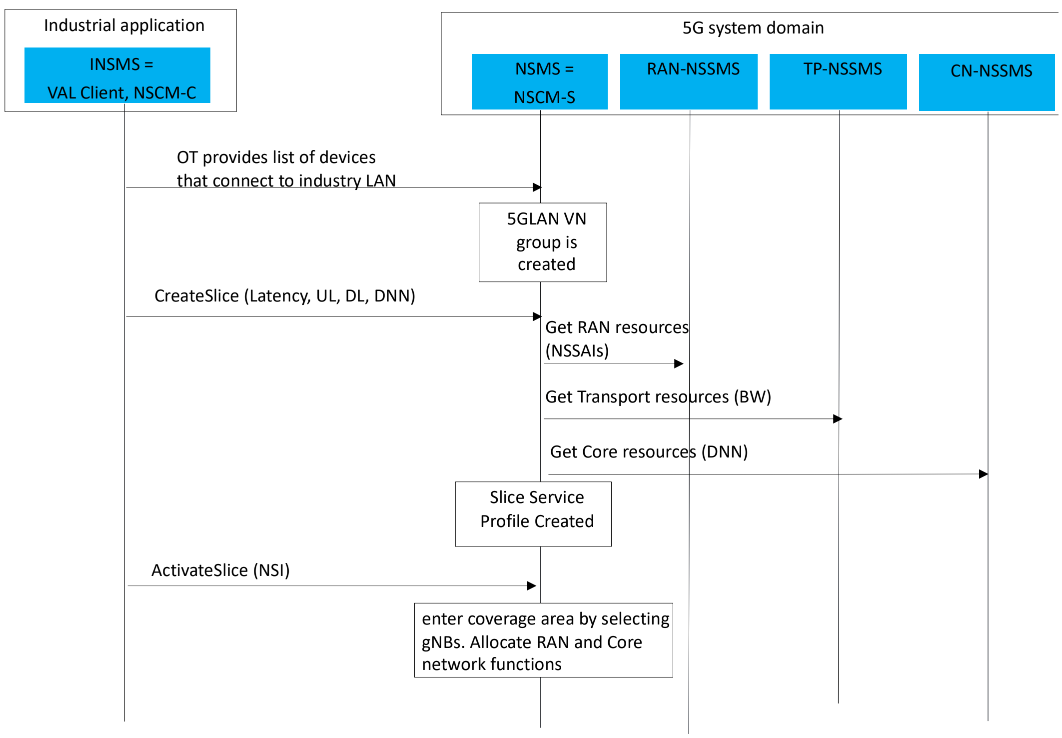

Figure 21 Sequence flow of creation of the slice and its activation

The RAN-NSSMS will collect or configure available resources on RAN subnets for creating the new slice. NSMS will interact with RAN-NSSMS which would be vendor-specific and will interact with the base stations to configure radio cells for the slice. The RAN-NSSMS will check the S-NSSAI (Single–Network Slice Selection Assistance Information) that has been configured in the gNB. The S-NSSAI is used to uniquely identify a Network Slice. The S-NSSAI contains two components: the SST (Slice/Service Type) and an optional SD (Slice Differentiator). The RAN-NSSMS will access the available information in the gNB to be selected for the network slice. The NSMS will interact with the vendor specific gNB manager to allocate the required radio resources and provide the following information to be associated with the slice to be created {gNB_ID, gNB_Name, gNB_TA, gNB_PLMN_list, gNB_NSSAI_list}.

The TS-NSSMS will check available transport capacity in the backhaul switches. The TS-NSMS might be vendor specific depending on the transport routers or switches used in the backhaul. The TS-NSSMS will interact with the NSMS to reconfigure the Transport Network to support new network slice. The NSMS sends the transport network related requirements (e.g., external connection point, latency and bandwidth) to the TN Manager which reconfigures the TN accordingly (3GPP TS 28.531, section 5.1.1) [3GPP20-28531].

The CN-NSSMS will utilize Network Function Virtualization Orchestrator (NFVO) to check available NF to be used by the network slices or the CN-NSSMS can be used also to allocate additional network functions required for the slice. The CN-NSSMS can check the available NF registered in NRF based on supported TN, DNN and available capacity. The CN-NSSMS might utilize network orchestrator based on OpenStack and Kubernetes to create new 5GC instances.

Thus, all the modules will interact with specific subnets of the end-to-end network slice to allocate the necessary resources at radio, transport, and core network. This module will interact with the NSMS which provides the endpoint to the OT application to create the network slice and associated the 5GLAN UE to the slice. Moreover, these modules will hide the vendor specific configuration tools used when deploying a multi-vendor network including components from different manufacturers. Figure 21 summarizes the complete procedure of the slice activation.

Summary of INSM implementation

The section provides details on the INSM implementation. The INSMS consists of a client module that provides the graphical interface to create and configure the network slices i.e., NSCM-C and server side i.e., NSCM-S that provides REST API to the GUI and interacts with the 5G internal network functions. The OT application can interact with the NSCM-C or even integrate the GUI provided by the NSCM-C to facilitate the network slice management functions as part of native OT modules.

Industrial applications can understand this network slice as a logical network. The industrial application does not need to handle the slice and complexity of configuring and monitoring. The proposed solution can be directly called by SEAL-enabled API. There is another possible solution enabled by SEAL architecture for dedicated network resources assignment (e.g., QoS monitoring, NRM acting as an element to control QoS as explained in section 5.3).

5 5G industrial-centric network management framework

For seamless integration of the 5G system with the existing and/or newly defined industrial communication network technologies (e.g., IEEE based TSN network), the focus on the 5G system should be on exposing its capabilities. This methodology is more feasible as OT management application does not require full knowledge of operation and management of the 5G system, rather it only needs knowledge on how to interact with the 5G management framework via standardized APIs.

