FUDGE-5G

FUlly DisinteGrated private nEtworks
for 5G verticals

Deliverable D3.2

FUDGE-5G On-boarding and Deploying of the Vertical Use Cases

Version 1.0

Work Package 3

Editor	Pousali Chakraborty and Marius-Iulian Corici (Fraunhofer FOKUS)
Month	30

Partners

Universitat Politècnica de València, telenor, athonet, Cumucore, Fraunhofer FOKUS, ONE2MANY, UBITECH, ONESOURCE, Fivecomm, interdigital, HUAWEI, THALES

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957242

Disclaimer

The FUDGE-5G project consortium does not accept any responsibility or liability for any use made of the information provided on this document.

All FUDGE-5G partners have agreed to the **full publication** of this document.

Project details

Project title:	FUlly DisinteGrated private nEtworks for 5G verticals
Acronym:	FUDGE-5G
Start date:	September 2020
Duration:	30 months
Call:	ICT-42-2020 Innovation Action

For more information

Project Coordinator
Prof. David Gomez-Barquero
Universitat Politecnica de Valencia
iTEAM Research Institute
Camino de Vera s/n
46022 Valencia
Spain

http://fudge-5g.eu
info@fudge-5g.eu

Acknowledgement

FUDGE-5G has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement Nº 957242. The European Union has no responsibility for the content of this document.

Abstract

This deliverable describes the integration work performed in FUDGE-5G during the second phase of the project (i.e., second half of the project until February 2023). In D3.1, the integration work performed in the first phase of the project for 5G core with 5G NR, vertical applications were reported. In D3.2, the integration done in that context to realize the use case and make the environment ready for the trials are depicted. Integration work performed to deploy the 5G cores in the e-SBA platform and prepare the infrastructure, integrate the innovations brought by FUDGE in the platform, onboard applications for use cases are illustrated in this deliverable.

Versioning and Contributions

Versioning

#	Description	Contributors
0.1	First version with the ToC	FHG
1.0	Final version and uploaded to website	ALL

Contributors

Partner	Authors
FHG	Pousali Chakraborty, Hemant Zope, Marius-Iulian Corici
TNOR	Faheem Muhammad, Ole Grøndalen, Andres Gonzalez
ATH	Daniele Munaretto, Nicola di Pietro
CMC	Jose Costa, Mika Skarp
O2M	Peter Sanders
UBI	Thanos Xirofotos
IDE	Sebastian Robitzsch
HWDU	Zoran Despotovic, Artur Hecker, Dirk Trossen
THA	Franck Scholler
ONE	Luís Cordeiro, André Gomes, João Fernandes
5CMM	Manuel Fuentes, Alberto Beltrán
UPV	Carlos Barjau, Josep Ribes, David Gomez-Barquero

Abbreviations

3GPP	3rd Generation Partnership Project
5G	5th Generation of mobile communications
5GC	5G Core
AAU	Active Antenna Unit
AF	Application Function
AMF	Access and mobility Management Function
API	Application Programming Interface
AUSF	Authentication Server Function
CBCF	Cell Broadcast Control Function
CBE	Cell Broadcast Entity
CPE	Customer Premise Equipment
DNS	Domain Name Service
DNN	Data Network Name
DS-TT	Device-side TSN Translator
E2E	End to End
GUI	Graphical User Interface
LAN	Local Area Network
MME	Mobility Management Entity
NEF	Network Exposure Function
NF	Network Function

NFV	Network Function Virtualization
NOW	Network on Wheels
NPN	Non-Public Network
NR	New Radio
NRF	Network Repository Function
PCF	Policy Control Function
PLMN	Public Land Mobile Network
PNI-NPN	Public Network Integrated-NPN
PPDR	Public Protection and Disaster Relief
PTT	Push To Talk
RAN	Radio Access Network
SA	Stand-Alone
SBA	Service-Based Architecture
SBC	Session Border Controller
SCP	Service Communication Proxy
SEPP	Security Edge Protection Proxy
SHs	Service Hosts
SMF	Session Management Function
SNO	Single Node OpenShift
SNPN	Standalone NPN
TN	Transport Network
TSN	Time Sensitive Networking

UC	Use Case
UDM	Unified Data Management
UE	User Equipment
UPF	User Plane Function
VA	Vertical Application
VAO	Vertical Application Orchestrator
VLAN	Virtual LAN
VM	Virtual Machine
VNF	Virtualized NF
VPN	Virtual Private Network

Executive Summary

FUDGE-5G aims to perform field trials for private 5G networks by showcasing five vertical use cases. In D3.1, the first phase of integration work performed for the use cases with the 5G Cores, NR, vertical applications were reported along with some integration planning for the next phase of the project. This deliverable D3.2, aims to describe the integration of technologies (those are defined in WP2 deliverables) for onboarding the use cases on the FUDGE platform, to technically validate the features and do the final phase of vertical trials with the stakeholders. In the tenure of the project to realize the use cases, technological components have been developed by the consortium partners including some 5G core (5GC) features developed by the 5G core network vendors. In order to deploy the use cases in the trial sites, infrastructures have been prepared by deploying 5G private networks, hosting the technological components and integrating with the vertical applications. The 5GCs available in the project and vertical application orchestrator (VAO) have been onboarded on the FUDGE-5G eSBA platform. This deliverable point out more on the work done on the packaging, configuration and integration of different components to realize the use cases. The technical validation of these components will be reported in D4.2 and the validation of the use cases with the help of several KPIs will be reported in D4.3.

Table of contents

List of Figures

List of Tables

1. Introduction

During its duration, the FUDGE-5G project strived to create components that empower European companies in the growth of 5G Non-Public Network (NPN) feature portfolio. This not only includes the provision of customized 5G Core (5GC) Network Functions (NFs), but also, tailored applications that fully leverage the NPN advantages and accommodate themselves to the need of the project stakeholders. To do so, significant effort was put into creating an appropriate test-bed to host the FUDGE-5G platform (described in D2.5) and deploying use case nodes that will integrate and on-board consortium components. Figure 1 below shows the components and nodes, including where have they been deployed.

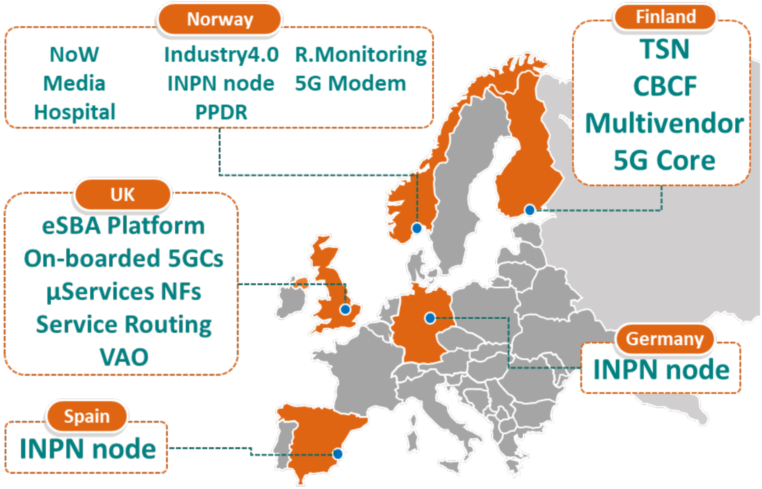


Figure 1: Main nodes, components, applications and use cases location.

Overall, the project prepared 4 nodes for use cases: the Network on Wheels (NoW), a portable all-in-one 5G NPN network used for the Media and PPDR use cases; the Virtual Office node in the Oslo Rikshospitalet; the Industry 4.0 node in ABB Norway premises; and three subnodes for the Interconnected NPN (INPN) use case, composed by a Valencia, Berlin and the Virtual Office one. Additionally, there is a multi-site infrastructure testbed in London which hosts the eSBA platform and has available several disintegrated components from the consortium, including the 5GC solutions from Athonet, Cumucore and FOKUS; with the Vertical Application Orchestrator (VAO) from Ubitech which manages Kubernetes clusters.

The nodes have been integrated to support novel key features, enabled by new components all developed as extensions of their existing product portfolio. In detail, six key features have been implemented: 5GLAN, Time Sensitive Networking (TSN) and Network Slicing in the Cumucore 5GC; Session Border Controller (SBC) in the FOKUS Open5GCore; the Cell Broadcast Control Function (CBCF) by One2Many; and the microservice based Network

Exposure Function (NEF) by OneSource. Aforementioned feature list has been integrated in different nodes and as close as possible to realistic environments, in order to validate their functionality. More detailed info of the features and their respective components can be found in D4.2.

Lastly, the on-boarding of vertical applications has been also covered during the project. A cross-project effort between Affordable5G [1] took place, where Nemergent provided a Push-To-Talk (PTT) for the PPDR use case and was integrated into the NoW. The other application on-boarded was Onesource Mobitrust into the Virtual Office node so it can gather medical instrument and sensors data over 5G.

All this information is further described in below sections. In detail, the deliverable is structured in five main chapters: Chapter 2 contains the description of the Key Features implemented; Chapter 3 defines the infrastructure provisioned for the use cases; Chapter 4 covers the vertical application on-boarding with FUDGE-5G components, and Chapter 5 describes the integration of Chapter 2 Key Features into the different nodes.

2. Key Features

During the tenure of the project some functionalities were developed by the consortium partners to achieve the motivation of the use cases. The following subsection discuss about six features which played key role in the use case validation.

2.1. 5GLAN

5GLAN functionality which emulates Layer 2 connectivity between devices in a 5G SNPN was developed by Cumucore [2]. This feature is useful in industrial environments, where machinery use non-IP protocols e.g. Ethernet frames and methods e.g. ARP discovery to communicate with other devices. To deliver 5GLAN functionality a new Network Controller has been introduced as a 5G Application Function (AF). Accordingly, the Cumucore 5GC SMF and UPF have been retrofitted to support 5GLAN functionality, as shown in Figure 2.

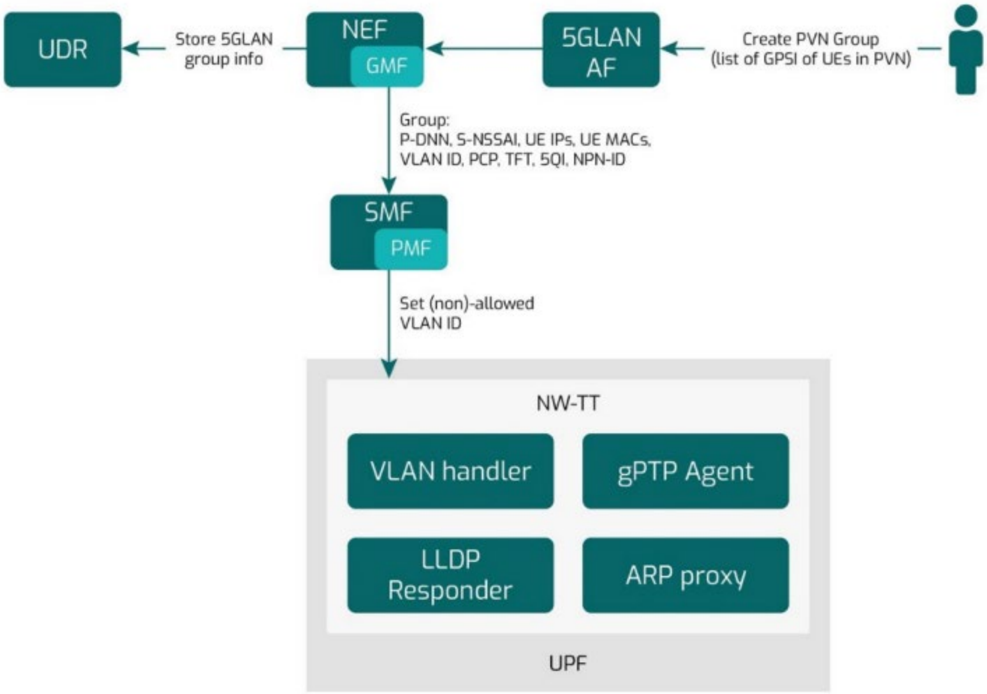

UDR
Store 5GLAN group info
NEF
GMF
5GLAN AF
Create PVN Group (list of GPSI of UEs in PVN)
Group:
P-DNN, S-NSSAI, UE IPs, UE MACs,
VLAN ID, PCP, TFT, 5QI, NPN-ID
SMF
PMF
Set (non)-allowed VLAN ID
NW-TT
VLAN handler
gPTP Agent
LLDP Responder
ARP proxy
UPF

Figure 2. 5GLAN functionality as part of the Cumucore solution.

