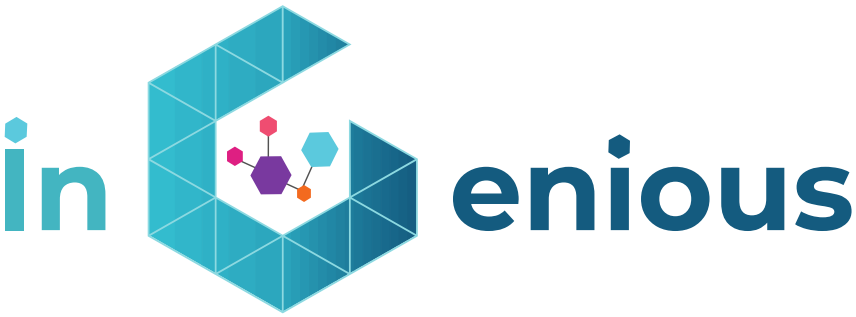
NEXT GENERATION INTERNET

Grant Agreement No.: 957216
Call: H2020-ICT-2018-2020

Topic: ICT-56-2020
Type of action: RIA



D4.3 Core network automation design for 5G-IoT

Revision: v.1.0

Work package	WP4
Task	Task 4.2
Due date	28/02/2022
Submission date	28/02/2022
Deliverable lead	CMC
Version	1.0
Authors	Jose Costa-Requena (CMC), Giacomo Bernini (NXW), Pietro Piscione (NXW), Gino Ciccone (TEI), Giuseppina Carpentieri (TEI), Anton Luca Robustelli (TEI)
Reviewers	Roberto Bomfin (TUD), Carsten Weinhold (BI), Nuria Molner (UPV)

Abstract	The automation of 5G core (5GC) installation with network orchestrator including network slicing, 5GLAN functionality and access control system based on clustering is described. This deliverable describes the integration of network slicing with 5GLAN to deliver enhanced for 5G IoT communications and preliminary results of automated deployment of the 5GC are shown.
Keywords	network orchestrator, network slicing, 5GLAN, access control, clustering

Document Revision History

Version	Date	Description of change	List of contributor(s)
V1.0	28/02/2022	EC version	See author and reviewers lists

Disclaimer

This iNGENIOUS D4.3 deliverable is not yet approved nor rejected, neither financially nor content-wise by the European Commission. The approval/rejection decision of work and resources will take place at the Mid-Term Review Meeting planned in June 2022, after the monitoring process involving experts has come to an end.

The information, documentation and figures available in this deliverable are written by the "Next-Generation IoT solutions for the universal supply chain" (iNGENIOUS) project's consortium under EC grant agreement 957216 and do not necessarily reflect the views of the European Commission.

The European Commission is not liable for any use that may be made of the information contained herein.

Copyright notice

Project co-funded by the European Commission in the H2020 Programme		
Nature of the deliverable:	**R**	
Dissemination Level		
PU	Public, fully open, e.g. web	✓
CL	Classified, information as referred to in Commission Decision 2001/844/EC	
CO	Confidential to iNGENIOUS project and Commission Services	

** R: Document, report (excluding the periodic and final reports)*

DEM: Demonstrator, pilot, prototype, plan designs

DEC: Websites, patents filing, press & media actions, videos, etc.

OTHER: Software, technical diagram, etc.

Co-funded by the Horizon 2020 Framework Programme of the European Union

Executive Summary

This deliverable describes the automation of 5G core (5GC) installation including network slicing, 5GLAN functionality and geographical anomaly detection based on clustering that can be built on top of dedicated network slices. This deliverable also describes the integration with network orchestrator for automating the deployment of the 5GC.

The first implementation of the network slicing and 5GLAN functionality has been completed and integrated with the network orchestrator for automated deployment of the 5GC. This deliverable includes the design and implementation principle of the 5GC as well as first results of the testing using network orchestrator.

The objective of 5GLAN and network slicing in 5GC consists of the isolation of IoT communications that have specific traffic requirements. The 5GLAN allows to connect both wireless and wired IoT devices as part of a Private Virtual Network (PVN) as defined in 3GPP. The network slicing creates a separate virtual network infrastructure dedicated to a group of devices. Thus, 5GLAN can be deployed on a selected slice that meets the IoT traffic requirements. Security needs to be integrated as part of IoT communications, thus anomaly detection is added to ensure security based on geographical information.

The reliability and easy deployment are important and this deliverable includes the integration of 5GC with network orchestrator to automate the deployment.

Co-funded by the Horizon 2020
Framework Programme of the European Union

Table of Contents

Co-funded by the Horizon 2020 Framework Programme of the European Union

List of figures

Co-funded by the Horizon 2020 Framework Programme of the European Union

Abbreviations

5GC	5G Core
5GS	5G System
AF	Application Function
AMF	Access and Mobility Function
DN	Data Network
DNN	Data Network Name
GPSI	General Public Subscription Identifier
INMS	Industrial Network Management System
IoT	Internet of Things
IP	Internet Protocol
MNO	Mobile Network Operator
NAT	Network Address Translator
NFE	Network Exposure Function (NEF)
NSMS	Network Slice Management System
NSSF	Network Slice Selection Function (NSSF)
NRF	Network Repository Function (NRF)
PCF	Policy Control Function (PCF)
RAN	Radio Access Network
SEAL	Service Enable Application Layer
SMF	Session Management Function (SMF)
TCP	Transmission Control Protocol
UDM	Unified Data Management
UE	User Equipment
UPF	User Plane Function

Co-funded by the Horizon 2020 Framework Programme of the European Union

1 Introduction

This deliverable has the objective of describing the technologies to automate the deployment of 5G Core network for 5G internet-of-things (IoT).

The 5G Core network is responsible for providing end-to-end data transmission by bridging different RAN to applications. Basically, the Core Network has the control over the RAN and devices by managing the traffic among the different nodes in the network.

The increase of network functions part of 5GC requires to be automated in the deployment and management. The network resource management and allocation in the network becomes more critical. Therefore, this document described the work of iNGENIOUS related to the automation of 5GC and all the required components such as network slicing and 5GLAN required to provide core functionality for IoT. These components are part of the iNGENIOUS network architecture depicted in Figure 1-1.

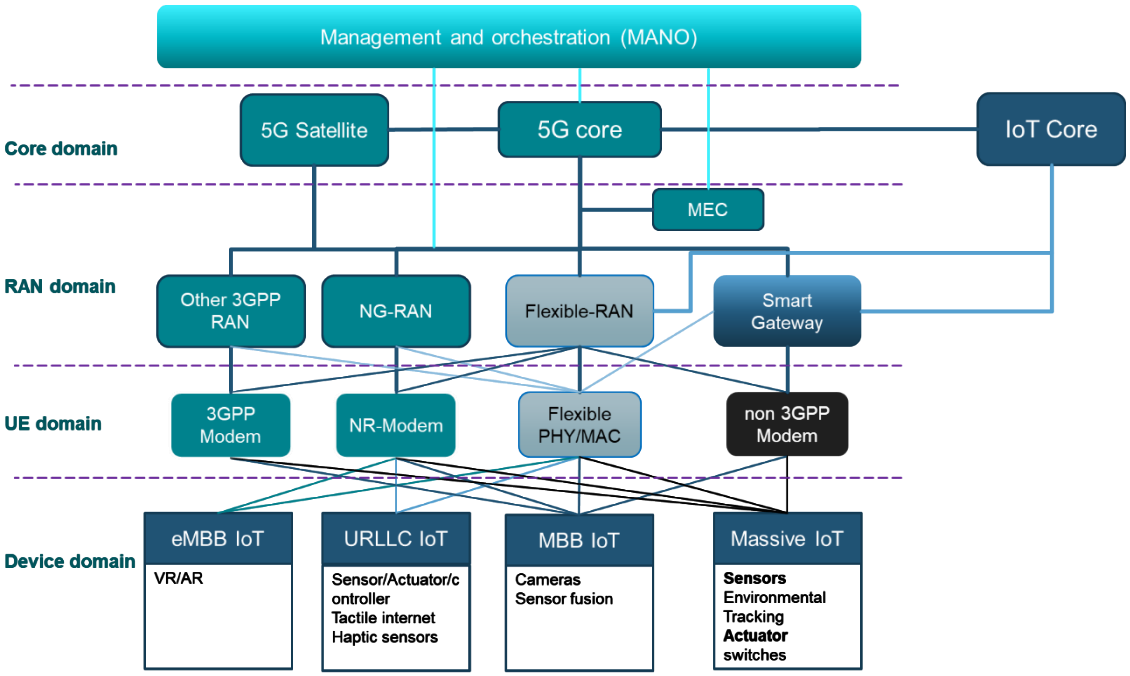


Figure 1-1: iNGENIOUS network architecture.

Lastly, this document describes the Service Based Architecture (SBA) and the components to provide network slicing, 5GLAN and TSN.

1.1 Objective of this Deliverable

This deliverable describes the design principles of 5G Core (5GC) as Service Based Architecture (SBA). This architecture allows to enhance the functionality of the 5GC by defining new network functions that automatically can be added to existing network.

Co-funded by the Horizon 2020 Framework Programme of the European Union

The first implementation of network slicing and 5GLAN is completed and this deliverable describes the modules completed as part of the implementation.

The deployment of communications infrastructure for IoT requires an orchestrator to automate the installation and management where scalability is handled properly. This deliverable presents the integration of such orchestrator with 5GC that includes all the functionality to support a scalable IoT network.

Besides the platform, the identity management of IoT devices is essential for the security of the system. Thus, an identity system is presented in the deliverable to ensure secure IoT communications.

1.2 5G Core SBA

The 5GC follows a number of principles that are mainly targeted for reaching higher flexibility, supporting many different use cases. This includes the introduction of service-based principles, where network functions provide services to each other. A clean split between control and user plane split allows independent scaling of control plane and user plane functions, and supports flexible deployments in terms of where the user plane can run (this principle was, in fact, already introduced in EPC in Release 14). The architecture allows for different network configurations in different network slices.

The 5GC control plane is based on the SBA shown in Figure 1-2. In SBA, the network functions communicate with each other via a logical communication bus and network functions can provide services to each other. A network function instance is registered to a Network Repository Function (NRF). Using the NRF, a network function instance can find other network function instances providing a certain service. The goal of such architecture is to get a higher flexibility in the overall system, and to make it easier to introduce new services.