This methodology is the driving mindset behind the development of the 5G industrial-centric network management framework. Figure 22 provides a view of the proposed network management framework. The proposed network management framework implements an application enablement architecture based on the CAPIF and SEAL components defined by 3GPP. The interaction on the northbound interface is via standardized API defined by 3GPP. Industrial applications such as Robot Operating System (ROS) and existing wired network management framework acts as an API invoker and can implement the API interaction with the framework. The essential building blocks of the framework are further discussed in the section below. The section provides a detailed view on the essential functionalities required for integration. This functionality can be easily triggered via standardized APIs from the OT management application. The framework is developed based on the assumption that existing OT management applications can implement the consumption of the APIs offered by the proposed network management framework.

The rest of the section describes the functional blocks of the 5G industrial-centric network management framework. Taking this functional block and its interface toward OT management application, section 5.4 provides details on how a plug and produce use case can be realized utilizing the 5G-SMART network management framework.

5.1 Functional blocks

Based on the described requirements, table 3 highlights the main functional blocks used for the 5G industrial-centric network management framework.

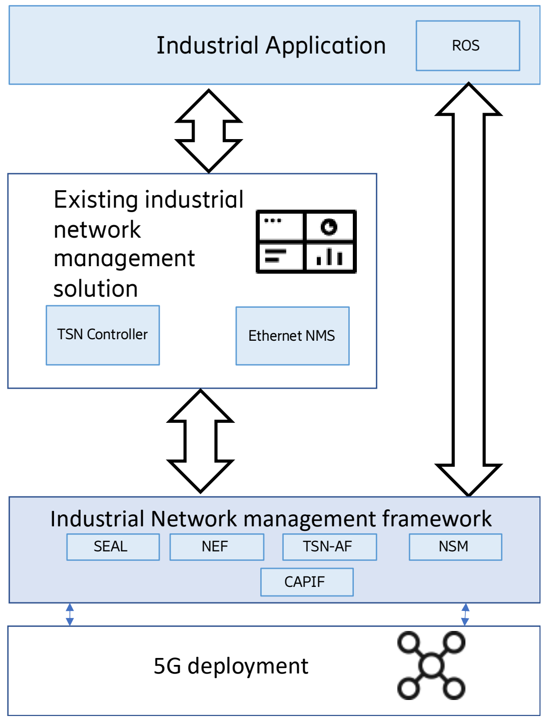

Figure 22: 5G industrial-centric network management framework architecture

Table 3: Mapping of the functional requirement to functional blocks of the 5G industrial-centric network management framework

Functional requirement	**Functional blocks of the 5G industrial-centric network management framework**
Network status, capability exposure, and interface towards Operation & Management (O&M)	SEAL application functions including device monitoring
Isolation between different network functions and its management	5G network slicing management tool (section 5), Network slice capability management
Time synchronization management	Time synchronization exposure support
Layer 2 switching/TSN management in integrated based network with 5G system	TSN application function to support integrated with centralized configuration model QoS monitoring for time sensitive communication services 5G LAN group management TSN/TSC configuration management by SEAL

5.1.1 CAPIF

CAPIF core function provides the essential functionalities for the discovery and authentication of the APIs. CAPIF API exposing function realized for the functionality would be essentially a SEAL server or optionally NEF. CAPIF also provides a mechanism to secure the communication between 5G network management framework and the industrial application. CAPIF is further explained in above section 3.1.1.

5.1.2 TSN-AF

TSN-AF as part of the 5G framework provides integration with existing Ethernet based industrial network management system. TSN-AF as explained in the section 3.3, will allow existing Ethernet network management system (e.g., CNC) to configure 5G bridges.

5.1.3 SEAL application enablement layer

SEAL is one of the essential components of the 5G industrial centric network management framework. SEAL along with application enablement server provides the essential functionalities tailored for the smart manufacturing use cases. Figure 23 shows the proposed application enablement architecture as part of the 5G industrial centric network management framework. The framework interacts with the 5GS over 3GPP defined N33, N5 interface. On the other side, it interacts with the industrial application and OT management system via harmonized API. In the case of the integrated 5G-TSN network, the TSN-AF is the main entity that interact with TSN CNC controller (as described in section 3.3).

Considering 5G connectivity native support for the industrial application, network resource management function within SEAL server interacts with CUC like industrial application. For native 5G connectivity support, 3GPP has defined 5G time sensitive communication services offered within 5G system (without integration with a TSN system) by the 5GS. Figure 24 depicts the application enablement architecture where network resource management function (NRM) residing with SEAL frameworks acts as an AF towards the 5G core network and performs the coordination of QoS flow to ensure E2E QoS requirements. NRM combines the role of the Time sensitive communication time synchronization (TSCTF) or TSN-AF and TSN CNC. This gives NRM control over the allocation of the resources of TSC communication within the boundaries of the 5G domain. Section 5.2 below provides more details on the Interface for such interactions.