The 5GLAN feature has been on-boarded into ABB premises. More information can be found in Section 3.2.2.

2.2. Time Sensitive Networking

Time Sensitive Networking (TSN) is a suite of functionalities to provide time constrained information across networks [3]. 3GPP included the capabilities for the 5GC to behave as a TSN switch in Release 16. In FUDGE-5G, this functionality was developed by Cumucore in their 5GC solution, including a TSN AF, UPF modifications and the DS-TT functionality in the UE. TSN feature is implemented on top of 5GLAN functionality explained before. TSN architecture is shown in Figure 3.

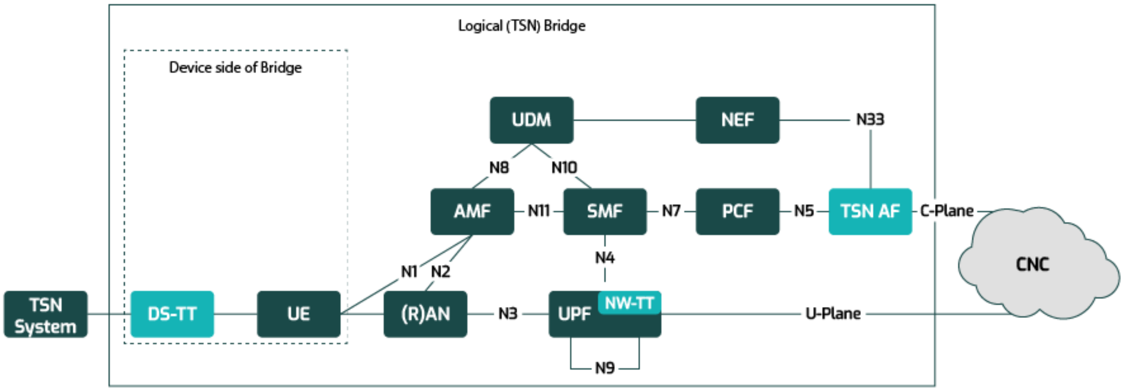


Figure 3. TSN architecture with the new components in light blue.

The TSN 5GC solution has been integrated with 5CMM modem, which identifies and forwards the TSN frames to the DS-TT side of the bridge.

2.3. Network Slicing

Network Slicing feature enables to deliver several virtual networks from one physical network, each with their own group of Network Functions, features, policies, group of users, external connectivity routing. This technology is paired with advanced features such as 5GLAN and integration to external Data Networks while ensuring the isolation (in terms of security and computation) between different slices, as shown in Figure 4.

Network Slicing is delivered over the Radio Access network which is shared with different group of users; but the transport is dedicated per slice and enabled using VLAN technology inside the 5GC and managed by an UPF virtual function per Network Slice. The rest of the 5GC NFs can be instantiated as needed, depending on service or customer needs. Similar to the 5G System, the UPF serves as an integration point for external data networks.

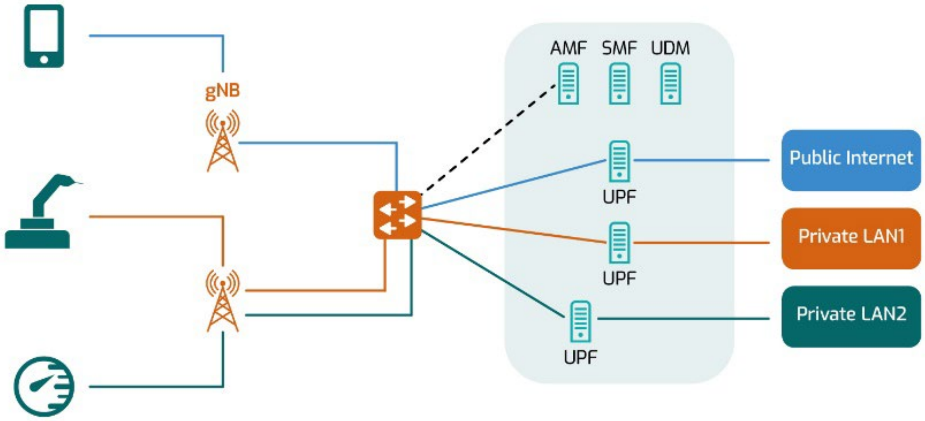


Figure 4: Network Slicing principle In the Cumucore solution.

2.4. Session Border Control

The Fraunhofer FOKUS core is running Session Border Control (SBC) to connect different NPN deployments. The implemented SBC in Open5GCore is a combination of the Service Communication Proxy (SCP) and Security Edge Protection Proxy (SEPP), for supporting roaming scenarios [4]. Currently SCP is available in the Open5GCore and the systems were already validated. The main goal of the SCP is to forward the request between two nodes, adding the capability of hiding the network edges behind one component. While the current version of the SCP uses unsecured communications, by adding the SEPP; the communications can be secured. In order to secure the links between SBC nodes, an upgrade to use HTTPs has been chosen. The current version of the Open5GCore uses nghttpx [5] software as a temporary solution to cypher outgoing SBC data. The way nghttpx proxy works is by doing HTTP2 forwarding alongside with basic HTTP1.1. As there are two separate streams, two proxies are needed: One forward proxy to convert HTTP to HTTPS and second as reverse proxy to convert HTTPS to HTTP. This is deployed on both locations (local and remote network) to handle forward and reverse traffic. Figure 5 shows the Open5GCore with the SCP.

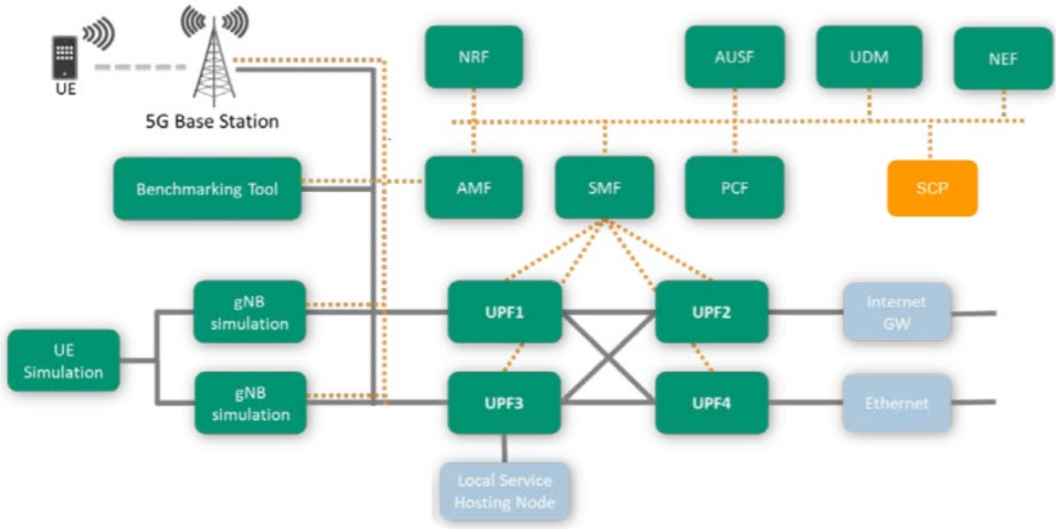


Figure 5: Open5GCore Architecture with SCP as CNF

2.5. Cell Broadcast Control Function

When the project started, the O2M Cell Broadcast Control Function (CBCF) [6] was a monolithic system consisting of an active-passive geo-redundant system. The CBCF was dependent on the Red Hat Linux OS and used Oracle ProC for its communication with the database. In case an upgrade of the software had to be done, the site needed to be made the passive before any upgrade could be performed. Scaling is static and can be done based on the number of radio cells that need to be supported.

The CBCF developed in the FUDGE-5G project features a decomposition of the functionalities in several micro-services, detailed as follow:

- **Rest**: which terminates and validates the incoming requests from a CBE, that includes a message and an alert area description (polygon, circle or geocode)
- **Dest**: which resolves the area description into a list of cells that need to broadcast the message
- **Kernel**: network technology agnostic scheduler of messages
- **Adapter**: network specific driver that sends messages to 2G and 3G RAN (BSC and RNC resp.) and 4G and 5G core network functions (MME and AMF resp.)

The micro-services are packaged in Docker containers which can be orchestrated with Kubernetes. The database architecture is shown in Figure 6 as a Mongo database, but the CBCF relies on a database service rather than a specific Mongo database as shown in the figure.

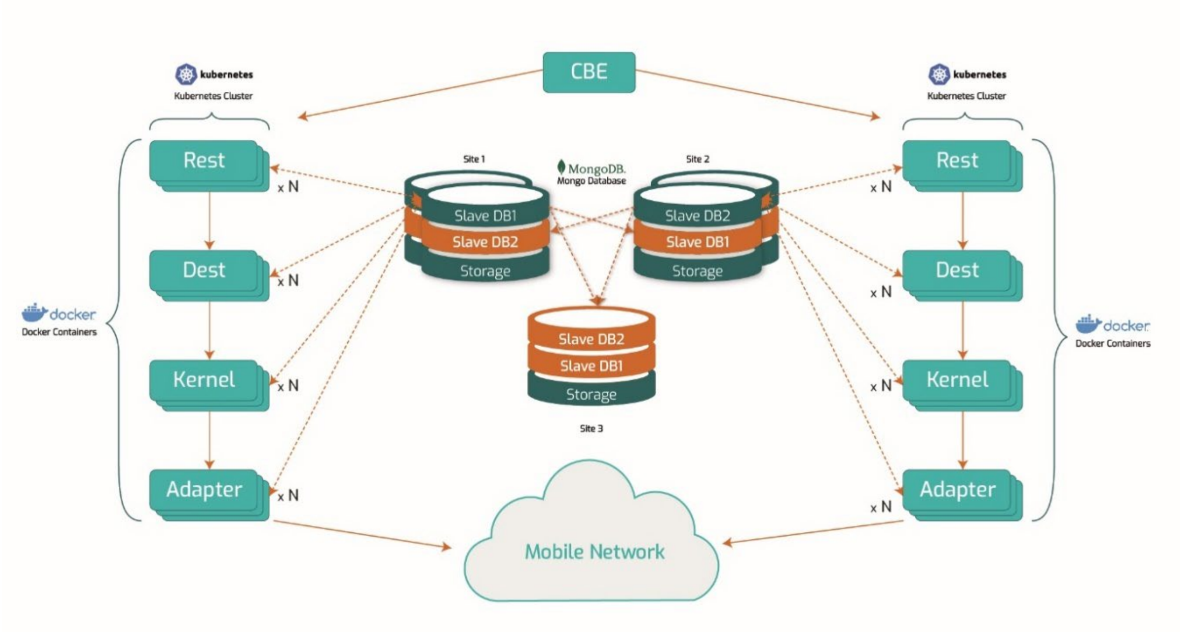


Figure 6: Decomposed CBCF architecture.