In the 5GC, the Access and Mobility Management Function (AMF) provides the interfaces towards the Radio Access Network (RAN), the Session Management Function (SMF) keeps track of the ongoing sessions for a user, and the Unified Data Management (UDM) keeps the subscriber profiles. The User Plane Functions (UPFs) implement the user plane between the Radio Access Network (RAN) that consist of all the radio base stations and the Data Network (DN) (which can be the Internet, an operator services network or a 3rd party services network). The Network Slice Selection Function (NSSF) is used to assist slice selection. The Network Exposure Function (NEF) is mainly responsible for exposure of capabilities and events. The Policy Control Function (PCF) governs the network behavior via policy decisions. The AF (Application Function) provide a way for applications to interact with the 5GC.

Co-funded by the Horizon 2020 Framework Programme of the European Union

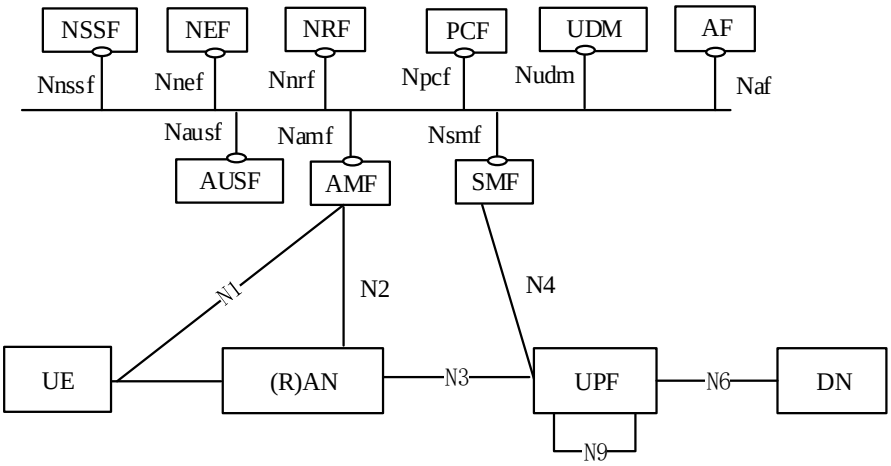


Figure 1-2: 5G Service Based Architecture.

The public mobile networks provide routing of data coming from UE to data networks that can be either public Internet or some other Data Network (DN). The mobile packet core normally assigns an IP address to the UE from own IP pool of addresses which are part of private address space. The mobile network includes a Network Address Translator (NAT) and Firewall (FW) that allows the UE can communicate with external DN such as Internet. However, the UE IP address is private and cannot be reached from external DN. Thus, when 5G has to be integrated as part of industrial or other fixed DN the UE have to be able to communicate with other devices in the fixed DN seamlessly. In order to allow this bi-directional communication between UE and wired devices, the 5GLAN feature is required.

Co-funded by the Horizon 2020
Framework Programme of the European Union

2 5GLAN

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.

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.

Further, Releases 16 and 17 introduced new NFs to support vertical specific features with the aim to simplify the implementation and deployment of 5GS in large scale vertical systems. To support seamless integration with smart manufacturing applications, 3GPP is currently finalizing the enhancement of the Service Enable Application Layer (SEAL) APIs functionality. This enhancement includes support for configuring and remapping of networking slicing based on changing requirements, geographic location and positioning information, time synchronization management, TSN integration support, QoS monitoring and 5GLAN 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 [4] provides further details on the solution. In this specification a new set of entities and terminology is defined as follows.

- 5G LAN-type service: a service over the 5G system offering private communication using IP and/or non-IP type communications.
- 5G PVN: a private virtual network capable of supporting 5G LAN-type service.

2.1 Design and implementation 5GLAN

The main feature of deploying a 5GLAN for IOT and industrial infrastructure is that any UE i.e. IOT device can communicate with any other UE that is a member of the 5G PVN from anywhere there is 5G service. Therefore, a 5G LAN-type service shall provide a mechanism for an authorized 5G PVN administrator to enable or disable a UE from accessing the 5G PVN. The 5G network shall enable the Mobile Network Operator (MNO) to remove a UE from a specific group of UEs of a private group communication.

Security is an important requirement so a 5G LAN-type service shall provide a mechanism to identify an authorized UE. Thus, the 5G network shall support a restricted set of UEs to communicate privately amongst each other even if these UEs are subscribers to different MNOs. Moreover, the 5GLAN should ensure that UEs that belong to a different private group cannot send data to any or all of the UEs in the group.

Co-funded by the Horizon 2020 Framework Programme of the European Union

If UE1 wants to establish private data communication with UE2, it sends a request to the 3GPP network for an on-demand private data communication connection to UE1. UE-A can also indicate what type of data communication it wants (e.g., IP, Ethernet or other) since the objective is that both devices connect through the 5GS as if they were physically connected with fixed link. The 5GLAN network shall enable the point-to-point addressing as well as multicast addressing between the different UEs in a private group. It is assumed that all UEs in a same private group use the same type of addresses (e.g., IP, Ethernet or other).

The wireless IoT and wired industrial devices communicate using standard Ethernet then 5G network shall support the routing of non-IP packet (e.g., Ethernet frame). Thus, to provide seamless end to end private communication between wireless and wired industrial devices 5GLAN is required.

There is huge variety of devices each with different traffic requirements when considering the integration of a 5G network with fixed infrastructure. Thus, in order to accommodate different type of devices the 5G network shall be able to provide the required QoS (e.g., reliability, latency, and bandwidth) for non-IP packet (e.g. Ethernet frame) for private communication between UEs

5GLAN supports the fast routing, broadcast virtual LANs, and Ethernet QoS classification. Ethernet frames are transported by the 5G network and routed to the correct destination 5G UE before being unpacked and forwarded to the correct Ethernet switch/device. The 5GLAN system must support the routing functionality based on Ethernet frame header information. The communications between UE and fixed devices must support Ethernet broadcast frames. Routing of Ethernet frames in the 5G system must be based on the spanning tree algorithm run by the Ethernet network being served

Finally, the 5G network should provide easy to manage interface for industrial OT operations. The 5G system shall enable the OT network operator to create, manage, and remove private groups including their related functionality (subscription data, routing and addressing functionality).

The 5GLAN administrator goes to the operator's portal and makes a request for 5G LAN-type service. The request includes the GPSI (General Public Subscription Identifier) or SUPI (Subscriber Permanent Identity) of all UEs that are supposed to use this 5G LAN-type service for private communication and the type of communication (IP or Ethernet). In addition, the 5GLAN administrator may indicate any of the following additional information: requested QoS, IPv4 or IPv6 communication, static or dynamic IP address, additional IP services (e.g., DNS, Dynamic DNS, DHCP, IMS, egress to Internet), additional Ethernet services (e.g., multiple IEEE 802.1Q VLANs).

A Private DNN uniquely identifies a 5GLAN group and all the member UEs of the same group need to establish a PDU Session towards the same Private DNN for 5GLAN group communication. Reserved special labels in the DNN syntax can easily indicate whether it's a Private DNN. Private DNNs might be preconfigured in the network and the group member UEs. They may also be dynamically created on demand by the operator or the group owners/administrators, as part of the 5GLAN group creation. When a new Private DNN is created on, the information may be propagated into the concerned network entities (e.g., AMF, SMF, UDR, etc.) in the core network and

Co-funded by the Horizon 2020 Framework Programme of the European Union

group member UEs may receive the Private DNN information, together with the related configurations such as the Service Area configuration, via signalling procedures (e.g., Registration or UE Configuration Update).

A 5GLAN group member UE establishes a dedicated PDU Session towards the target Private Data Network Name (DNN) before it can communicate with the group. The legacy Packet Data Unit (PDU) Session management procedures can be reused for group communication. According to the Private DNN, the network selects the appropriate network functions (e.g., SMFs and UPFs) for the UEs of the same group. For example, all the UEs of the same group and in the same local area may be assigned the same SMF and UPF.

2.1.1 5GLAN DESIGN AND IMPLEMENTATION

This section describes the design and implementation of 5GLAN for IoT communications. The process for assigning 5G devices to be part of the 5GLAN virtual network consist of the following process.

During the PDU Session Establishment procedure, the SMF retrieves SM subscription data related to 5GLAN type service from the UDM as part of the UE subscription data for the DNN and S-NSSAI.

A NEF may also support a 5GLAN Group Management Function: The 5GLAN Group Management Function in the NEF may store the 5GLAN group information in the UDR via UDM as described in TS 23.502.

UDR will store application data (including Packet Flow Descriptions (PFDs) for application detection, AF request information for multiple UEs, 5GLAN group information for 5GLAN management). Storage and retrieval of NF Group ID corresponding to subscriber identifier (e.g., IMPI, IMPU, SUPI).

2.1.2 5GLAN ARCHITECTURE 23.502

The information of 5G VN group is provided by the AF to the NEF and is stored in the UDR, by using the NEF service operations information flow procedure
The SMF shall create a group-level N4 session on the UPF for a 5G VN group when N19-based forwarding is applied. The group-level N4 Session management procedures enable the SMF to create, update or delete the group-level N4 Session, e.g., add or delete N4 rules, allocate or release the N19 tunnel resources.

2.1.3 UPF FUNCTIONALITY

The design of the User plane function (UPF) includes the following functionality in order to support the 5GLAN feature, ARP Proxy, VLAN handler and LLDP responder as depicted in Figure 2-1.