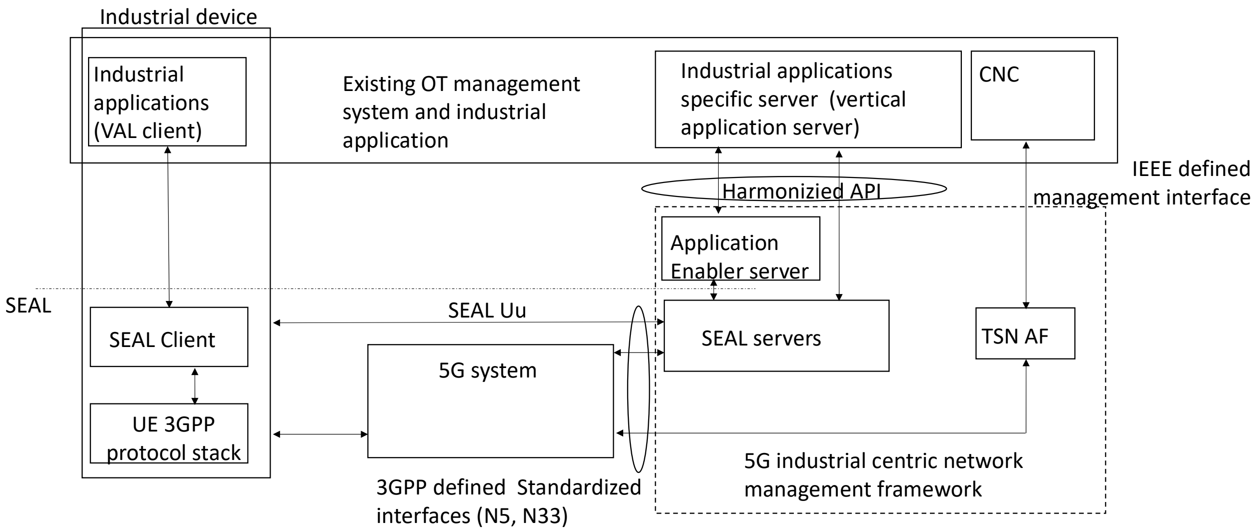

Figure 23 Application Enablement architecture for industrial-centric network management system that support 5G-TSN integrated network

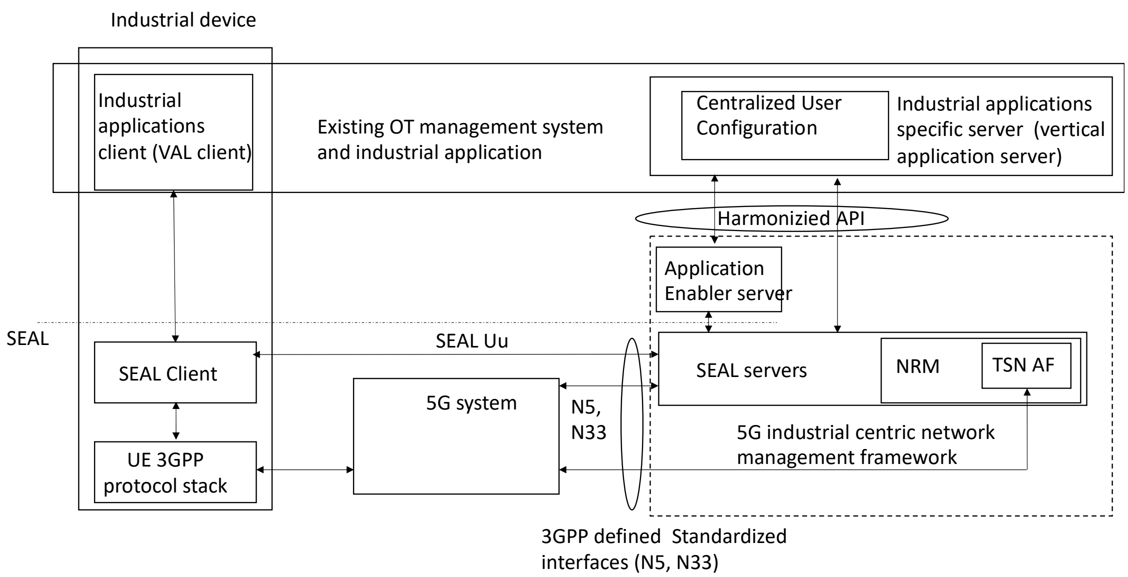

Figure 24 Application Enablement architecture for industrial-centric network management system that support native 5G TSC network

Figure 23 and Figure 24 show how the SEAL essential technical enablers (application functions) interact with 5GS and industrial application. This application function has essential functionalities proposed based on the smart manufacturing requirement including,

1. Time synchronization exposure support[14]
2. Support for Time sensitive communication services
3. QoS monitoring
4. 5GLAN group management
5. Geographic location monitoring and positioning information support
6. Device monitoring

5.2 Interaction of functional blocks within 5G network management framework

The 5G industrial centric framework builds upon the two main 3GPP components: CAPIF and SEAL. SEAL together with application enablement layer (shown in 5.1.3) enables exposure towards OT application. CAPIF API exposing function wraps around SEAL server to ensure secure communication with OT application. SEAL interacts with 5GS via N33 and N5 interface towards NEF and NSMS to retrieve requested functionality from OT application as shown in Figure 25. TSN-AF can be part of SEAL depending upon the type of Time sensitive communication (TSC) service support required.

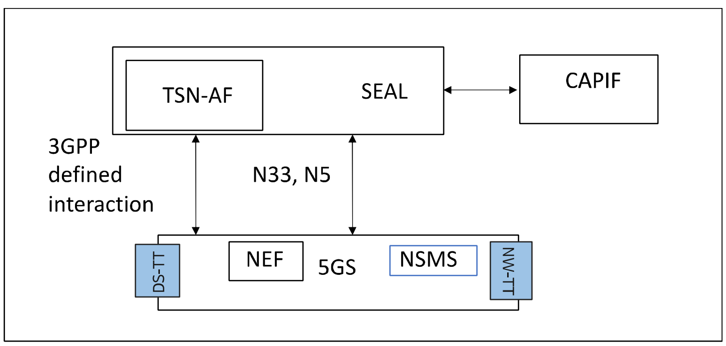

Figure 25 Interaction among the functional blocks of the network management framework

5.3 Integration with existing OT management platform and industrial applications

This section provides details on how proposed framework interact with existing Ethernet network management system and industrial applications. There are two main interfaces as shown in Figure 26 considered for integration of 5G network management framework with existing OT management system,