The adapter for 5G has been tested with core net vendors such as Ericsson, Nokia, and Huawei. An entire single-side system has been successfully tested with the Cumucore 5G core network. This same system will be used for the demonstration in the NOW and the results reported in D4.2 and D4.3.

2.6. Network Exposure Function

The Network Exposure Function (NEF) used in the context of this project is based on a microservice design proposed by OneSource. As described in D2.4 [5], by being located between external Application Functions (AFs) and the 5GC, NEF provides an access point for such applications to interact with the 5GC securely as per 3GPP specification.

Coupling a scalable and stateless API Gateway with the three microservices shown in Figure 7, both a logical separation and self-compartmentalization are achieved, with meaningful improvements in reliability, security, and performance.

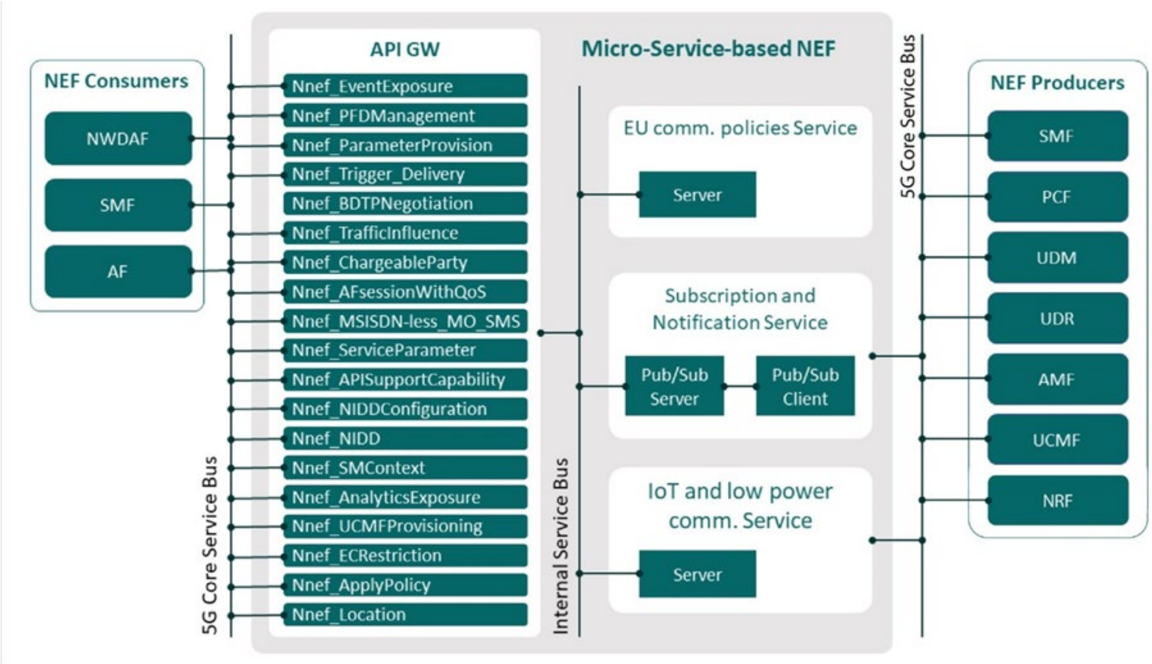


Figure 7: Proposed microservice-based NEF design

3. Infrastructures

During the project duration, several nodes have been provisioned in order to test, on-board, connect and perform trials of the 5 Use Cases and validate the consortium components. They can be classified into three main groups: The Fornebu Telenor testbed, used for preliminary integrations; the three main nodes, Industry 4.0 at ABB Norway, mobile NoW, Oslo Riksohospitalet and the interconnected NPNs network between Valencia, Berlin and Oslo. The last infrastructure is located in IDE premises on London, where the cloud-native SBA-based platform is located. The details for the integration work and feature of each node are listed in the rest of this section.

3.1. Preliminary Test Setup at Fornebu

Telenor's 5G Experimentation Platform includes a central site in Fornebu as well as several edge and RAN sites across Norway, which are interconnected by Telenor Norway's commercial transport network (TN). This testbed has been used extensively during the Phase 1 of the project as described in D3.1, where the methodology has been to perform an initial integration of 3rd party RAN components with the 5GC components of the consortium or implementation technologies such as Openshift or Kubernetes before replicating the deployment into actual trial sites or the NoW.

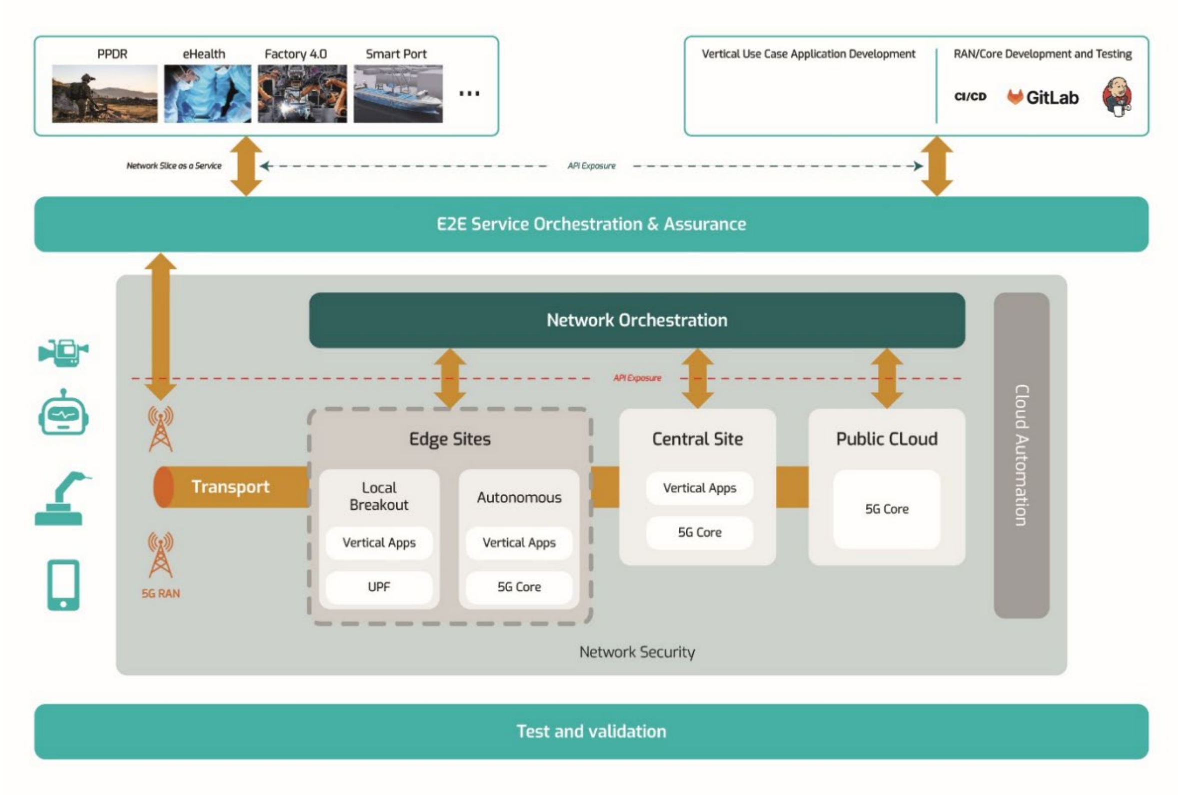


Figure 8: High level description of Telenor's Fornebu infrastructure

Radio Infrastructure and Devices: The Fornebu site is equipped with an outdoor Huawei gNB as part of the experimental testbed with configuration information detailed below in Table 1. For FUDGE-5G Use Case integration, a Nokia node has been used preliminary to evaluate the correct behavior for the Virtual Office and the Industry 4.0, more information is shown in their respective sections.

Table 1: Telenor outdoor radio parameters

NR DU Cell ID	Duplex Mode	Physical Cell ID	Frequency band	NARFCN	Spectrum	Bandwidth	Subcarrier spacing	Transmit Power (0.1 dBm)	Transmit and Receive Mode
401	TDD	401	N77	638134	3300 to 4200 MHz	40 MHz	30 KHz	349	64 Tx and 64 Rx
501	TDD	501	N78	623334	3300 to 3800 MHz	80 MHz	30 KHz	320	64 Tx and 64 Rx

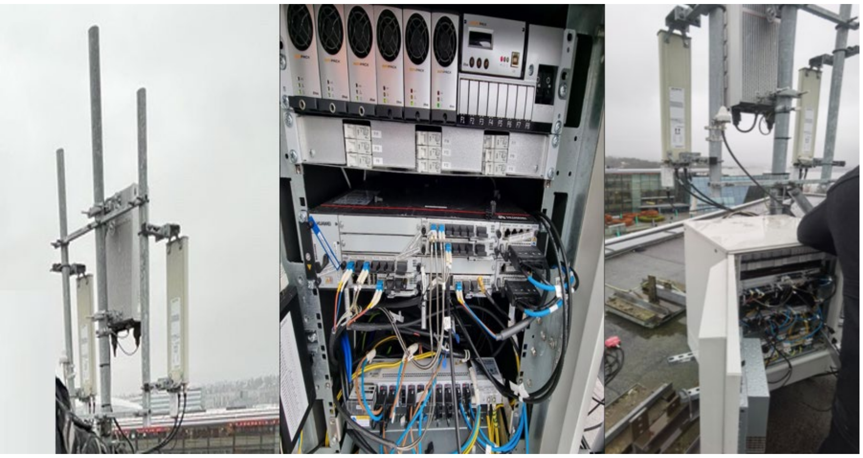


Figure 9: Telenor Research facility radio site at Fornebu.

Core Network: the experimental and cloud-native 5G core network solution is compliant with 3GPP 5GC service-based architecture and contains all the fundamental independent, reusable, and independent 5G core network functions. In the scope of the project, several 5GCs, in form of software binaries or physical boxes have been integrated in Fornebu laboratory, before being moved into other nodes.

Cloud, Edge Computing Resources: virtualization platform based on Red Hat OpenShift Container Platform which can host both VNF's and CNF's. For the small form factor edge sites, Single Node OpenShift (SNO) is used. This was used to on-board Cumucore 5GC into the OpenShift platform [7].

3.2. Trial Sites

3.2.1. Network on Wheels

Fudge 5G Network on Wheels (NoW) is standalone autonomous solution to provide a 5G Network connectivity for public protection and disaster relief services. Following are key advantages and functionality of NoW.