Co-funded by the Horizon 2020 Framework Programme of the European Union

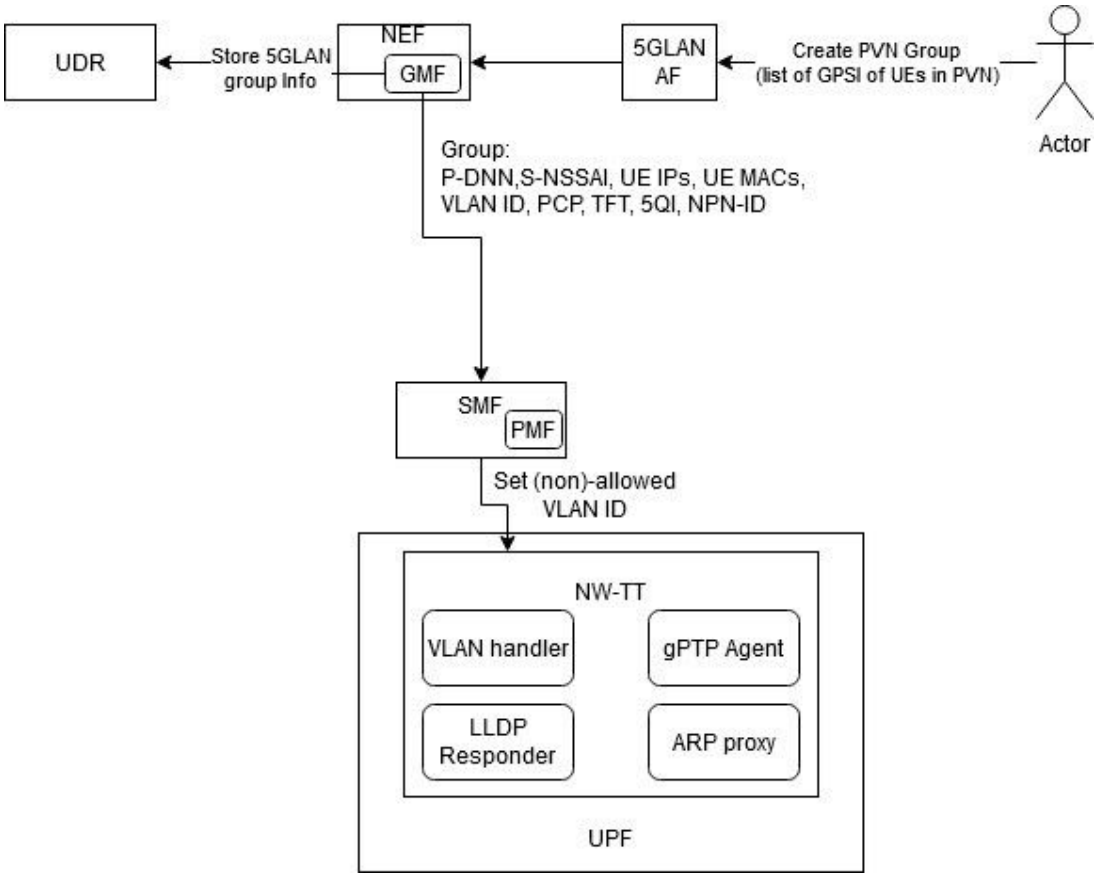


Figure 2-1: UPF architecture with modules to implement 5GLAN functionality.

ARP Proxy

This module has to respond to Address Resolution Protocol (ARP) requests and / or IPv6 Neighbour Solicitation requests based on local cache information for the Ethernet PDUs. The UPF responds to the ARP and / or the IPv6 Neighbour Solicitation Request by providing the MAC address corresponding to the IP address sent in the request.

VLAN handler

The SMF may receive a list of allowed VLAN tags from Data Network Authentication Authorization Accounting (DN-AAA) (for a maximum of 16 VLAN tags) or may be locally configured with allowed VLAN tags values. The SMF will set the policies in the UPF with instructions on VLAN handling (e.g., the VLAN tag to be inserted or removed, S-TAG to be inserted or removed). Taking this into account, the SMF determines the VLAN handling for the PDU Session and instructs the UPF to accept or discard the UE traffic based on the allowed VLAN tags, as well as to add/remove VLAN tags. Packet routing and forwarding support the Uplink classifier to route traffic flows to an instance of the data network, as well as support the branching point to hold multi-homed PDU session, and support traffic forwarding within a 5G group (UPF local switching, via N6 or via N19).

LLDP responder

5GLAN module should support link layer connectivity discovery and reporting on behalf of the devices connected to the UE. The 5GLAN should perform link

Co-funded by the Horizon 2020 Framework Programme of the European Union

layer connectivity discovery and reporting as defined in IEEE Std 802.1AB for discovery of Ethernet devices attached to the UE device. If 5GLAN has to performs link layer connectivity discovery and reporting on behalf of the devices connected to the UE, it is assumed that LLDP frames are transmitted between UPF and UE on the QoS Flow with the default QoS rule. Alternatively, SMF can establish a dedicated QoS Flow matching on the Ethertype defined for LLDP (IEEE Std 802.1AB).

2.2 Relation to UCs

As described in this section 5GLAN allows to create Private Virtual networks that connect 5G UE with fixed devices. This facilitates direct and secure communication within group of wired and wireless devices. Thus, 5GLAN can be applied to the use cases that require secure communication within reduced group of devices and is built on top of network slicing. Therefore, 5GLAN is relevant for following use cases.

- Automated robots with heterogeneous networks - Factory UC
- Transportation platforms health monitoring - Transport UC
- Situational understanding and predictive models in smart logistics scenarios - Port Entrance UC
- Improved driver's safety with mixed reality and haptic solutions - AGVs UC
- Inter-modal asset tracking via IoT and satellite - Ship UC

Co-funded by the Horizon 2020 Framework Programme of the European Union

3 Network Slicing for IoT Applications

The deployment of IoT devices in mobile networks has increased rapidly and it cannot be predicted how much of traffic they will generate. Moreover, the IoT traffic has different pattern compared to consumer data. Thus, in order to ensure that the IoT traffic is managed efficiently the network slicing functionality defined in 5G would be the right tool. The possibility of creating a virtual network on top of the physical infrastructure allows to assign different resources and to isolate the IoT traffic in a separate network slice.

3.1 Network Slicing Introduction

An introduction of network slicing is defined in GSMA [1]. Itconsist of the separation of radio, network, transport, and computing resources to provide individual virtual networks on top of same physical network infrastructure.

From a mobile operator's point of view, a network slice is an independent end-to-end logical network that runs on a shared physical infrastructure, capable of providing a negotiated service quality. The technology enabling network slicing is transparent to devices and end users.

A network slice could span across multiple parts of the network (e.g., terminal, access network, core network and transport network) and could also be deployed across multiple operators. A network slice comprises dedicated and/or shared resources, for example in terms of processing power, storage, and bandwidth and has isolation from the other network slices. The Next Generation Mobile Networks (NGMN) alliance also refers to network slice concept as follows [2]. "A network slice instance may be fully or partly, logically and/or physically, isolated from another network slice instance".

The network slicing has been defined part of 5G architecture in 3GPP [2]. A network slice is considered a logical end-to-end network that can be allocated to several User Equipment (UE) and it can be dynamically created and modified. A network slice is defined within a PLMN and shall include: the Core Network Control Plane and User Plane Network Functions and the NG RAN. A UE may have access to multiple slices that are linked to a Public Land Mobile Network (PLMN) where each UE is registered. The slices are associated to given Service-level Agreement (SLA) based on bit rate, latency, and packet loss.

Each slice is identified by a Single Network Slice Selection Assistance Information (S-NSSAI). 3GPP has defined eight S-NSSAIs in the NSSAI which is the group of S-NSSAI that is sent between the UE and the network during the registration and signalling procedure. The UE provides the network the NSSAI which then must allocate the required resources at radio, network, and mobile core network functions.

The S-NSSAI consists of following elements:

- A Slice/Service type (SST), defining the requirements in terms of features and services associated to the network slice.

Co-funded by the Horizon 2020 Framework Programme of the European Union

- A Slice Differentiator (SD), which is optional and provides additional information to differentiate each slice amongst multiple slices with the same SST to for example isolate traffic to different services into different slices.

In the first 3GPP release 16 the following basic slice IDs have been identified:

Table 1. 3GPP defined slice types.

Slice/Service type	SST value	Characteristics
eMBB (enhanced Mobile Broadband)	1	Slice suitable for the handling of 5G enhanced Mobile broadband, used for general consumer space mobile broadband applications including streaming of high quality video, fast large file transfers etc.
URLLC (ultra-Reliable Low Latency Communications)	2	Slice suitable for the handling high demand low latency communications.
MIoT (Massive IoT)	3	Slice suitable for the handling large amount of IoT devices.

3.2 Design of Network Slicing for IoT

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

With network slicing 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.

The INSM tool is developed based on the principle of hiding the complexity of the 3GPP defined network slice configuration parameters. INSM allows an Over the Top (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 INGENIOUS project, INSM tool has been designed taking into the 3GPP Rel 17 Service Enabler Architecture Layer (SEAL) architecture where a RESTful interface is provided by a Network Slice Management Capability internally known as 5G Network Slice Management Service (NSMS) to external

Co-funded by the Horizon 2020 Framework Programme of the European Union

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 is able to define the QoS parameters in terms of bandwidth, and maximum delay for the group of devices assigned to the network slice created. The INSM configures the slice from an E2E perspective, meaning 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 industrial application that implements the RESTful APIs and integrating it with existing industrial applications.

The INSM design considered in INGENIOUS follows the architecture defined in 3GPP TS 28.531 [3] that consists of an external industrial AF that is provided to the OT manager and will interact with the INSMS that will utilize the NSMS, which interacts directly with the 5G internal network functions as shown in Figure 3-1.

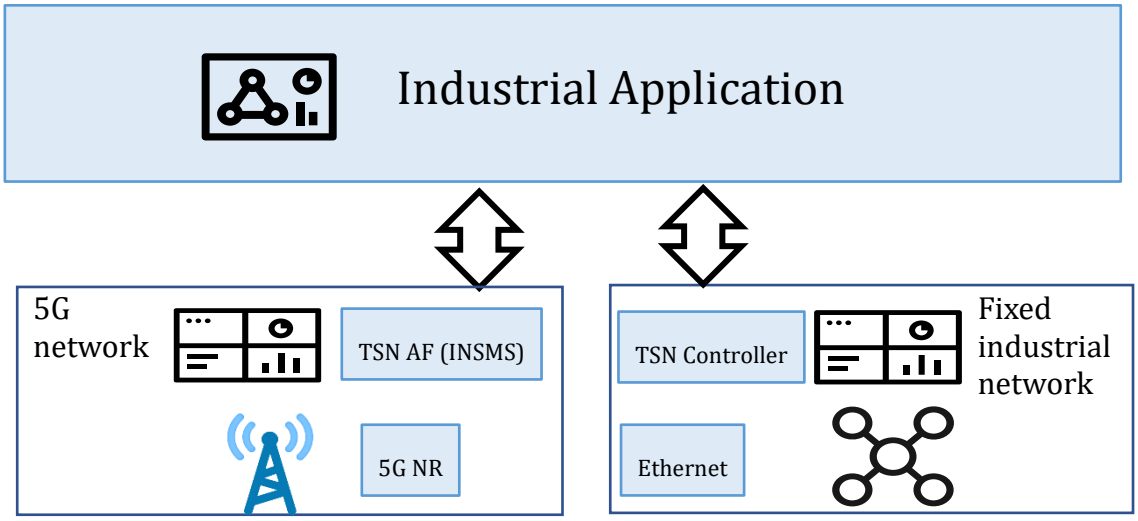


Figure 3-1: INSM integration with INGENIOUS network management framework.