1. Interface a: Towards industrial network management solution
2. Interface b: Towards industrial application

[14] Planned to be included in 3GPP Release 18

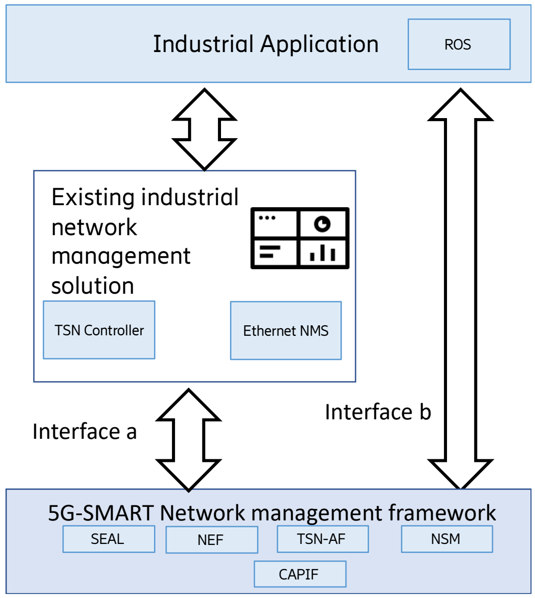

Figure 26 interface toward network management and industrial application

Interface a

5GS is integrated with Ethernet based industrial network as an Ethernet bridge as seen in section 3.3. Interface *a* between 5GS network management framework and the industrial network management is realized in similar fashion as the control plane communication between industrial network management and IEEE 802.3 based standard bridges (or TSN bridge). Interface *a* will carry all the IEEE and IETF (e.g., SNMP) specified communication between 5GS and the network management system. TSN-AF is the main entity to ensure interaction with existing industrial network management solution. Furthermore, industrial network management framework can implement API invoker to trigger API exposing functions such as SEAL or NEF (explained in section 3.1.2).

Interface b

Interface *b* is more focused towards integration of the 5G network management framework with industrial application. To realize this interface, industrial application must implement API functionality exposed by the network management framework. The exchange of the message over such interface is based on the 3GPP specification defined for the NEF and the SEAL.

Both the interface *a* and *b* can leverage the functionality of the CAPIF to enable secure communication. Below sequence diagram in Figure 27 shows how the communication channel over interface *a* and *b* is secured. The solution is based on the 3GPP specification defined for the interaction of external 3rd party application with CAPIF framework (3GPP TS 23.222 [3GPP20-23222] and TS 33.122 [3GPP20-33122]). It is assumed that the industrial application is already configured with necessary initial enrollment information towards the 5G network management framework. This includes address of the CAPIF core function, root Certification Authority (CA) certificate and onboarding credential (e.g., OAuth 2.0 access token). Based on this above information, the industrial application can establish a secure Transport Layer Security (TLS) session. Over this TLS session, industrial application onboard itself after successful validation of the security credentials. After onboarding, industrial application can discover the APIs (SEAL functions) and it establishes the TLS session for the future communication with SEAL functions.

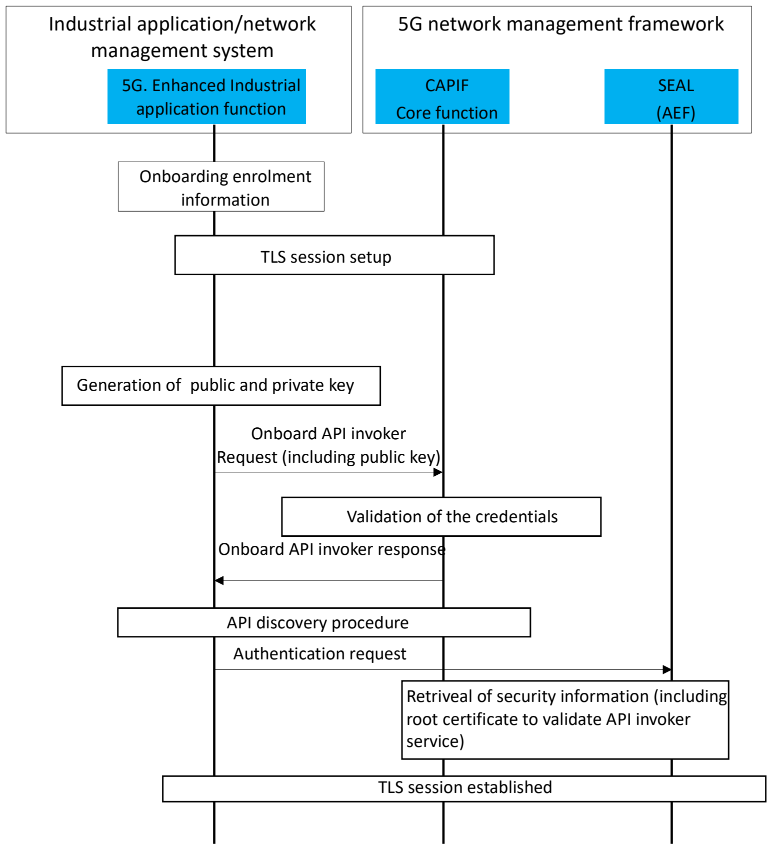

Figure 27 Procedure of securing communication between industrial application and 5G network management framework

5.4 Plug and produce use case realization

To investigate the 5G network management framework capabilities an advanced plug and produce use case is analyzed. The following steps are assumed for the use case as defined by Industry RAMI 4.0 model [PI019-I40].

1. Physical connection
   A new device is plugged into the network. In the case of the 5G network, the physical industrial device can be an embedded together with UE, which is switched on.

2. Discovery
   After physical connection, the device management server in the OT management applications need to realize the presence of the new device in the network.

3. Basic communication
   Initial communication between the device management server and the connected device is established to start the automated integration of the device.

4. Capability assessments
   The device management server residing in the OT domain evaluates the identity, functionality and requirements of the new device based on the device description received from the previous step. If the device is trusted, the integration process is continued.

5. Configuration
   The device information is integrated into the existing network system for example to allow for real-time configuration. Plant information models may need to be updated to reflect the new situation. Parameters of the device itself may be set based on the needs of the production system.

6. Integration
   Beside configuration the individual device or newly connection production module, process control system, manufacturing execution systems (MES) and enterprise resource planning (ERP) may need reconfiguration.

Considering the 5G system as integral part of the industrial communication network, based on the above steps and described capabilities of the 5G system, Figure 28 below shows how the 5G-SMART configuration framework mechanisms are mapped to the plug and produce steps. The configuration and integration steps are based on the requirement of the industrial application, which can result in various types of configurations and integration within the 5G system domain. Hence, we have divided the use case into six sub use cases based on the configuration and integration desired by the industrial application.