- Coverage on demand with guaranteed QoS
- Compute at the Edge
- Fully autonomous
- Quick to deploy, simple to operate
- Possibility to connect partner's edge
- Secure and ruggedized

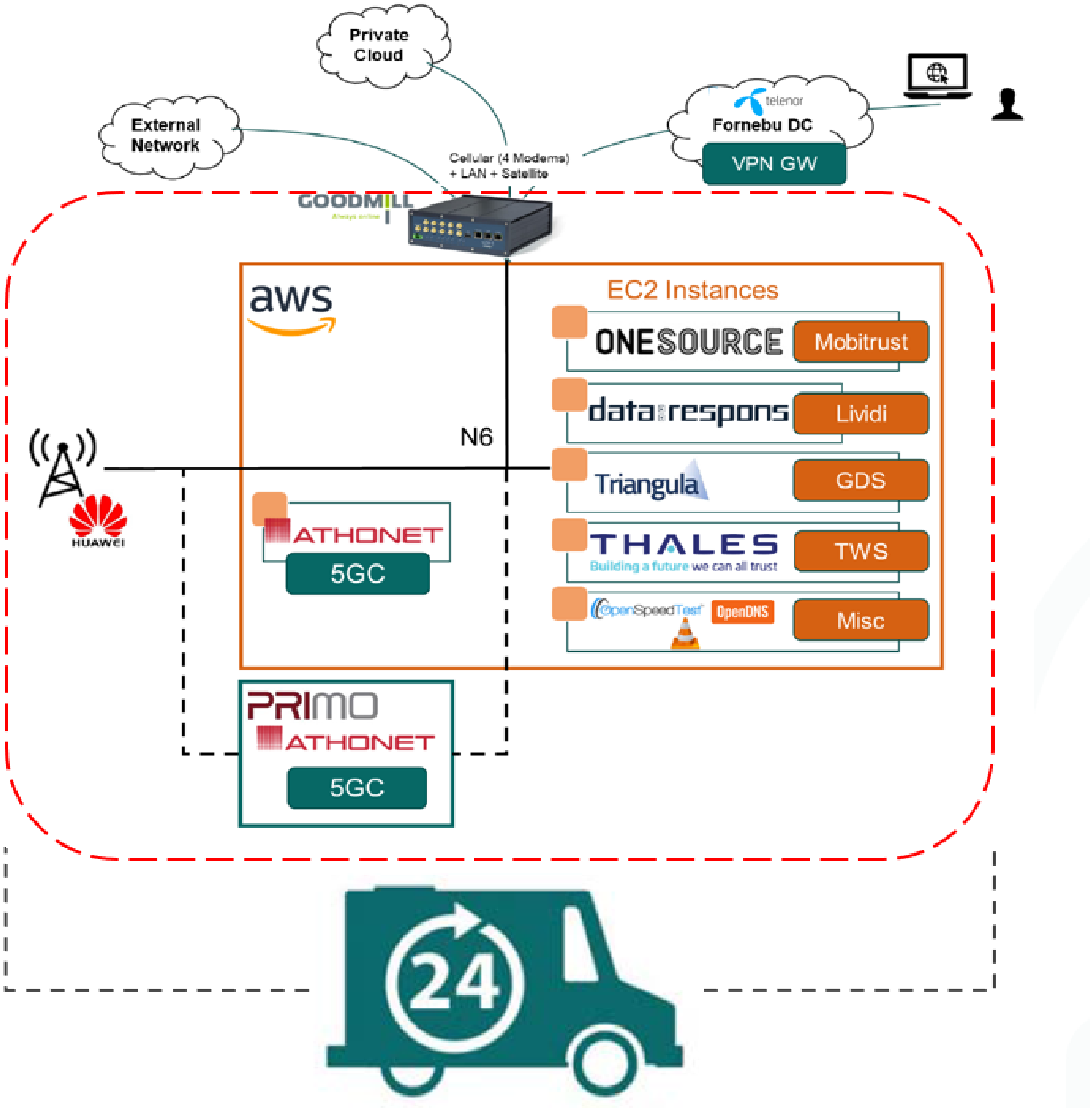


Figure 10: NoW infrastructure, 5G NR, 5G Core, and deployment of vertical applications

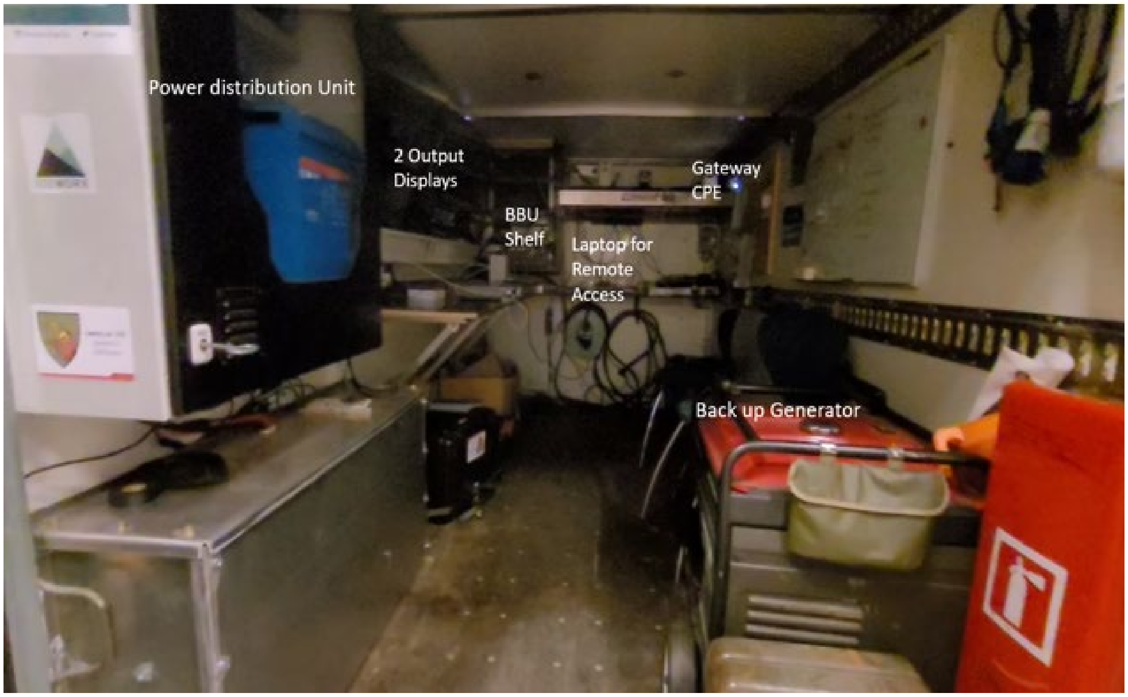


Figure 11: Equipment deployment inside the NoW and AAU shown on the mast outside

3.2.1.1. NoW infrastructure

NoW hosts the 5G NR, 5G standalone core and other applications as a one in all mobile solution that can be transported easily to different locations either for emergencies e.g in case of PPDR scenarios or can also be utilized in case of remote media production for media use cases.

Figure 10 shows the overall infrastructure of the components deployed in NoW showing 5G Radio, 5G core, switch, Goodmill gateway and vertical applications deployed in AWS Snowball edge server. Similarly, Figure 11 shows the NoW with indoor equipment and Active Antenna Unit (AAU) mounted on the mast outside.

3.2.1.2. NoW 5G Radio

Huawei is the radio equipment vendor, deployed in NoW. The radio equipment constitutes BBU model DSB 5900 inside NoW as shown in Figure 12 and the active antenna unit (AAU), model AAU5636 3400 MHz & AAU5649 3600 MHz deployed on a radio mast outside network on wheels as shown in Figure 13.

Figure 12: BBU inside the NoW.

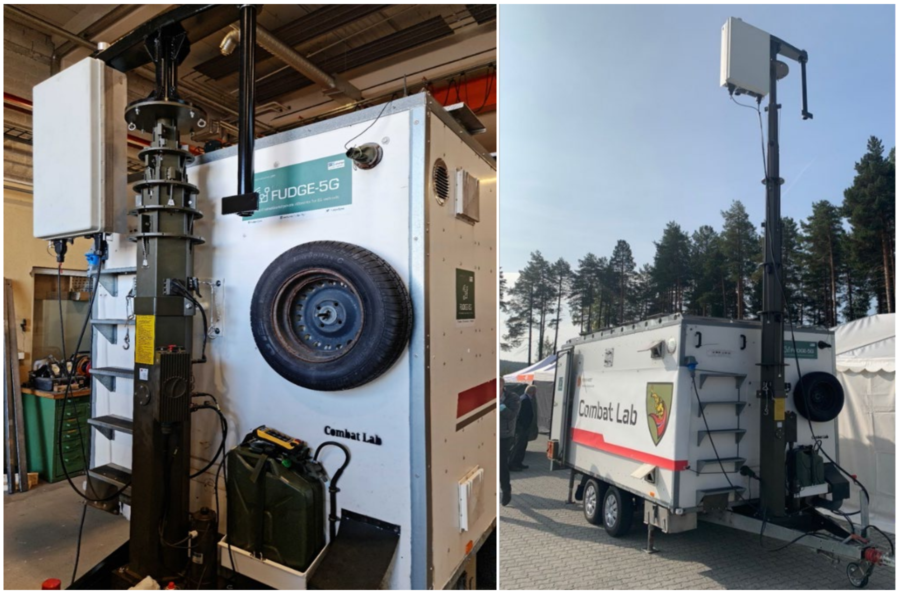


Figure 13: Huawei AAU mounted on the NOW mast in retracted and deployed position.

The radio parameters of the NoW can be found in the table below.

Table 2: Radio Parameters for the BBU and AAU

NR DU Cell ID	Duplex Mode	Physical Cell ID	Frequency band	NARFCN	Bandwidth	Subcarrier spacing	Transmit Power (0.1 dBm)	Transmit and Receive Mode
10	TDD	10	n78	638112	40 MHz	30 KHz	100	64 Tx and 64 Rx

11	TDD	11	n77	623334	100 MHz	30 KHz	100	64 Tx and 64 Rx

3.2.1.3. 5G Core

The 5G core solution for NoW is provided by Athonet as a software solution running ruggedized server with minimum footprint (PriMo solution) and also Athonet’s core is deployed on an AWS Snowball Edge hardware.

3.2.1.4. Vertical applications Integration

In addition to the Athonet core, the AWS Snowball Edge hardware is also deployed in NoW to hosts different vertical applications. Initially, an EC2 Linux instance including a handful of testing and troubleshooting tools –including an iperf, an open speed test, a VLC, and DNS (Domain Name Service) servers – was deployed on the AWS Snowball Edge server. Along with these testing applications, the other applications that are used to test the UC are ONE source Mobitrust Situational Awareness platform and a Gunshot Detection (Triangula) application. The traffic towards the backhaul is routed by a resilient router provided by Goodmill System. Initially these applications were deployed on AWS SNO, however later these applications were also deployed on second rugged Athonet PriMo solution with minimum footprint. In addition to that Nemergent MCx PTT application has also been added in the last phase of the project in collaboration with Affordable5G project [1].

3.2.2. Industry 4.0 Node

The infrastructure integration for the Industry 4.0 use case has been done in two steps. First, all needed components were deployed and tested together in Telenor premises in Oslo. After several iterations, and once all components were working as expected, the second step consisted in moving them to ABB lab, also located in Oslo. Figure 14 shows both locations where this integration work happened.