Internally, the NSMS has to deliver end-to-end resource allocation which has to be managed through different vendor-specific functions managing the internal functions of the 5GS. 3GPP has defined in TS 28.531 the concept of slice subnet which is considered a different subsection or subnet of the end-to-end system or network. There are defined three subsections which are RAN subnet, Transport subnet, Core Network subnet. Each subnet is managed using a different module and the NSMS will interact with the different modules managing each subnet to allocate the required resources for creating the end-to-end network slice as shown in Figure 3-2. The INSMS can be considered in this figure as the external AF that includes a GUI for creating and managing the slices.

Co-funded by the Horizon 2020 Framework Programme of the European Union

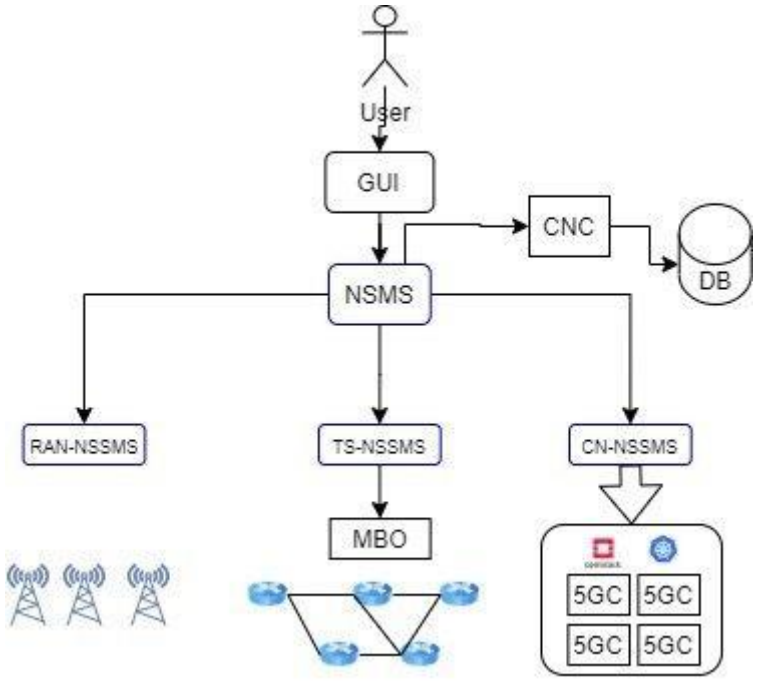


Figure 3-2: 3GPP architecture 28.531 to create end to end slice resources.

3.3 Network slice subnet modules

The INSMS directly interacts with the upper layer industrial application or the INSMS can include 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 NSMS interacts with the 5G internal NFs that provide 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 [3] are subnet components that manage the RAN, Transport and 5G Core resources to be allocated when INMS request from the NSMS to create 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 (RAN 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 (Transport Network Subnet Slice Management System) and the NSMS will allocate core network functions for each slice with the CN-NSSMS (Core Network, Network Subnet Slice Management System). However, all these 5G complexity is hidden for the OT application with the GUI for easy management of network slices.

3.3.1 DESIGN AND IMPLEMENTATION NETWORK SLICING

In this subsection we describe the design and implementation of network slicing for iNGENIOUS in the context of IoT applications. 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 3-3 displays the first step where the OT manager can

Co-funded by the Horizon 2020 Framework Programme of the European Union

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.

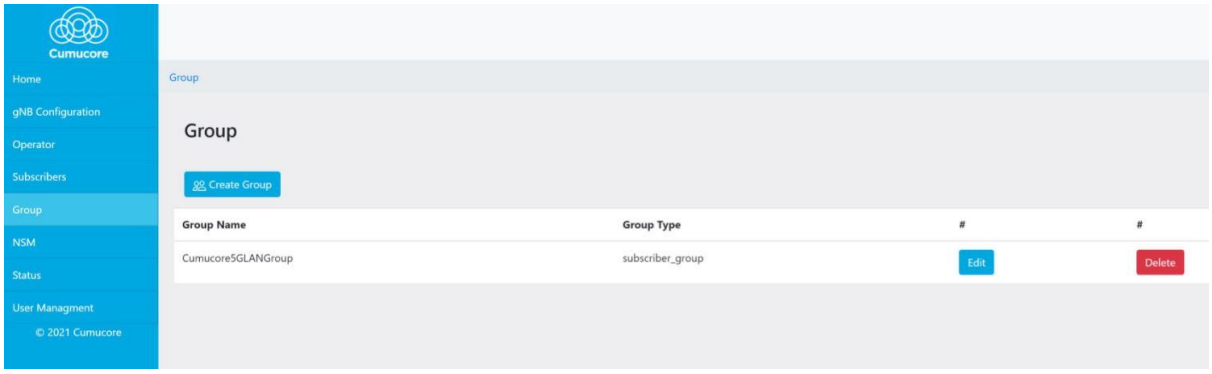


Figure 3-3: OT application for creating 5GLAN group.

Figure 3-4 shows that the OT manager has to select the devices to be part of 5GLAN group.

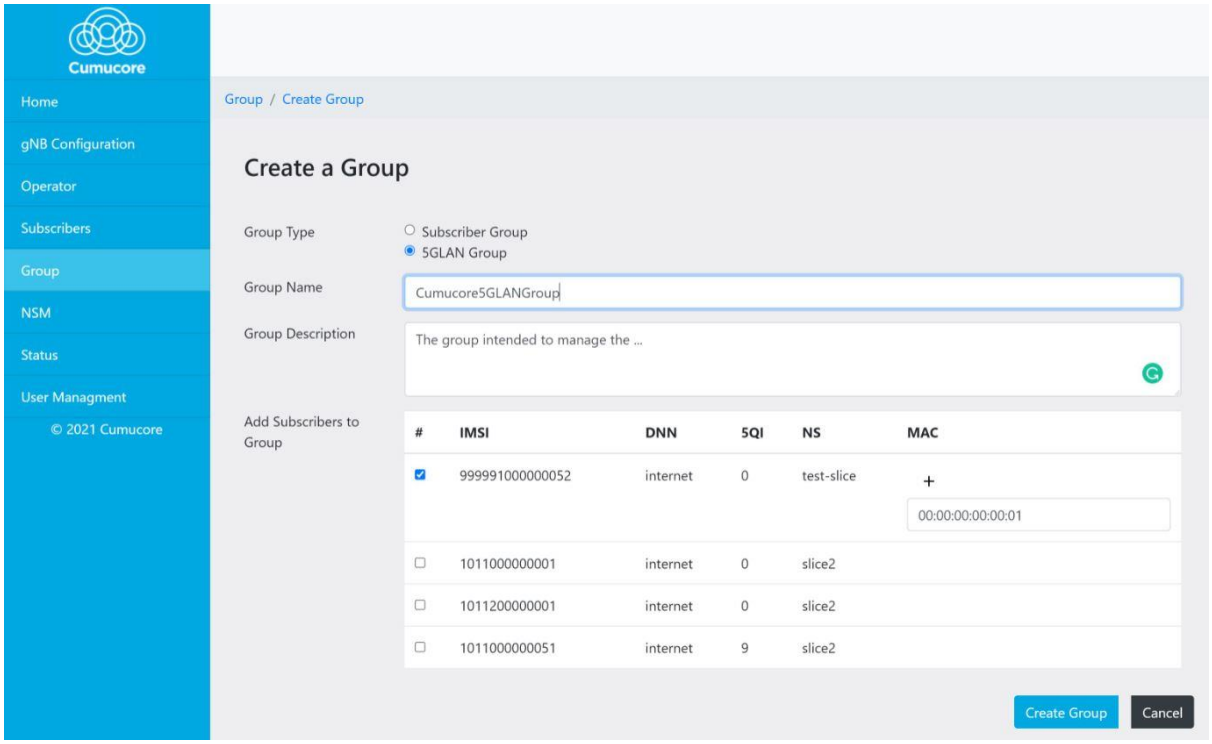


Figure 3-4: GUI in the OT application to create 5GLAN groups.

The creation of 5GLAN group is not mandatory before creating a slice and 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 menu in the GUI to visualize the network slices available or create new one as shown in Figure 3-5.

Co-funded by the Horizon 2020 Framework Programme of the European Union

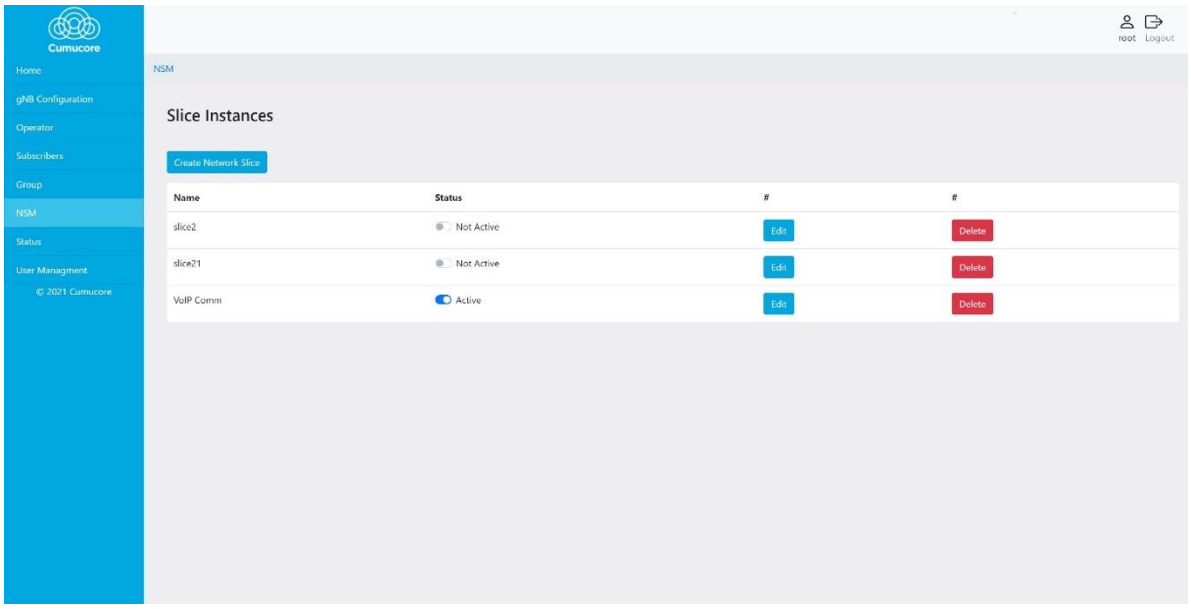


Figure 3-5: OT application to edit or create network slices.