The sub use cases are as follows:

1. Industrial device group communication
2. 5G network slice configuration
3. Enabling end device monitoring
4. Time Sensitive Communication service configuration with TSN network
5. TSC service configuration without TSN network
6. Time synchronization service configuration
7. Robotics application (ROS) specific QoS configuration as an example for Application specific QoS configuration

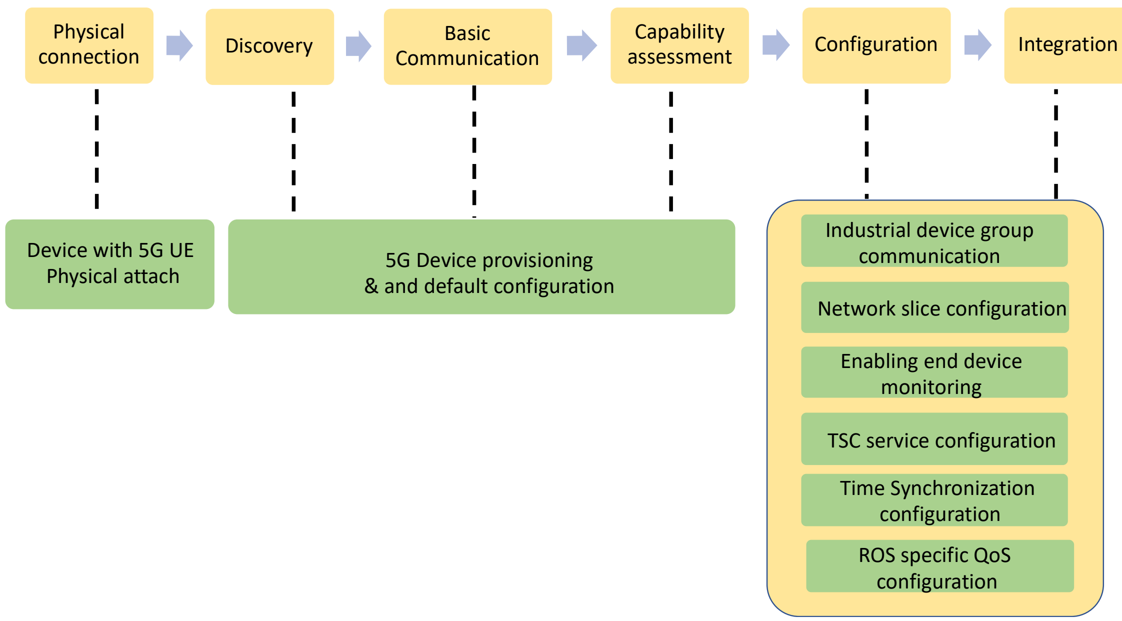

Figure 28: Mapping of the 5G configuration steps with plug and produce configuration use case

5G deployment description for plug and produce use case

The 5G NPN is operational and contains of the 5G-SMART conceptual network management framework. The network management framework is interfaced with OT management application. The OT management application implements the RESTful APIs as defined in the section 5.2. The device is preconfigured with the device manufacturing or vendor certificate (or other type of credentials). This certificate allows the device to successfully perform the identification and authentication with the 5G network. The device is also pre-configured with the non-public network (NPN) identity. The interface of the OT management toward 5G system is via Application Function. CAPIF as described in the section 3.1.1 provides the framework via which OT management application can discover, authenticate the API. OT management application includes group management server functionality and DN-AAA server for secondary authentication during PDU session establishment/modification procedure. The 5G NPN also includes a default logical network (typically for best effort connectivity) used for application-level device configuration purposes.

For all the six subcases, the first four steps of the physical connection, discovery and basic communication will be same.

1. Device provisioning and default configuration

The 5G-SMART network management framework provides a RESTful API for the OT management application to invoke device provisioning. The OT management function creates a default configuration for the new device subscription including basic IP connectivity and QoS parameters (e.g. DNN=” Factory LAN”, 5QI=9, PDU Type=IP, GPSI or SUPI, S-NSSAI). The OT management application generates the provisioning information with the default configuration which is delivered to the device (e.g., SIM or eSIM) for establishing a basic connectivity. OT management exposes this information towards 5GS via implemented SEAL APIs. When the device is turned on and successfully connected to the default logical network (DNN = "Factory LAN"). The device connectivity service in the 5G-SMART network management framework notifies the device management server that a new device is 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 new device.

2. Configuration: Industrial device group communication

The device management server residing in the OT management application set up a group of end devices. This group communication can be for example Ethernet based communication between a set of the sensors, actuator and controller connected to the same modular robot or automation cell on the factory floor.

The device management server will now trigger an API call towards the device group management service (within 5G-SMART network management framework, SEAL server) to configure the 5G LAN service. It will provide relevant attributes such as data network name, communication type (IP or Ethernet), Virtual LAN identifier (VLAN) and default QoS parameter. These attributes ensure that the authorized set of devices can connect to a 5G LAN group. This is realized by the Group creation request message according to the SEAL architecture.

The device group management service notifies the 5GS over N33 or N5 interface about the newly created 5G LAN group. 5GS in return provides the external group to the device management server. This external identifier can be further used to add new device to a 5GLAN group.

The 5G VN group information (DNN, S-NSSAI, PDU session type) is delivered to the VAL UEs belonging to the same group. The 5G VN group configuration information is delivered in the UE Route Selection Policy (USRP) from the 5GS to all VAL UEs (in the same UE group) using UE configuration update procedure.

After the 5GLAN group creation procedure is complete, the SEAL device group management service notifies the device management server. The device group management service provisions the modification and notifies the devices and the device management server that devices are added to a 5GLAN group.