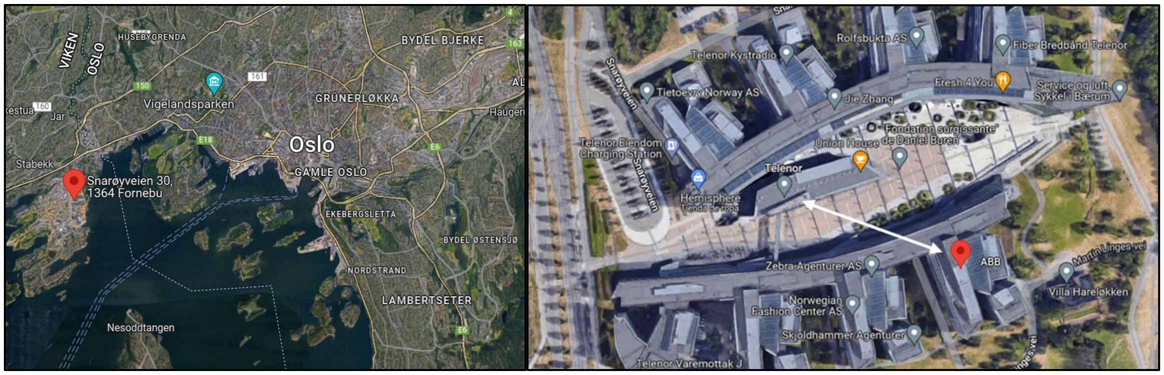


Figure 14. Telenor and ABB premises location in Fornebu, Norway.

The following components were integrated in the Industry 4.0 node:

- **5G core** from Cumucore (bare-metal version first, 5GC on FUDGE platform later): integrating 5GLAN functionality (TSN was also tested but in Cumucore premises in Finland, not included as part of the final trial).
- **5G radio infrastructure** from Nokia: BBU, Hub and radio dots, provided and integrated by Telenor.
- **5G devices** from Fivecomm: first device integrated in Telenor and moved to ABB, second device integrated in ABB directly. Additional 5G CPEs were also available.

3.2.2.1. 5G network integration in Telenor

For the first integration step in Telenor premises, the involved partners faced some interoperability issues between the 5GC and Nokia radio equipment. Intensive work by the partners (Cumucore, Telenor, Fivecomm and Nokia as external support) was done in order to solve this problem. The setup used for this use case is similar to the one deployed for the hospital use case. Figure 15 shows the 5G components, deployed in Telenor premises.

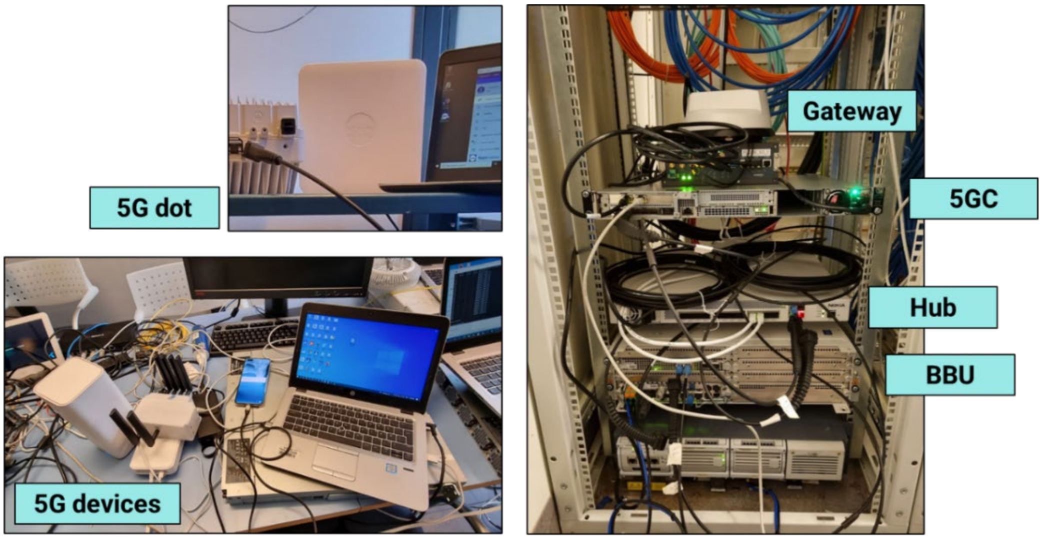


Figure 15. 5G components (5G core, radio and devices) deployed at Telenor premises.

After their successful integration, such components were validated by doing end-to-end 5G network measurements, in terms of latency and throughput. The results are reported in D4.2 as part of the validation work.

3.2.2.2. 5G network integration in ABB

The next natural step was to move the equipment to ABB. Figure 16 shows the equipment in their laboratory. On the top left side, the 5G dot used is shown. On the bottom left side, the figure shows the radio and core components, which were later placed in the rack showed in the right side of the figure.

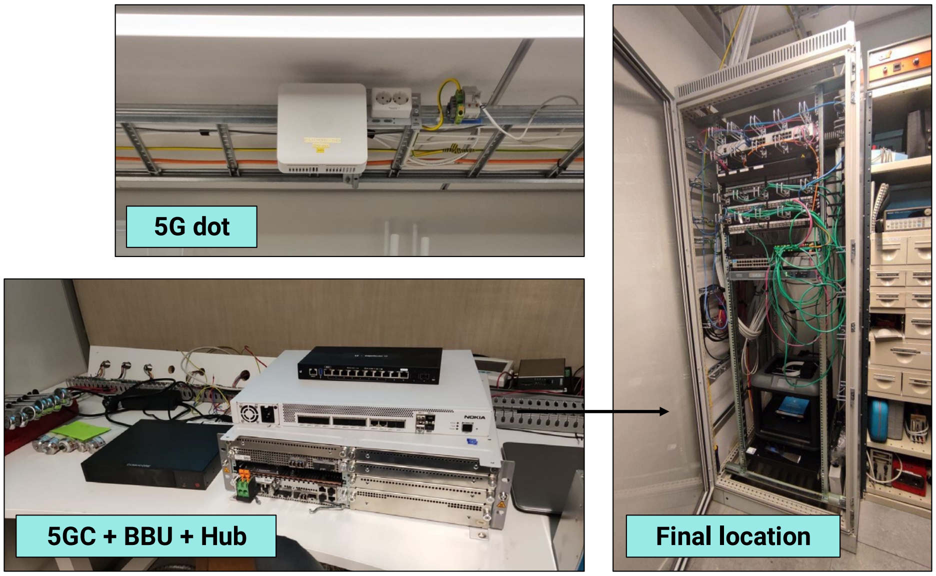


Figure 16. 5G components (5G core, radio and devices) deployed at ABB lab.

Once all these components were integrated and deployed in ABB, they were additionally validated in preliminary tests performed in November 22. Such measurements used different configurations and topologies, depending on the KPI to be validated. Figure 17 shows the end-to-end architecture used for measuring the one-way latency KPI. Results obtained in ABB for the components' validation are reported in D4.2. After such validation, the integration was considered done. Final end-to-end test cases are reported in D4.3.

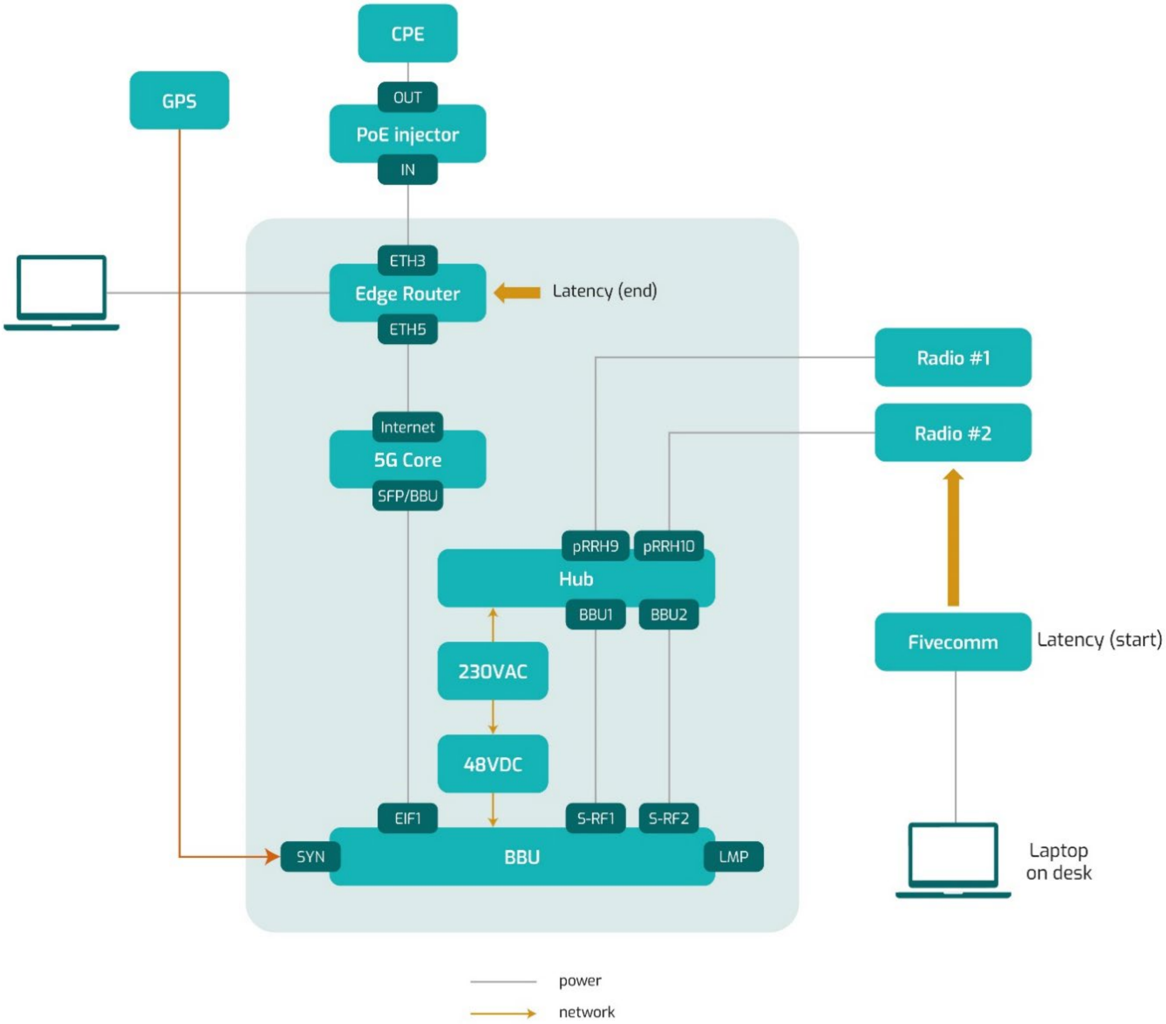


Figure 17: End-to-end architecture deployed in ABB premises for the final trials (one possible setup, more have been tested).

3.2.3. Hospital Node

A hospital node supports UC3 – 5G virtual office. The node provides secure access to a specific set of corporate services, in that case, a hospital environment where doctors, nurses, paramedic staff monitor patients by using different sensors connected to patients broadcasting securely over 5G and presented in a dashboard.

As like traditional 5G network, the hospital node hosts the private network, including the 5G NR, 5G core and similarly vertical applications all deployed in the edge server to provide different corporate services. Figure 18 shows the high-level diagram overview of infrastructure deployed in the Hospital whereas Figure 19 showcases the actual physical setup.