The OT manager selects “Create Network Slice” 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 3-6. In order 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.

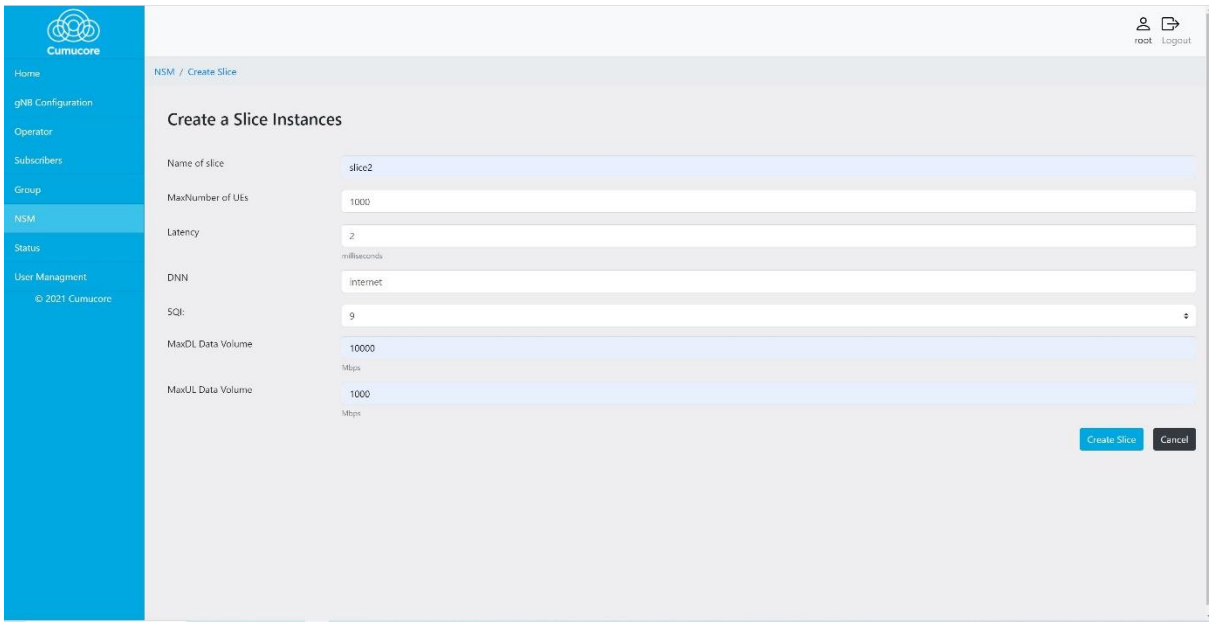


Figure 3-6: GUI in OT application to enter parameters for creating a slice.

After the slice is created the OT manager will have to activate it by going to NSM menu and selecting the “Create Slice” button, 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

Co-funded by the Horizon 2020
Framework Programme of the European Union

be allocated for the slice (shown in Figure 3-7). The coverage area of selected base station will be deciding factor for coverage of selected slice.

Figure 3-7: 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.

3.4 Relation to UCs

Network slicing is used similarly in all the use cases to create virtual networks for different applications within the common physical network. Thus, network slicing is relevant for most of use cases that require to allocate resources for different devices that need specific resources to fulfil their QoS needs.

Therefore, the following use cases can utilize the network slicing.

- Automated robots with heterogeneous networks – Factory UC
- Transportation platforms health monitoring – Transport UC
- Situational understanding and predictive models in smart logistics scenarios – Port Entrance UC
- Improved driver's safety with mixed reality and haptic solutions – AGVs UC
- Inter-modal asset tracking via IoT and satellite – Ship UC

Co-funded by the Horizon 2020 Framework Programme of the European Union

4 Geographical Anomaly Detection

Purpose of the present deliverable was to analyze possible metrics for anomaly detection of IoT devices in a vehicular context. The considered data included metrics about temporal ranges, spatial constraints, device identities and other parameters. Given the Port Entrance use case, focused on access devices which are located on top of transport trucks, the outcome of the analysis was that the most relevant gap to address in the anomaly detection procedures refers to the possibility to validate the paths followed by trucks inside the target areas, against admissible or expected routes.

The anomaly detection principle we adopted is based on the geographical validation of the routes followed by the truck-based IoT devices during their movement inside the target area (Valencia port).

The proposed detection mechanism can be deployed for the group of devices associated to the network slices and 5LAN groups.

Several decision mechanisms were considered, based both on rule engines and clustering algorithms. The features of the iNGENIOUS use cases as well as the dataset available led to the selection of clustering-based algorithms. The main motivation for this choice was that rule-based mechanisms are typically suitable for situations which are well defined and are not easily adapted to different contexts or evolving environments. On the other hand, clustering algorithms are particularly oriented to problem domains where constraint rules are difficult to identify, and frequent changes are to be expected.

Furthermore, an architectural definition activity was carried out, which aimed at proposing a strategy to integrate the geographical anomaly detection component within the data flow for the target use case.

The proposal is to integrate the component in a non-real-time validation data flow chain. Within the use-case data flow, the component will:

- Receive path-related data as input;
- Carry out classification of the dataset;
- Produce outcomes and, in case of detected anomalies, generate alarms as output.

The main feature of the iNGENIOUS use-case relevant for the vehicular geographical anomaly detection is the arbitrary shapes of possible paths followed by trucks.

Clustering algorithms help in case of geographical data which cannot be aggregated according to geographical constrains known in advance. Such algorithms are used to group sets of data points so that similar data points are grouped together. In order to achieve that, they look for similarities or dissimilarities in the data points.

Supervised and unsupervised learning methods are available, where clustering belongs to the unsupervised category.

Co-funded by the Horizon 2020 Framework Programme of the European Union

Different approaches and algorithms are available. They can be broadly divided into three main groups:

- Clustering based on partitions;
- Hierarchical clustering;
- Clustering based on density.

Both partition-based and hierarchical clustering algorithms are very efficient with clusters of normal shapes. In contrast with clusters of arbitrary shapes, techniques based on data density are more efficient.

Within density based-algorithms, DBSCAN (Density-Based Spatial Clustering of Applications with Noise) appeared particularly promising because is capable of finding arbitrary-shaped clusters as well as clusters with outliers (noise).

Another advantage of the usage of the DBSCAN algorithm is that it will be easily adapted to evolving environments.

Design specifications

As clustering library Scikit-learn was selected both for the high quality of the library and its very wide adoption. Scikit-learn is a machine-learning library for Python. It includes various classification, regression, and clustering algorithms, including support vector machines, random forests, gradient boosting, k-means. And DBSCAN.

The first challenge was to reduce the size of the path-related spatial data (latitude-longitude coordinates) through the DBSCAN clustering algorithm, in order to group geographically close data-points into “centroids”. Centroids will be automatically defined by the algorithm according to the strategy that training data-points are grouped together if their distance from a centroid is less than a given threshold ε. The set of all centroids will represent the admitted paths within the reference location. The picture on the right in Figure 4-1 below shows an example of such elaboration based on a single training path (picture on the left) for a value of 100 meters for ε. The geographic area corresponds to the Valencia sea port.

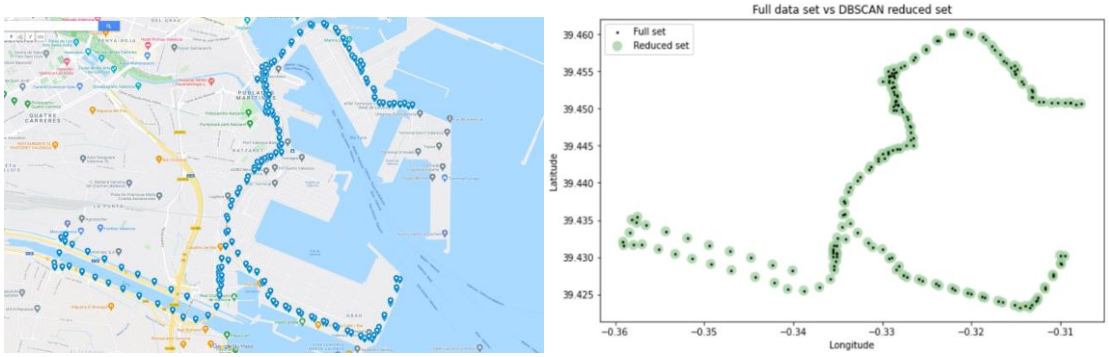


Figure 4-1: Representation of centroids.

The first observation is that the picture on the right-hand side presents gaps between centroids shown in green circles, which could invalidate acceptable

Co-funded by the Horizon 2020 Framework Programme of the European Union

paths. The improvement could be to use denser sampling data. The picture in Figure 4-2 below shows validation of a path against the computed centroids.

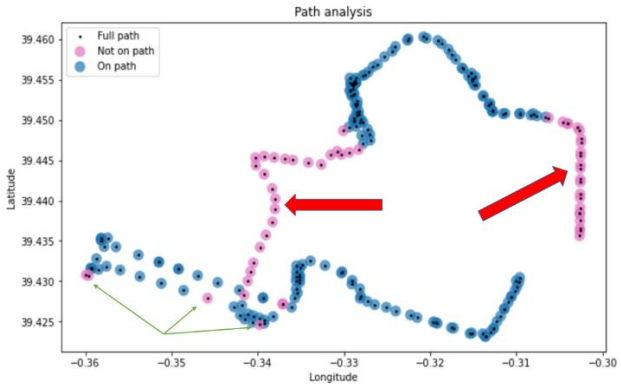


Figure 4-2: Validation path of computed centroids.