3. Configuration: Time Sensitive Communication service configuration in an integrated 5G-TSN system

In an integrated 5G-TSN system, where there can be multiple TSN capable 5G bridges as described in the Section 3.3. The configuration of the 5G bridge can be done via Centralized Network Controller (CNC) entity residing in the network management system. Figure 29: Configuration of 5G-TSN system shows the sequence flow for the TSC service configuration in the 5G-TSN network. CUC residing in Industrial application provides details on the end user requirements. CNC based on this information computes the schedules and configures the path of TSN stream from talker (source) to listener (destination). CNC information includes behavior of bridges (ingress and egress port) that are on path of the TSN stream from talker to listener. Since 5GS is modelled as a TSN capable bridge, CNC considers 5GS as bridge for its configuration. Below are the sequence steps of the configuration.

1. UE establishes PDU session with the 5GS
2. TSN-AF binds the bridge ID with UPF-ID and gathers the standardized and deployment specific port management information container (PMIC) from every DS-TT attached to UEs in the network. TSN-AF also gathers all the information concerning standardized and deployment specific bridge management information container (BMIC). Standardized PMIC and BMIC are defined in 3GPP TS 23.501 [3GPP20-23501].
3. TSN-AF provides information of the 5GS bridge and its topology information according to IEEE 802.1AB.
4. CNC uses remote management protocol to read capabilities of the TSN bridges and 5G bridges.
5. CUC based on the end device and industrial application requirement signals TSN stream joint request to CNC. TSN stream joint request includes talker and listener groups of TSN stream join request. The parameters within joint request are specified according to IEEE 802.1Qcc.
6. CNC based on the physical network topology and end station address discovers the bridges (TSN and 5G bridges) that are within the path of TSN stream. Based on the MAC address and VLAN ID provided by bridges and TSN-AF, CNC creates a the TSN domain.
7. Using management of IEEE 802.1Q, CNC now configures bridges between the path from talker to listener. If the path includes 5G bridge, CNC will provide all the relevant information of the TSN features configuration to TSN-AF.
8. TSN-AF based on the received information triggers the mapping of the TSN configuration to 5G specific configuration.
9. TSN-AF further triggers the update of configuration of DS-TT and NW-TT via PMIC and BMIC.
10. CNC now provides response to CUC with all the relevant configuration for the end devices (talker and listener).

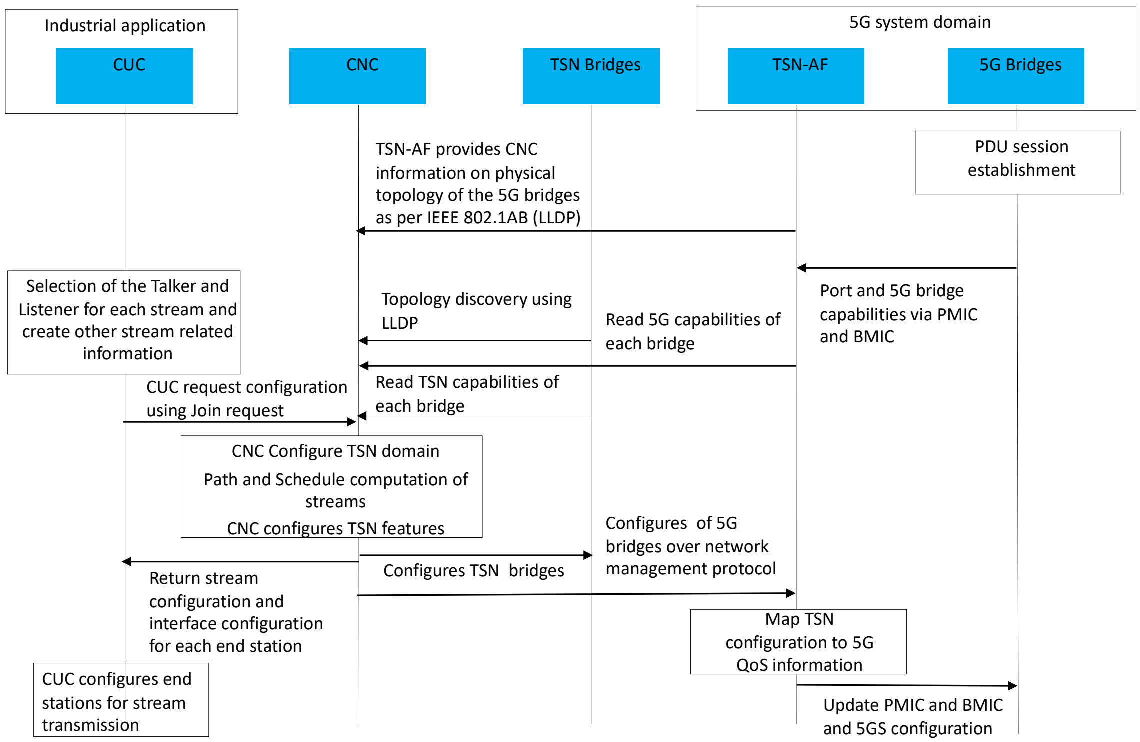

Figure 29: Configuration of 5G-TSN system

4. Configuration: Time Sensitive Communication service configuration without integration with TSN network

As indicated in the section 5.1.3, 5GS support for time sensitive communication services are not only limited to TSN integration. This means, 5GS can support time sensitive communication services for a wide range of the industrial applications where TSN integration is not realized. Other examples of such TSC support would be, 5GS enabling TSN based communication service between two DS-TT ports and without any wired network in between talker and listener. To enable configuration and interaction with industrial applications, the 5G industrial centric network management framework NRM functionality can be utilized. NRM server acts as an application function towards 5G core network and performs coordination of the QoS flows to fulfill the E2E QoS requirement of the TSC communication service. NRM combines the role of the TSN-AF and CNC. Below are the steps followed.