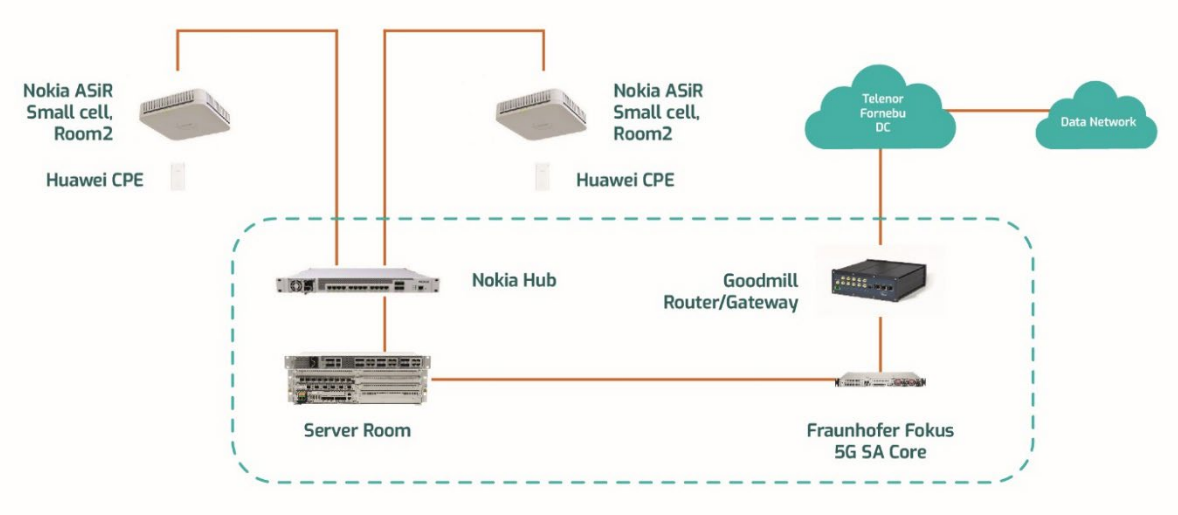


Figure 18: 5G private network Infrastructure deployed in Hospital

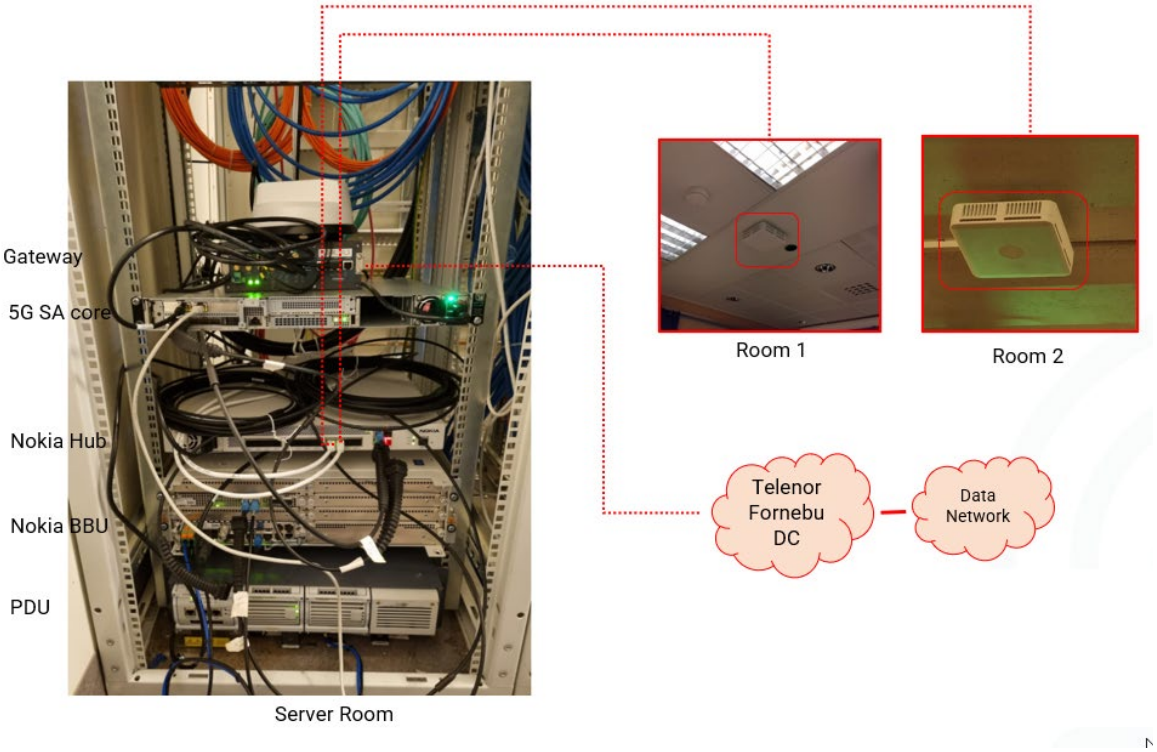


Figure 19: Actual deployment of 5G private network Infrastructure deployed in Hospital

3.2.3.1. 5G NR

In hospital node, Nokia was used to provide the indoor 5G private network solution. The Nokia Airscale System module consists of following key components:

- NOKIA BBU: contains 2 cards, capacity card connected to the Nokia Hub and transmission card connected to the 5G core directly.
- NOKIA HUB is utilized to aggregate the traffic from different pico cells and forward it to the BBU. In total traffic from 12 picos can be aggregated.
- NOKIA ASiR picocells are the indoor remote radio head units to provide the coverage in different hospital rooms.

The Table 3 shows the 5G radio parameters configured in the hospital node.

Table 3: 5G Radio parameters of the Nokia gNB.

NR DU Cell ID	Duplex Mode	Physical Cell ID	Frequency band	NARFCN	Frequency	Bandwidth	Subcarrier spacing	Transmit Power (dBm)	Transmit and Receive Mode
1	TDD	1	n78	622668	3340.02 MHz	80 MHz	30 KHz	23	4 Tx and 4 Rx

3.2.3.2. 5G Core

In hospital node, the Open5Gcore is provided by Fraunhofer FOKUS deployed on bare metal HPE DL110 telco server. The telco server hosts both 5G core and the OneSource's Mobi-trust vertical application. The server is connected to a BBU via a single mode optical fiber cable. Similarly, to provide the Internet access the server is connected to Goodmill router equipped with commercial Telenor SIM card which is connected via VPN solution to the to the Telenor's Fornebu data centre.

3.2.3.3. Vertical application hardware

Integrated in the Hospital Node, the User Equipment (UE) is part of the hardware developed by OneSource. This device consists of a single-board computer coupled with custom PCBs that include a microprocessor, a Telit FN980 5G modem and batteries for operation without mains power. It acts as an interface between the multiple sensors with different communication technologies (serial, Bluetooth, Wi-Fi, etc.) used in the 5G Virtual Office UC and the 5G NPN that relays the communication to the Vertical Application. Figure 20 shows the end user devices.

Figure 20: OneSource End-User devices.

3.2.4. Interconnected NPNs Nodes

The interconnected NPNs nodes builds on the setup described in D3.1 [8]; where the three nodes are geographically located apart. In detail, UPV premises in Valencia, the Oslo Hospital in Norway, and the Fraunhofer FOKUS Berlin offices form the INPN deployment. The three locations are connected via Wireguard. A high-level design of the three interconnected nodes are shown in Figure 21.

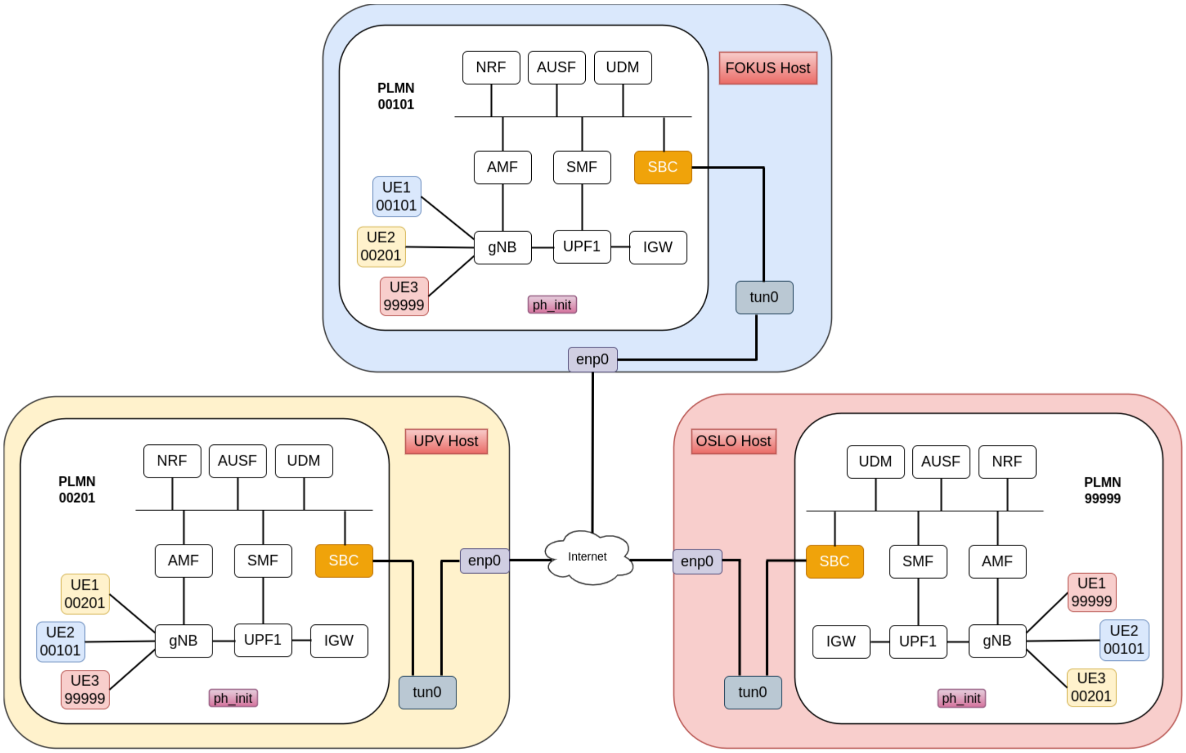


Figure 21: INPNs nodes deployed for the INPNs use case, without the platform on-boarding.

3.2.4.1. 5G Core and NG-RAN

The core deployed at these locations is a modified version of the FOKUS Open5GCore, which features the SBC, a component previously documented in D1.3 [9] and D2.5 [10]. The deployment running in these locations follows a centralized 5G Core where all required NFs are running over the same physical resources; in order to ease the configuration. The three edges are running the same components, the only difference is the radio and device equipment from each node and the PLMN configured in each site. In FOKUS, the PLMN is 00101 and the radio is an Amarisoft gNB. In UPV, the PLMN is 00201 and the gNB is provided by Amarisoft. Last, the hospital has a PLMN of 99999 and radios provided by Nokia. The devices in these nodes are both virtualized, using UERANSIM or FOKUS Benchmarking Tool and physical ones, such as the ZTE and Huawei CPEs. More information of the tests carried out using this setup can be found in upcoming D4.3.