Blue points refer to valid sub-paths, while pink points refer to invalid paths, because they do not follow the green centroids (see Figure 4-1). Some of the scattered invalid points are false negative classifications (see green arrows) due to insufficient training data, as pointed out before, while most of them correspond to true negative classifications (see red arrows).

The integration of the geo-classification component into the iNGENIOUS architecture will follow the scheme in Figure 4-3 below. The components could be integrated with the 5GS as external AF.

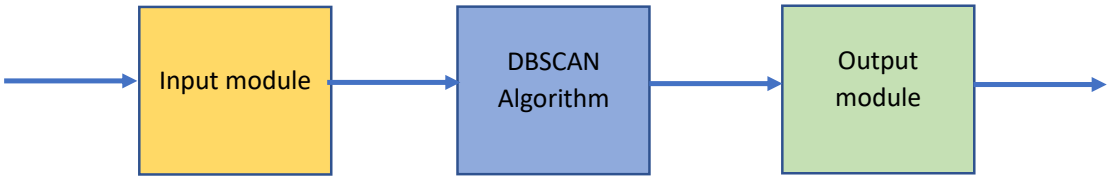


Figure 4-3: Geographical Anomaly detection components.

The input module will receive CSV-formatted data from upstream components, while the output module, based on the algorithm execution, will provide possible alerts about anomalies to downstream components. The detailed definition of the interworking mechanisms for I/O modules will be carried out during the integration phase for Port Entrance use case. Geographical anomaly detection will be done as a post processing validation audit of collected truck paths records, as part of the automated deployment of 5GC for IoT.

Co-funded by the Horizon 2020 Framework Programme of the European Union

5 Automatic Deployment of 5GC for IoT

Automation of supply-chain and industrial IoT services provisioning and operation is one of the key objectives in iNGENIOUS. For this, the IoT network layer in the iNGENIOUS architecture include dedicated Management and Orchestration (MANO) functionalities to automate the management and control of resources spanning RAN, edge, and core network segments in support of network slices. As explained in Section 3, network slicing allows the network operators to provision dedicated logical end-to-end networks spanning several network segments, to interconnect heterogeneous devices (including IoT) and create seamless end-to-end communications. iNGENIOUS aims to satisfy the heterogeneous requirements posed by supply chain and industrial IoT services in terms of network QoS and reliability.

In this direction, 3GPP defined a framework that specifies the functional components required for the management and orchestration of network slices [6], also identifying the network segments (i.e., radio, access, core) to be covered in end-to-end network slice deployment scenarios. On top of that, 3GPP has also defined recently in TS 28.533 [7] a practical deployment scenario for the management and orchestration framework of network slices. Here, following the SBA approach, the typical deployment of the 3GPP management and orchestration system is structured by combining (as shown in Figure 5-1) a top-level Network Slice Management Function (NSMF) with domain-specific Network Slice Subnet Management Functions (NSSMFs). In particular, the NSMF is responsible for the management and end-to-end orchestration of network slice instances. It splits each network slice into per-domain slice subnets and manages their lifecycle. Therefore, the NSMF makes decisions about the composition of a network slice, including the re-use of pre-existing slice subnets that can be shared among multiple network slices. On the other hand, the NSSMFs are customized according to the specific requirements and technologies adopted in their own target domain, i.e., RAN, Core Network and where applicable Transport Network domains.

3GPP standard do not detail any specific implementation of the NSMF and NSSMF components. However, they propose a widely used deployment option where the management of the network slices and slice subnets lifecycle is mandated to ETSI NFV MANO systems [8]. iNGENIOUS, as detailed in the following sub-sections, follows this approach for the Core Network domain, where the 5GC NFs are modelled as Virtualized Network Functions (VNFs), with an NFV Orchestrator responsible for the lifecycle of the 5GC NFV Network Services associated to the related slice subnets.

Co-funded by the Horizon 2020 Framework Programme of the European Union

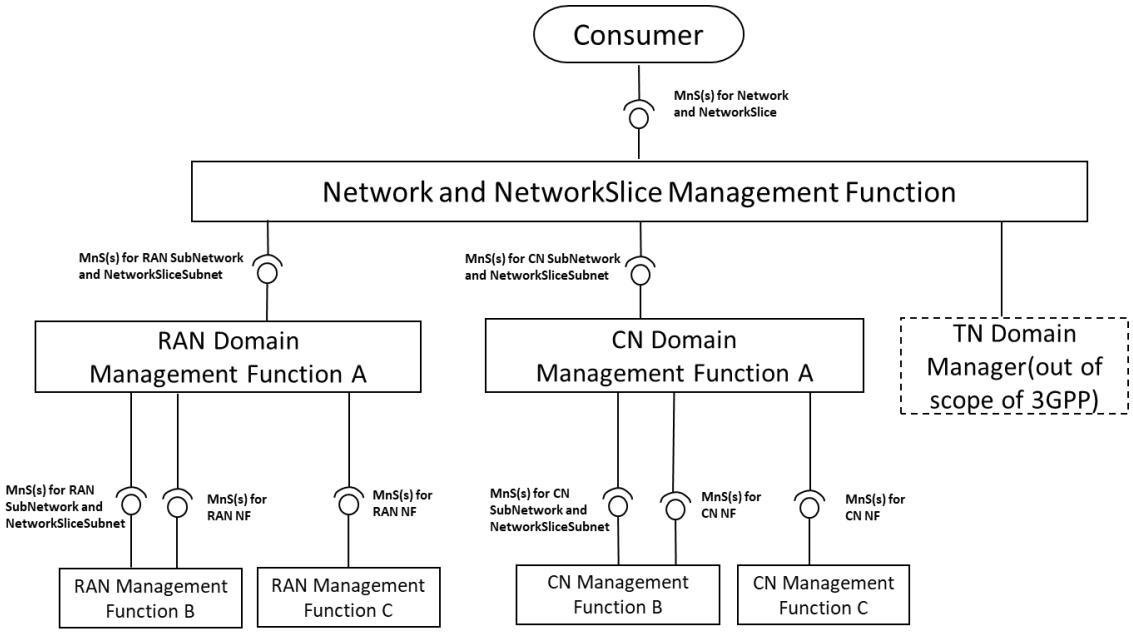


Figure 5-1: 3GPP NSMF and NSSMF deployment model [7]

5.1 5GC Virtualization and Automated Deployment

The 5G network architecture brings a new disruptive approach that considers a high degree of virtualization of the network functions and services by design. In particular, the 5GC architecture, based on the SBA principles, and its NFs are defined in the 3GPP standards to be natively deployed and operated on top of NFV infrastructures. In this perspective, 3GPP and ETSI NFV are aligned in their views and network slicing definitions [9]. NFV Network Services are indeed considered the basic logical elements to implement network slice subnets (e.g., providing 5GC functionalities). The 5G NFs defined by 3GPP can be modelled as VNFs and can therefore be managed and orchestrated through ETSI NFV MANO components.

For what concerns the specific Core Network domain (according to the Figure 5-1 architecture diagram), the first step towards the implementation of the 5G network virtualized approach is the virtualization of the 5GC NFs. Following the ETSI NFV principles and specifications, each NF (either belonging to the 5G control plane or user plane) can be modelled as an independent VNF. In practice, each 5GC NF runs in software on top of commodity hardware, allowing to replicate and easily manage multiple instances of the same NF across several virtualized infrastructures. The integration of multiple VNFs through the 5GC SBA interfaces compose a 5G NFV Network Service.

There are two main options, both compatible with the ETSI NFV definitions, to have 5GC NFs implemented as virtualized functions (i.e., VNFs): (Docker) containers and Virtual Machines (VMs). These two options mainly distinguish how the NFs themselves run in the virtualized infrastructure, in terms of type of software image used. Docker containers allow to package a 5GC NF application with all its dependencies into a standardized unit for software deployment, offering a logical packaging mechanism in which applications

Co-funded by the Horizon 2020 Framework Programme of the European Union

can be abstracted from the environment where they actually run. Docker containers are the base foundation of cloud-native and microservice deployments, and do not require operating system virtualization. Moreover, Docker enables a semi-automated process for container images creation and exposure starting from the raw software code of the 5GC NF. On the other hand, VMs are a specific case of software images that provide a full package including operating system, application logics and the required binaries and dependencies (such as libraries and other applications) to run a given 5GC NF application. 5GC NFs implemented and packaged as containers can be deployed and operated on top of cloud-native infrastructures, e.g., based on Kubernetes. On the other hand, 5GC NFs implemented and packaged as VMs have to be operated with traditional Infrastructure as a Service (IaaS) platforms like Openstack and VMWare. Independently of the two approaches, iNGENIOUS models 5GC NFs as VNFs, thus supporting the standard ETSI NFV descriptors and packages, as templates expressing the requirements (in terms of virtualized resources constraints, including network, storage, and processing) to be satisfied to properly run the NFs.

On top of the modelling of the 5GC NFs as VNFs, there is the need of an orchestration framework to provide full automation of VNFs and 5GC NFV Network Services deployment and operation, as part of end-to-end network slices. As anticipated in deliverable D4.2 (with further details to be provided in D4.4), and recalled here for the sake of completeness of this document, iNGENIOUS implements a cross-layer MANO framework, aligned with the 3GPP approach specified in 3GPP TS 28.533 [7], where the network slice orchestration functionalities are provided by an NSMF and multiple NSSMFs (see Figure 5-2). In particular, each NSSMF is dedicated to the management of its technology or network domain (access, core or transport network), and interacts with per-domain resource controllers and orchestrators that take care of allocating and configuring slice resources (e.g., VNFs, radio resources, etc.).

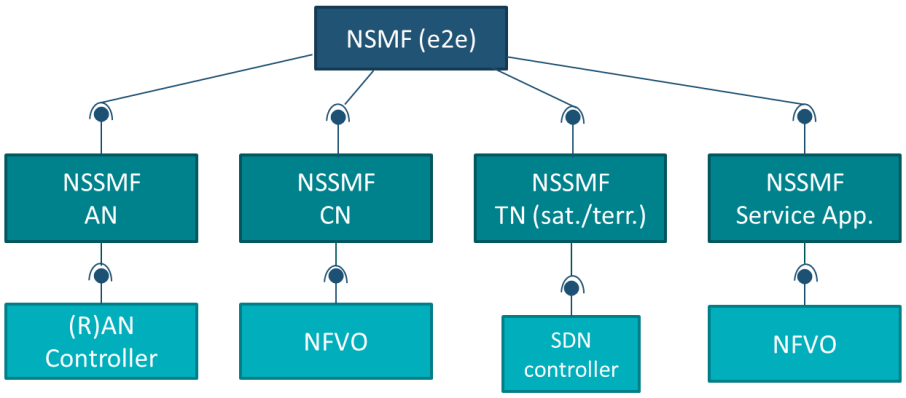


Figure 5-2: Architectural diagram of Network Slice Management in 5G network.