1. UE establishes PDU session with 5GS
2. NRM retains the PMIC and BMIC related information from the DS-TT and NW-TT and performs calculation of the bridge delay for each port pair (for UE to UE TSC flow, it will calculate ingress DS-TT port to egress DS-TT port delay).
3. Industrial application indicates the requirement of the certain QoS via stream specification identifier.
4. NRM validates the connection between UE-TSCs and calculate the latency

5. NRM based on the calculation of latency provides the response to industrial application with stream specification and list of the traffic class supported by the TSC flow.
6. Industrial application acting as CUC triggers the TSC stream create request API towards NRM server. This request includes VAL stream ID, DS-TT ports and requested traffic class
7. NRM server calculates the schedule for the VAL stream ID. Depending upon the requirements, NRM server calculates the pre-stream filtering (PSFP) used to derive the TSC QoS information and related TSC flow information. NRM provides forwarding rule used to identify the DS-TT MAC address of the PDU session.
8. NRM acting as Time Sensitive communication and Time Synchronization Function (TSCTSF) triggers policy authorization create service operation as described in 3GPP TS 23.502 [3GPP20-23501] API call for creation for setting up the uplink and downlink QoS flow. This service creation request includes DS-TT port MAC address, TSC QoS information, TSC Assistance Information, flow bit rate, Service Data Flow indicator containing flow description including Ethernet Packet Filters.
9. Within 5GS necessary network function takes care of assigning QoS flow for the PDU session for the source MAC address for the uplink direction and for the PDU session for the destination MAC address for the downlink direction.

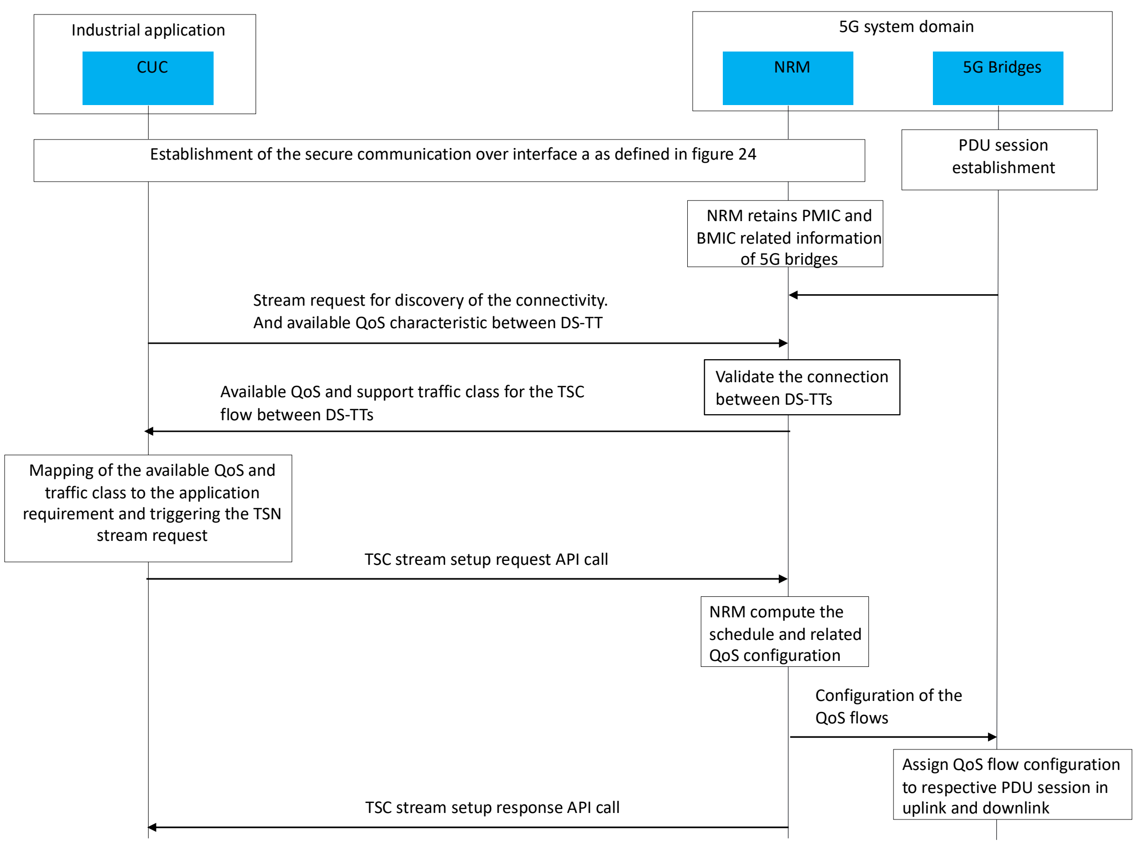

Figure 30: TSC stream setup in 5GS without TSN integration

5. Configuration: Network Slice configuration

The configuration steps are described in section 4.2.1

6. Configuration: Enabling end device monitoring

OT management application would like to monitor the status of the end device. 5G-SMART framework exposes the RESTful API that can be used to periodically or event-based monitoring of device connectivity status. The APIs provides related the information concerning the 5G device connectivity. It includes monitoring and reporting of events such as Loss of connectivity, UE reachability, location reporting, roaming status, communication failure and PDN connectivity status (defined in 3GPP TS 29.522 [3GPP21-29522]).

7. Configuration: Time synchronization management

There are several industrial use cases where time synchronization between end devices and manufacturing application is required. From the management perspective, OT management application might require the information on supported time synchronization methods by the 5GS. Specifically, OT management application may require,

1. Support for the time synchronization method,
2. Supported gPTP versions,
3. Minimum time accuracy supported,
4. Minimum gPTP or PTP message generation supported,
5. Maximum number of end device that can be supported at the minimum gPTP or PTP message rate.

5G network management framework supports such exposure of the information towards the OT management. OT management can indicate the request in API call for time synchronization capability request towards 5G-SMART network management framework. 5G server can retrieves this information from 5G network (for example by extracting UE capability information and UPF Ethernet port capabilities). Further, 5G-SMART network management framework can also allow OT management application to trigger activation, deactivation, and modification of the time synchronization mechanism for selected end device.