3.3. Multi-Site Infrastructure for eSBA Platform

FUDGE-5G follows a Platform-as-a-Service (PaaS) proposition to offer service routing, location-aware orchestration and monitoring as a unified SBA platform across many trial sites. To demonstrate this proposition and derive KPIs and deployment insights across FUDGE-5G use cases, the consortium agreed to deploy a single platform across a sub-set of use cases. Figure 22 illustrates the four locations that are interconnected via two separate Virtual Private Networks (VPNs):

- L2 VPN: This VPN is hosted in London and allows the routing component of the platform, aka the Service Communication Proxy (SCP), to delivery packets among Enterprise Services.
- L3 VPN: This VPN is hosted in Berlin and allows the routing of user plane traffic between UPFs (N6 and N9).

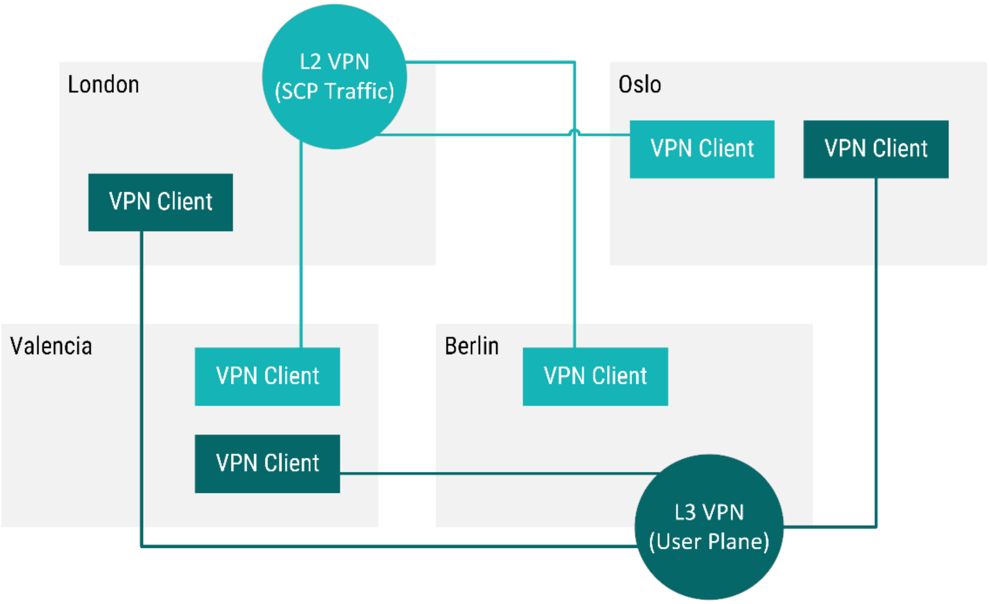


Figure 22: Multi-Site Infrastructure for eSBA Platform

Each site illustrated in the figure above offers the ability to deploy Virtual Machines (VMs) via Kernel Virtual Machine (KVM). The VMs deployed at each site comprise the FUDGE-5G platform with the control entities for routing, orchestration and monitoring located in London. Furthermore, as illustrated in Figure 23, each of the other sites host five VMs and have a physical gNB attached to the SCP (denoted as $SP_{<LOCATION>-gNB}$). The L2 VPN offers direct LAN-like communication among all OVS VMs of each site. The OVS VM at each site then connects on a dedicated port to a Service Proxy (SP) VM. Each site also hosts two Service Host (SH) VMs with one allowing to host the UPF and the other all other NFs. The reason for the separated SH for UPFs is the network requirements of UPFs (more info can be found in D2.5 [14]).

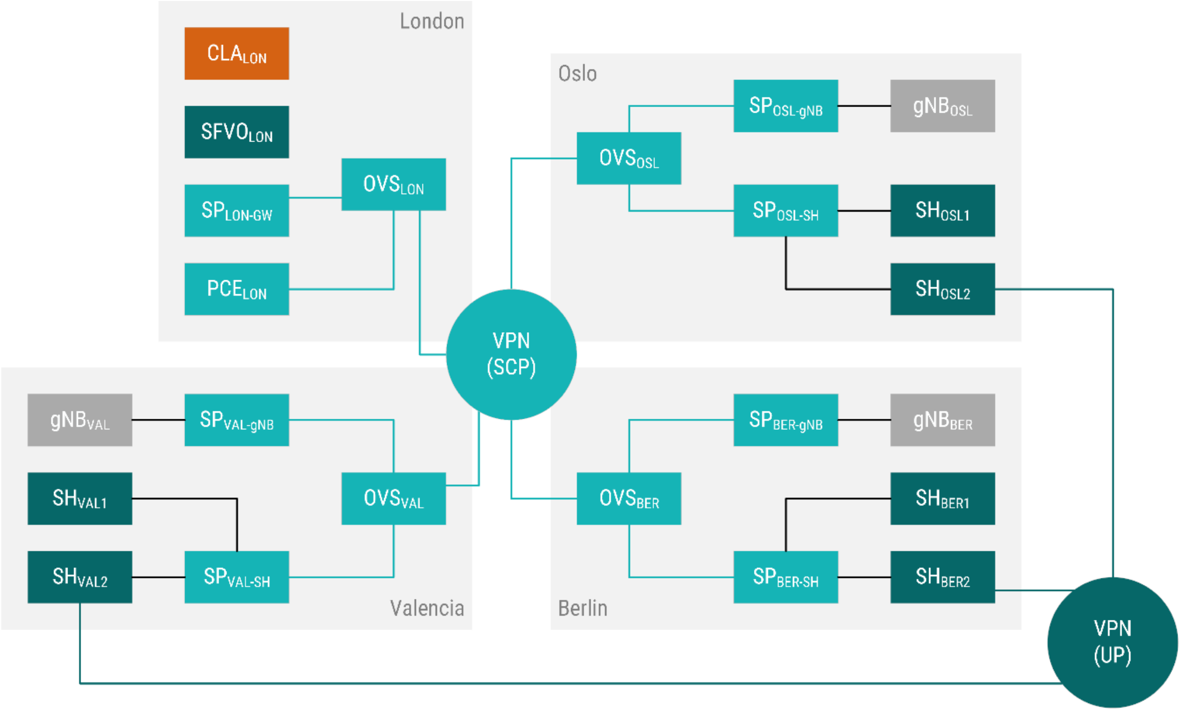


Figure 23: Logical eSBA Deployment Across all Four Sites.

4. Integration with eSBA platform

FUDGE-5G eSBA platform has on-boarded several consortium components during the project duration, including three 5GCs and Ubitech Vertical Application Orchestrator (VAO). The on-boarding process is detailed in subsequent sections.

4.1. FOKUS O5GC

4.1.1. Packaging automation

The packaging of the containers that implement the Open5GCore Network Functions has been fully automated with a bash script that creates LXC containers, copies the necessary files and configures the containers. Once the containers are created, they can be exported and used in the FUDGE-5G SBI Platform.

4.1.2. Configuration files and FQDNs

The SBI Platform exposes the FQDN of the containers using the WHOAMI service and setting up environmental variables that be used by the program that implements the Network Function.

The Open5GCore needs to be configured with IPs or FQDNs in the configuration files. The IPs can come from environmental variables in the configuration files, but the FQDNs can't come from environmental variables. This is because they use a special syntax for the FQDNs, so the Open5GCore cannot execute this correctly:

```
      "addr": "ipv4#%WHOAMI_SFIDS"
```

To solve this issue, we needed to expand the variables before executing the Open5GCore binaries, so every time the container starts, a new configuration file is created from a template, and the resulting file is given to the Open5GCore binary.

Once the issue is solved, we can use the following syntax in the template to resolve our own FQDN:

```
      "addr": "ipv4#%WHOAMI_SFIDS",
```

To resolve the FQDN of other Network Functions we use this:

```
    "ipv4#<network_function>.%WHOAMI_DOMAIN"
```

where network_function is the Network Function that we want to resolve (for instance, NRF or AMF).

4.1.3. Waiting for dependencies

By default, the Open5GCore Network Functions fail if they cannot access other services they depend on (such as the SQL database or the NRF). To solve this issue, we need to wait until the FQDN of the service is resolvable and check that the socket that is used to access the service is available. This is implemented in the systemd service file used to start the Open5GCore binary.

4.1.4. Data path issues

Once the core was packaged, there were some issues in data path communication. For this we have to update the packaging script to expose correct IP's which fixed the issue and we were able to setup the complete authentication and data path from a UE.

4.2. Cumucore 5GC

The Cumucore 5GC network functions (NFs) were deployed as containers. Docker images of the network functions were created and pushed to a registry that can be accessed in any location, in this case docker hub. The docker images of the NFs were modified to support Fully Qualified Domain Names (FQDN) to suit the Interdigital virtualization platform. With the docker images present in docker hub, the 5GC NFs docker images were pulled and deployed on the platform. Each NF after deployment runs a container and is able to communicate with other running NFs using their FQDN on the platform. The NFs running as containers cannot be accessed from outside providing some form of security to the 5GC. Testing of the 5GC was carried out in the Interdigital premises in London.