As depicted in Figure 5-2, for the specific case of the Core Network domain, the related NSSMF interfaces with an NFV Orchestrator (NFVO) to delegate the lifecycle management of VNFs (and NFV Network Services) that implement the 5GC NFs and services. In particular, iNGENIOUS makes use of the ETSI OSM open-source tool as NFVO [10]. ETSI OSM is the ETSI-driven NFV MANO reference implementation, that is supported by a wide industry community and has built a wide ecosystem with heterogeneous industry and

Co-funded by the Horizon 2020 Framework Programme of the European Union

research related activities [11] in relevant 5G environments. From a technical perspective, ETSI OSM provides full NFVO and VNF lifecycle management capabilities, supporting both VM and container based VNFs deployments, with integration of heterogenous private and public cloud infrastructure (e.g., based on Openstack, Kubernetes, VMWare, AWS, Azure). This is performed according to the ETSI NFV specifications for NFVO northbound REST APIs, as well as VNF and Network Services descriptors (VNFD and NSD) and packages.

In the specific context of the management and orchestration of the 5GC, the following sub-section provides a description of the initial activities carried out for the integration and validation of ETSI OSM with the Cumucore 5GC described in the previous chapters. More work in this direction, specifically targeting the integration with the full iNGENIOUS cross-layer MANO depicted in Figure 5-2 will be reported in deliverable D4.4.

5.2 MANO Orchestration

This subsection describes the initial integrations between the 5GC by Cumucore and the NFVO implemented by ETSI OSM, as part of cross-layer MANO. In particular, the integration works related to the configuration and tests of a 5G network in a local testbed are described. Furthermore, experiments related to the manual configuration, deployment, and execution of the 5G network with cross-layer ETSI OSM are described too.

Before proceeding with the integration between 5GC and ETSI OSM, the 5GC itself must be properly set up and tested with at least one gNB, for providing 5G connectivity to the UE. In this sense, emulated gNBs and UEs have been broadly exploited for this purpose.

The emulated gNB is part of the UERANSIM open-source tool [12], widely used for testing 5GC Networks. Briefly, it allows not only to emulate a gNB that connects to a 5GC but also to emulate several UEs that can be connected to different gNB. The usage of several instances of UERANSIM allows to simultaneously connect several gNB and UEs to the same 5GC, with the aim of performing stress tests towards the 5GC itself.

Additionally, the 5GC contains the Control Plane (AMF, SMF and NRF) and User Plane (UPF) Network Functions for providing 5G connectivity. The 5GC instance also contains a web service for managing information related to the subscribed UEs, the gNBs and Telecommunication and Network Operators information of the UEs themselves.

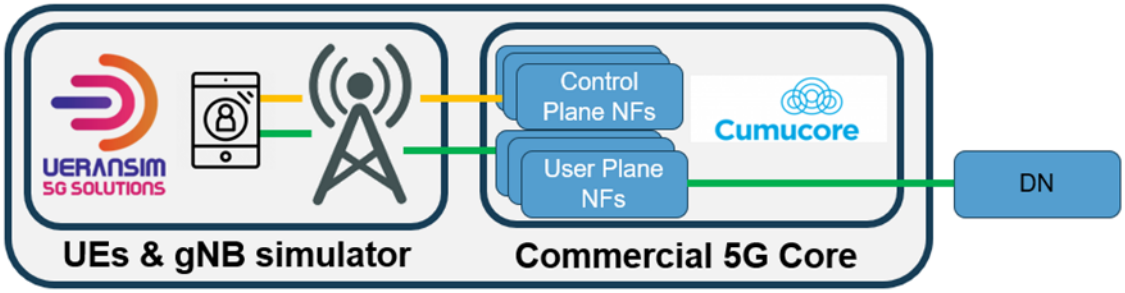


Figure 5-3: 5G Network deployment in a local testbed

Co-funded by the Horizon 2020 Framework Programme of the European Union

The diagram depicted in Figure 5-3 shows how the emulated gNB and the 5GC are first deployed and then properly configured to connect them to each other. The deployment of the 5GC is in stand-alone mode, meaning that all the NFs are available in a VM. In particular, after the gNB and the 5GC establish an SCP connection (yellow line), then a PDU connection between the UE and the 5GC is established too (green line). This implies having the UE(s) connected to the Data Network (DN), in the case of the experiment the DN would be public Internet.

The initial integration between the 5GC with ETSI OSM mainly consists of the automated instantiation of the corresponding Network Service. In particular, the UERANSIM tool and the 5GC have been defined as two VNF Packages referenced within an NFV Network Service Descriptor (NSD). Eventually, the NSD is then deployed as a Network Service Instance on top of the Virtual Infrastructure, which is based on OpenStack in the particular case of the early integration tests.

Figure 5-4 depicts a high-level diagram of the deployment of the NSD, which is composed of such VNF packages. The NSD and VNF Packages are onboarded within the ETSI OSM platform for being ready to be deployed. For the early integration tests, ETSI OSM relies on a Virtualized Infrastructure managed by OpenStack, and takes care to deploy and configure the 5GC and UERANSIM VNFs referenced within the NSD. In particular, the day-0 and day-1 configurations available in the VNF packages have been executed using cloud-init [13] and Juju charm open-source tools [14], respectively. The former is used for configuring the VM once at the very first boot (e.g.., network interfaces, users' credentials and so on), while the latter is used for configuring the services embedded within the VM (e.g., IP address exposed by a service, listening port and so on). Since the day-1 configuration is an automatic process occurring at the deployment time and it can be parametrized, different custom instances of 5GC can be configured. For example, a 5GC instance with either only Control Plane NFs or a 5GC instance with only User Plane NFs can be deployed. In this particular case, the parameters involved in the configuration could be for instance the type of Network Functions made available once the 5GC is ready.

Co-funded by the Horizon 2020
Framework Programme of the European Union

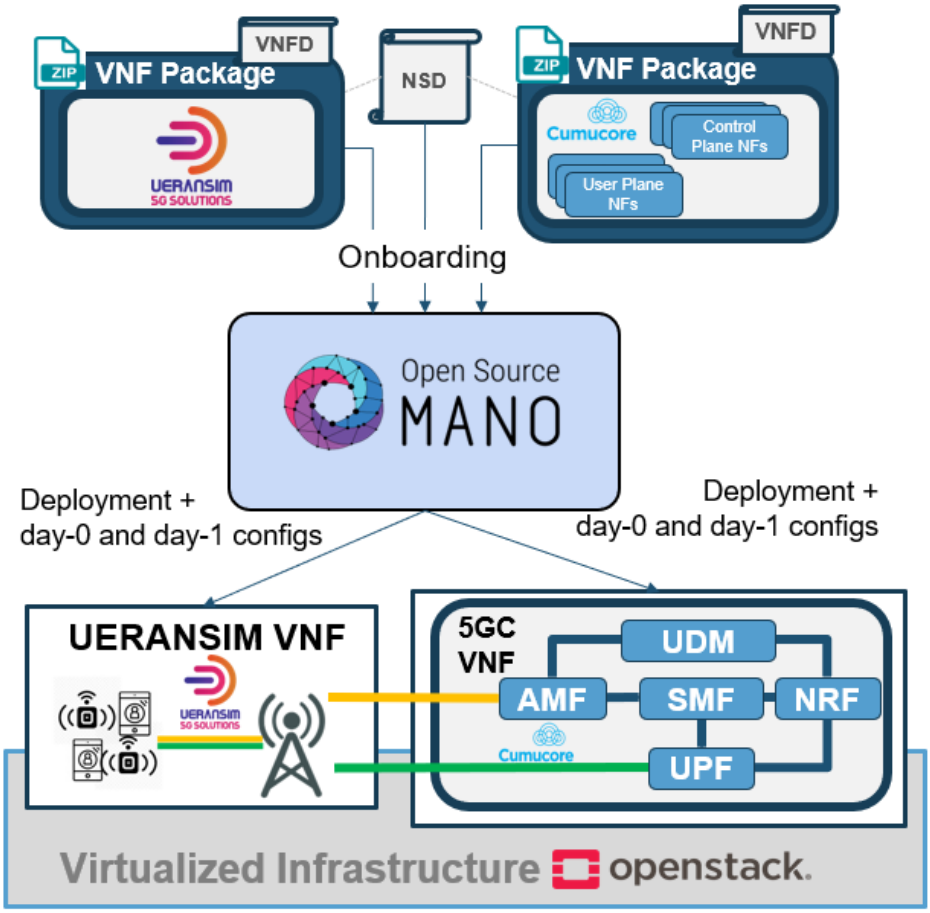


Figure 5-4: High-level workflow of manual deployment of a 5G network.

Figure 5-5 shows some details on how the NSD and the related VNF packages composition. Each VNF Descriptor contained into the VNF Package is based on the ETSI SOL006 specification [15]. In general, a VNF Descriptor encloses all the technical details related to the deployment of the VNF itself: deployment flavour, instantiation level, disk size, RAM used, virtual links and so on.

The NSD not only refers to the VNF Packages for their deployment, but also creates the network connections among the virtual links defined within the VNFs. Moreover, during the deployment process, the NSD with the support of the Juju relation, is able to provide configurations from one VNF to another creating the relationship among them.