8. Configuration: Robotics application (ROS) specific QoS configuration

ROS is a framework used for development robotics application. It is a collection of libraries, tools and design pattern that enable productive development of software for robotic systems. ROS is not an actual operating system, but it resides on top of existing operating system such as Linux, Windows and MacOS. ROS2 applications can be based on the applications are distributed across multiple machines within a local network (LAN) based on the Ethernet and WiFi. Today, ROS application communicating over WAN is rare and multi-network configuration support in ROS is poor. Networking expertise is required to configure parameters when ROS2 applications are realized over mobile communication technology such as 5G.

Today all the ROS2 publishers and subscribers in communicating nodes have the same packet flow descriptors[15]. Since ROS release version Galactic, an application can configure unique packet flow

[15] https://docs.ros.org/en/galactic/Releases/Release-Galactic-Geochelone.html

descriptors to flows between communicating nodes. 5G network management framework allow mapping these flows to 5G Quality of Service indicators (5QI), which is further provisioned within 5GS.

6 Summary

5G integration over the north-bound interface towards manufacturing applications and the existing industrial communication systems requires an aligned configuration and network management of the 5G and non-5G components. This report describes a conceptual network management framework based on 3GPP technical features and inputs from the 5G-SMART use cases. The framework provides standardized APIs to leverage 5G infrastructure functionality (e.g., group management, location, time synchronization) with minimal efforts. The essential functional blocks of the framework are based on the 3GPP-defined CAPIF and SEAL architecture. The report further details on how 5G configuration and management functions can be realized by analyzing a plug and produce use case with different industrial configurations.

Network slicing is one of the enablers for ensuring high reliability and dedicated network resources for specific industrial applications. This report provides details on how the 5G-SMART project has prototyped the industrial network slice management function INSMS that allows in an intuitive way to create and manage network slices. The network slicing in industrial networks can ensure that a specific group of industrial end devices, i.e., 5GLAN VN get the required network resources to communicate with selected data networks. Thus, network slicing can deliver reliability and security so the network slice can connect with a DNN that can be associated to specific security zones.

7 Reference

[5GS20-D11] 5G-SMART Deliverable D1.1, "Forward looking smart manufacturing use cases, requirements and KPIs", June 2020. https://5gsmart.eu/wp-content/uploads/5G-SMART-D1.1.pdf

[3GPP20-23222] 3GPP TS 23.222, "Common API Framework for 3GPP Northbound APIs", July, 2021

[3GPP20-23501] 3GPP TS 23.501, "System Architecture for the 5G system (5GS)", March,2020.

[5GS20-D52] 5G-SMART Deliverable D5.1, "First report on 5G network architecture options and assessment", November 2020. https://5gsmart.eu/wp-content/uploads/5G-SMART-D5.2-v1.0.pdf

[IEEE18-8021QCC] IEEE, "P802.1Qcc Draft Standard for Local and metropolitan area network - Bridges and Bridged Networks - Amendment:Stream Reservation Protocol (SRP) Enhancements and Performance Improvements," IEEE, 2018.

[3GPP20-33122] 3GPP TS 33.122, "Security aspect of Common API Framework (CAPIF) for 3GPP northbound APIs", October,2020

[3GPP20-23434] 3GPP TS23.434, "Service Enabler Architecture Layer for Verticals (SEAL); Functional architecture and information flows", September 2021

[5GS20-D51] 5G-SMART Deliverable D5.1, "First report on new technological features to be supported by 5G standardization and their implementation impact", May 2020. https://5gsmart.eu/wp-content/uploads/5G-SMART-D5.1.pdf

[DT20-5GACIA] 5G-ACIA, Using Digital Twins to integrate 5G into Productions Networks, 2019, https://www.5g-acia.org/publications/

[3GPP20-28531] 3GPP TS 28.531, "Service Enabler Architecture Layer for Verticals (SEAL); Functional architecture and information flows", September, 2021

[PI019-I40] Industrie 4.0 Plug and Produce for Adaptable Factories: Example Use Case Definition, Models, and Implementation

[3GPP21-29522] 3GPP TS 29.522, "5G System; Network Function Northbound APIs; Stage 3", September 2021

Appendix

List of abbreviations

gPTP	Generalized Precision Time Protocol
AAS	Asset Administration Shell
RAMI	Reference Architecture Model for Industry 4.0
DS-TT	Device Side TSN Translator
NW-TT	Network Side TSN Translator
LLDP	Link Level Discovery Protocol
O&M	Operation and Management
LAN	Local Area Network
TSN	Time Sensitive Networking
CAPIF	Common API Framework
CNC	Centralized Network Configuration
CUC	Centralized User Configuration
UNI	User to Network Interface
VLAN	Virtual Local Area Network
MAC	Medium Access Control
UPF	User Plane Function
NEF	Network Exposure Function
NMS	Network Management System
QoS	Quality of Service
TSCTSF	Time Sensitive Communication Time Synchronization Function
TSN-AF	Time Sensitive Networking Application Function
NRM	Network Resource Management
NSMS	Network Slice Management Service
AF	Application Function
NVFO	Network Function Virtualization Orchestrator
SD	Slice Differentiator
IEC	International Electronical Committee
UPF	User Plane Function
LLDP	Link Level Discovery Protocol
PCP	Priority code point
PMIC	Port management information container
BMIC	Bridge management information container
INSM	Industrial Network Slice Management tool
GUI	Graphical User Interface
DNN	Data Network Name
NSSMS	Network Subnet Slice Management System
NVFO	Network Function Virtualization Orchestrator

NRF	Network Function Repository Function
UE	User Equipment
UNI	User Network Interface
MES	Manufacturing Execution System
ERP	Enterprise Resource Planning
PDU	Packet Data Unit
GPSI	Generic Public Subscription identifier
SUPI	Subscription Permanent Identifier
SEAL	Service Enablement Architecture Layer
LAN	Local Area Network
DS-TT	Device Side-TSN Translator
NW-TT	Network Side TSN Translator
ROS	Robot Operating System
CA	Certification Authority
TSC	Time Sensitive Communication
TLS	Transport Layer Security
NPN	Non-public network
USRP	UE Route Selection Policy

Table 4: List of abbreviations