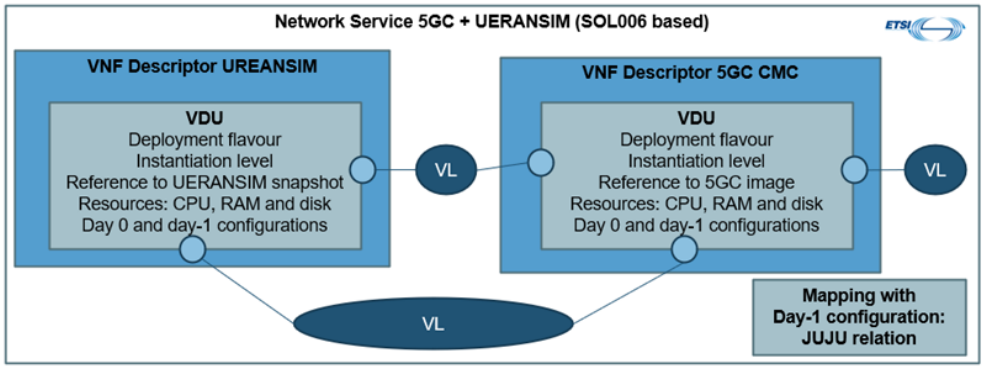


Figure 5-5: High-level diagram of Network Service

Co-funded by the Horizon 2020 Framework Programme of the European Union

For triggering the deployment and configuration of the aforementioned Network Service, the web GUI of OSM has been used, specifying the NSD to instantiate, the name of the Network Service Instance, a custom description and optionally some custom configurations (Figure 5-6 (a) and (b)).

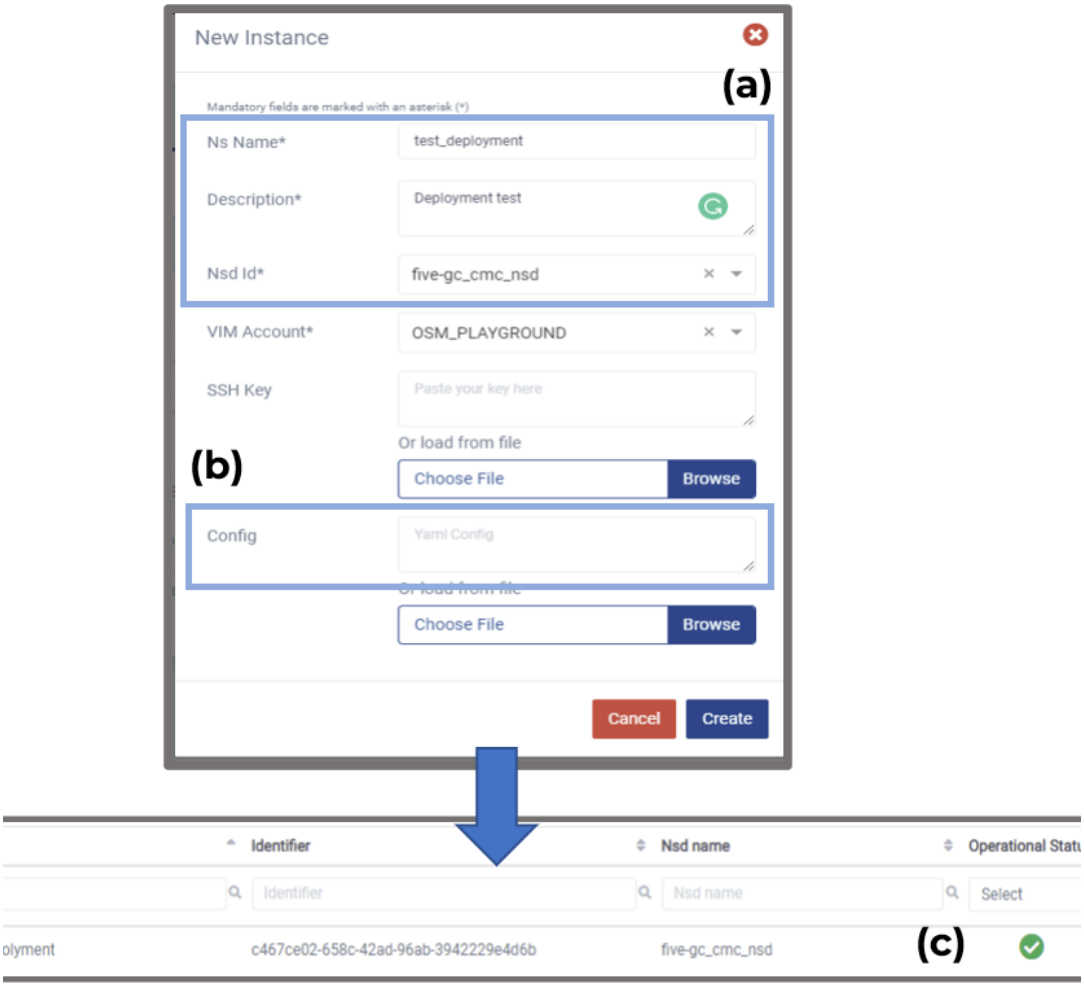


Figure 5-6: Creation of a Network Service Instance using the OSM Web GUI.

As a final result of deployment, the Network Service Instance is up and running on ETSI OSM (Figure 5-6 (c)) meaning that two instances are successfully configured and deployed on OpenStack premises and the related day-0 and day-1 configuration have been successfully executed. This results in having the UERANSIM instance with the gNB ready to be connected to the 5GC instance, which is up, running and listening for incoming connections. For finalizing these initial integration tests, some emulated UEs have been connected to the 5GC for providing 5G connectivity. Figure 5-7 depicts a connectivity test where a UE downloads a 1GB sample file using the HTTP protocol through the wget tool using the tunnel interface towards the 5GC.

Co-funded by the Horizon 2020
Framework Programme of the European Union

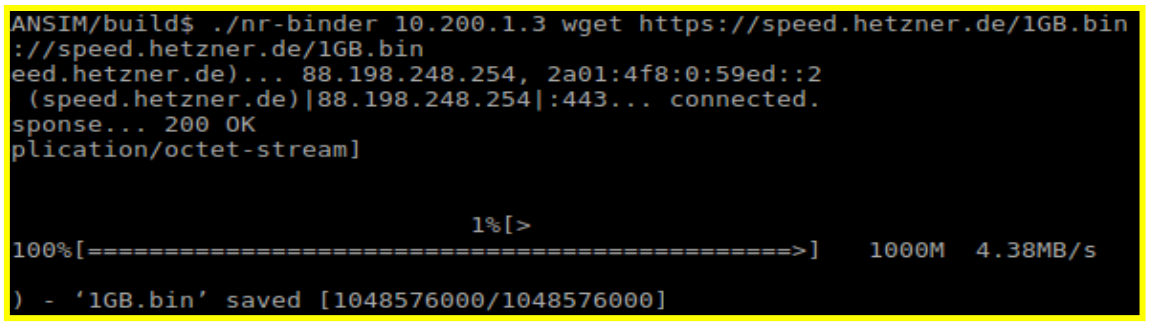


Figure 5-7: Connectivity test with emulated UEs with 5GC

As part of future work that will be reported in the D4.4 deliverable of INGENIOUS, additional integrations with the 5GC will be supported. Figure 5-4 depicts an edge-core deployment of the 5GC. In particular, the Control Plane NFs and the User Plane NFs are in two different VMs, one placed at the Core of the 5G Network and one placed at the Edge of the 5G network. The main motivation is to reduce as much as possible the network latency of the User Plane for satisfying the low-latency requirement of a generic edge application. Moreover, the deployment through ETSI OSM of the containerized version of 5GC will be also validated. This allows a more flexible management and configuration of the 5GC NFs. Once the dockerized version of the 5GC will be available, the new Network Service Descriptor(s) will be designed and tested. Finally, the current ETSI OSM web GUI driven deployment and configuration of the 5GC Network Services will be fully automated, as part of the integration with the full cross-layer MANO framework. Specifically, the ETSI OSM NFVO will be integrated with the dedicated Core Network NSSMF in the context of end-to-end network slice provisioning automation.

Co-funded by the Horizon 2020
Framework Programme of the European Union

6 Conclusions

This deliverable has described the design and implementation of 5GC 5GLAN, network slicing and cluster-based access control for INGENIOUS IoT communications. The automated deployment of the 5GC with the integration MANO orchestrator has been presented in the deliverable.

The first implementation of the network slicing and 5GLAN functionality has been completed and integrated with the network orchestrator for automated deployment of the 5GC. This deliverable has included the design and implementation principle of the 5GC as well as first results of the testing using network orchestrator.

The integration and validation of 5GLAN with network slicing has been completed as part of the 5GC to provide reliable communications. The integration of 5GC with orchestrator has been finalized and validated so the automated deployment and management of the 5GC is performed.

Co-funded by the Horizon 2020
Framework Programme of the European Union

References

[1] An Introduction to Network Slicing by GSMA, https://www.gsma.com/futurenetworks/wp-content/uploads/2017/11/GSMA-An-Introduction-to-Network-Slicing.pdf.

[2] Description of Network Slicing Concept by NGMN Alliance, https://www.ngmn.org/fileadmin/user_upload/161010_NGMN_Network_Slicing_framework_v1.0.8.pdf

[3] 3GPP TS 28.531 (https://www.etsi.org/deliver/etsi_ts/128500_128599/128531/16.06.00_60/ts_128531v160600p.pdf)

[4] 3GPP TS 23.434 (https://www.etsi.org/deliver/etsi_ts/123400_123499/123434/16.04.00_60/ts_123434v160400p.pdf)

[5] 3GPP TS 23.501 (https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3144)

[6] 3GPP TR 28.801, “Telecommunication management;Study on management and orchestration of network slicing for next generation network”, Release 15

[7] 3GPP TS 28.533, “Management and Orchestration; Architecture framework", Release 17

[8] ETSI GS NFV-MANO 001, “Network Function Virtualisation (NFV); Management and Orchestration”, v1.1.1, December 2014

[9] ETSI GR NFV-EVE 012 V3.1.1, “Report on Network Slicing Support with ETSI NFV Architecture Framework”, December 2017

[10] ETSI Open Source MANO (OSM), https://osm.etsi.org/

[11] ETSI OSM Ecosystem, https://osm.etsi.org/wikipub/index.php/OSM_Ecosystem

[12] UERANSIM tool for gNB and UE Emulation: https://github.com/aligungr/UERANSIM

[13] Cloud-init tool for day-0 configuration: https://cloudinit.readthedocs.io/en/latest

[14] Juju Charm tool for day-1 configuration: https://cloudinit.readthedocs.io/en/latest

[15] ETSI SOL006 Specification: https://www.etsi.org/deliver/etsi_gs/NFV-SOL/001_099/006/02.07.01_60/gs_nfv-sol006v020701p.pdf

Co-funded by the Horizon 2020 Framework Programme of the European Union