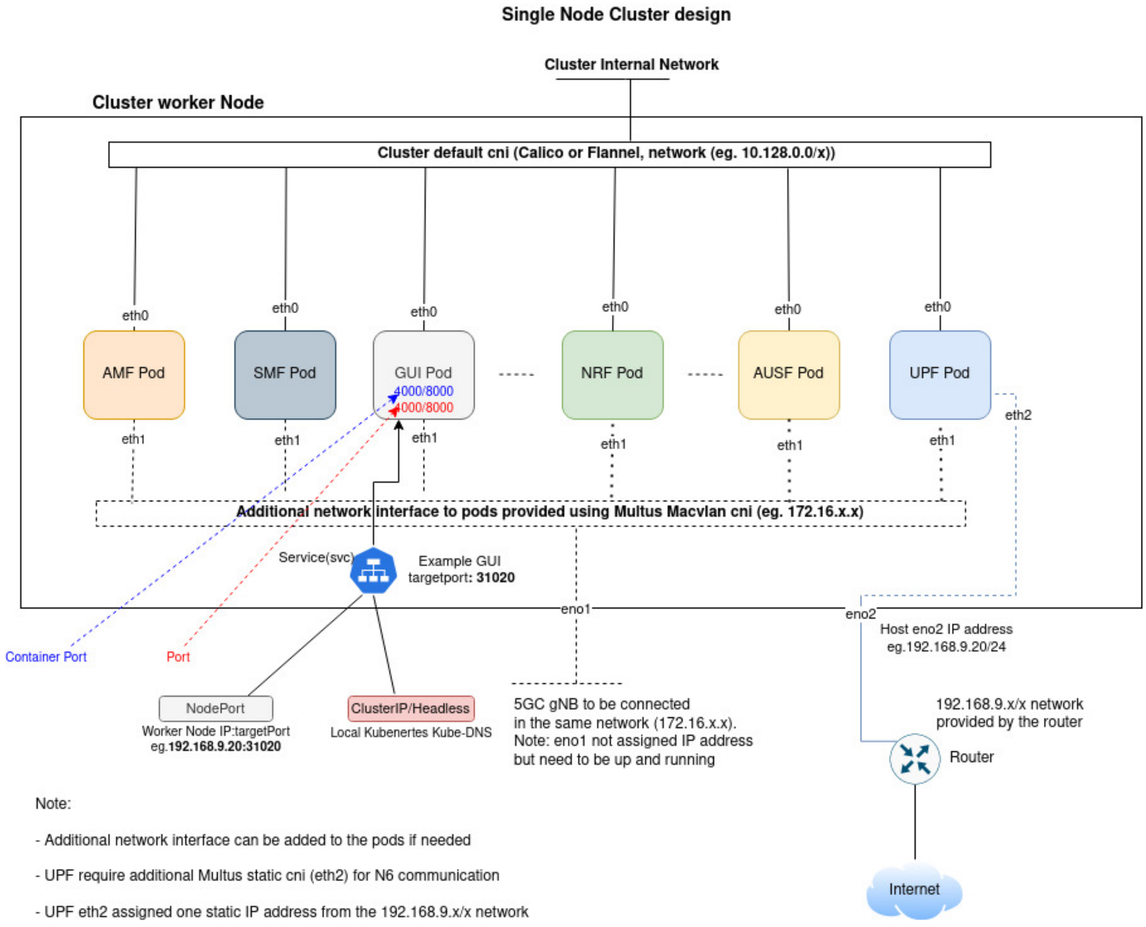

Single Node Cluster design
Cluster Internal Network
Cluster worker Node
Cluster default cni (Calico or Flannel, network (eg. 10.128.0.0/x))
eth0
eth0
eth0
eth0
eth0
eth0
AMF Pod
SMF Pod
GUI Pod
4000/8000
4000/8000
NRF Pod
AUSF Pod
UPF Pod
eth2
eth1
eth1
eth1
eth1
eth1
eth1
Additional network interface to pods provided using Multus Macvlan cni (eg. 172.16.x.x)
Service(svc)
Example GUI
targetport: 31020
eno1
eno2
Host eno2 IP address
eg.192.168.9.20/24
Container Port
Port
NodePort
Worker Node IP:targetPort
eg.192.168.9.20:31020
ClusterIP/Headless
Local Kubenertes Kube-DNS
5GC gNB to be connected
in the same network (172.16.x.x).
Note: eno1 not assigned IP address
but need to be up and running
192.168.9.x/x network
provided by the router
Router
Internet
Note:
- Additional network interface can be added to the pods if needed
- UPF require additional Multus static cni (eth2) for N6 communication
- UPF eth2 assigned one static IP address from the 192.168.9.x/x network

Figure 24: Cumucore cluster structure deployed in London Testbed.

Testing of Cumucore 5GC on Interdigital platform was carried out in Interdigital premises in London. Test set-up is shown in Figure 24.

4.3. Athonet 5GC

Athonet makes available its 5GC solution on the AWS public cloud for integration with technology partners requesting for a simple and quick way to interwork with its core network components. Such solution, represented in Figure 25, includes the full set of core network components, which can directly connect to gNBs of the RAN deployed locally at the customer/partner's premises via simple Internet connectivity, protected by VPN. Thanks to the modularization of the core, the same cloudified solution can be split between control- and user-plane components to allow the integration of the counterpart's components by any technology partner.

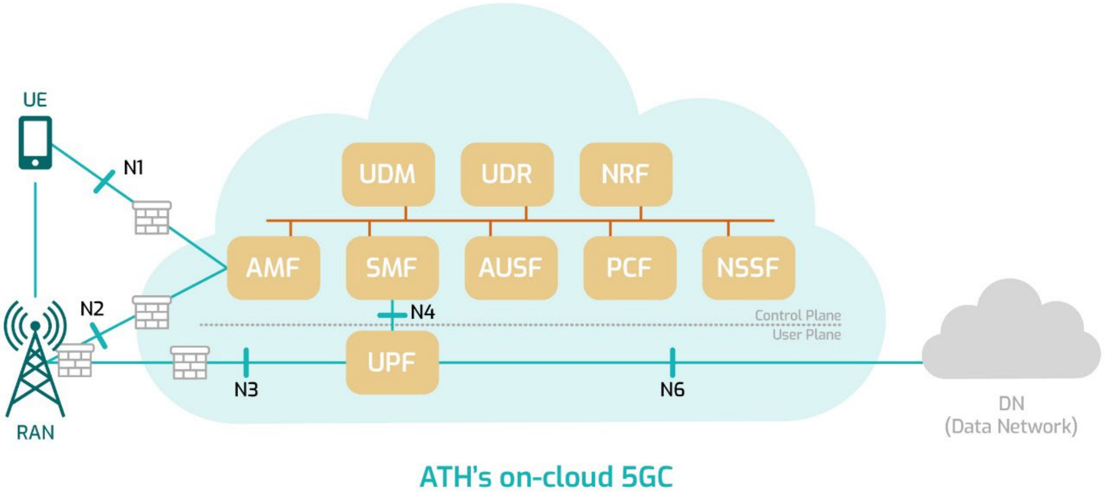


Figure 25: On-cloud 5GC integrated with on-premise RAN equipment.

To integrate the gNB available in the London integration testbed, ATH provided a VPN connection into a public cloud where their 5GC is deployed. The VPN connection was established directly on the gNB of the integration testbed. By configuring the AMF (N2) and GTP endpoint (N3), the gNB was able to attach to the AMF directly. The other information that had to be manually configured were the TAC (100), PLMN (00101) and NASSAI (SST=1, SD=00001). A 5G Quectel modem RM500Q-GL was used to verify the 5G network by attaching and establishing an IP PDU session. ICMP and standard web traffic towards the internet was used to verify the deployment.

4.4. Ubitech VAO

Ubitech have successfully integrated the Vertical Application Orchestrator with the SBA Platform over London's Testbed. The VAO is the entry point for the service providers to onboard and manage the vertical applications. The deployed version of the VAO is comprised by 14 micro services as it can be seen in Figure 26.

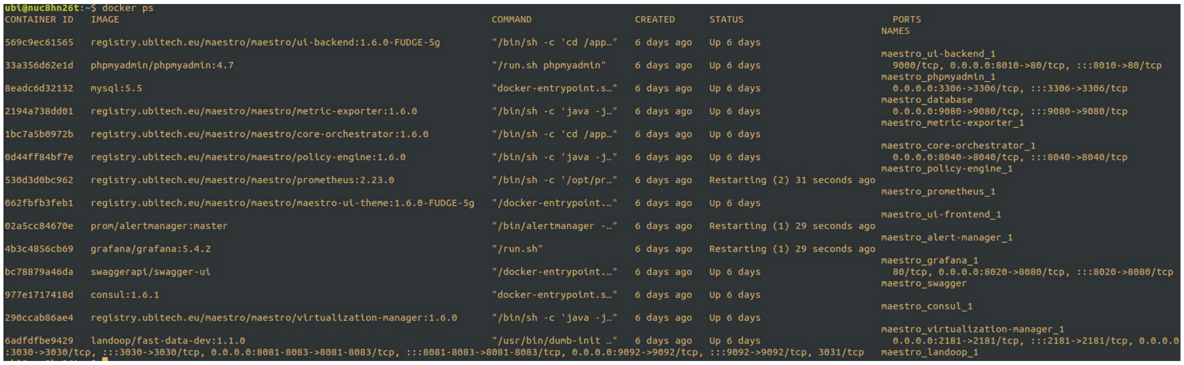
The connectivity requirements for the VAO are three interfaces. One interface with the management network for the signaling between the VAO and the Kubernetes cluster. Another interface is needed with the data network in order for the vertical components of the application to communicate with each other. The third interface bridges the deployed vertical service with the 5GC through the AF.

4.4.1. VAO Prerequisites

It is important to note that the VAO has been tested in the IDE's environment with the following characteristics:

- VM Instance with Ubuntu Server 20.04
- JAVA JDK 1.11.0_56
- Apache Maven 3.8.6
- Git 2.38
- Node.js 16.13
- Docker 20.10.21
- Docker Compose 1.27.4

In addition, as Figure 26 shows VAO requires and deploys MariaDB v5.5 and Kafka v3.3.2 which is wrapped with landoop.



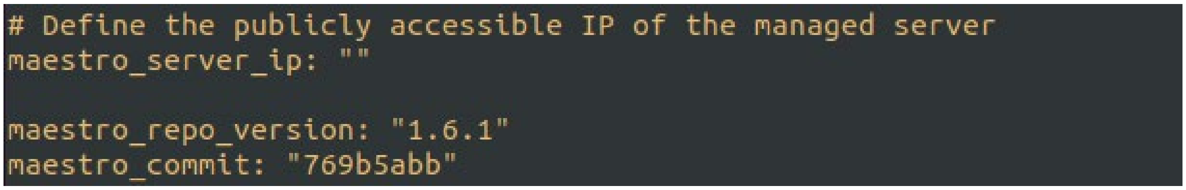
```
ubi@nuc8hn26t:~$ docker ps
CONTAINER ID   IMAGE                                                              COMMAND                   CREATED      STATUS                          PORTS
                                                                                                                                                              NAMES
569c9ec61565   registry.ubitech.eu/maestro/maestro/ui-backend:1.6.0-FUDGE-5g      "/bin/sh -c 'cd /app…"   6 days ago   Up 6 days
                                                                                                                                                              maestro_ui-backend_1
33a356d62e1d   phpmyadmin/phpmyadmin:4.7                                          "/run.sh phpmyadmin"      6 days ago   Up 6 days                         9000/tcp, 0.0.0.0:8010->80/tcp, :::8010->80/tcp
                                                                                                                                                              maestro_phpmyadmin_1
8eadc6d32132   mysql:5.5                                                          "docker-entrypoint.s…"   6 days ago   Up 6 days                         0.0.0.0:3306->3306/tcp, :::3306->3306/tcp
                                                                                                                                                              maestro_database
2194a738dd01   registry.ubitech.eu/maestro/maestro/metric-exporter:1.6.0          "/bin/sh -c 'java -j…"   6 days ago   Up 6 days                         0.0.0.0:9080->9080/tcp, :::9080->9080/tcp
                                                                                                                                                              maestro_metric-exporter_1
1bc7a5b0972b   registry.ubitech.eu/maestro/maestro/core-orchestrator:1.6.0        "/bin/sh -c 'cd /app…"   6 days ago   Up 6 days

                                                                                                                                                              maestro_core-orchestrator_1
0d44ff84bf7e   registry.ubitech.eu/maestro/maestro/policy-engine:1.6.0            "/bin/sh -c 'java -j…"   6 days ago   Up 6 days                         0.0.0.0:8040->8040/tcp, :::8040->8040/tcp
                                                                                                                                                              maestro_policy-engine_1
530d3d0bc962   registry.ubitech.eu/maestro/maestro/prometheus:2.23.0              "/bin/sh -c '/opt/pr…"   6 days ago   Restarting (2) 31 seconds ago
                                                                                                                                                              maestro_prometheus_1
062fbfb3feb1   registry.ubitech.eu/maestro/maestro/maestro-ui-theme:1.6.0-FUDGE-5g   "/docker-entrypoint.…"   6 days ago   Up 6 days
                                                                                                                                                              maestro_ui-frontend_1
02a5cc84670e   prom/alertmanager:master                                           "/bin/alertmanager -…"   6 days ago   Restarting (1) 29 seconds ago
                                                                                                                                                              maestro_alert-manager_1
4b3c4856cb69   grafana/grafana:5.4.2                                              "/run.sh"                 6 days ago   Restarting (1) 29 seconds ago
                                                                                                                                                              maestro_grafana_1
bc78879a46da   swaggerapi/swagger-ui                                              "/docker-entrypoint.…"   6 days ago   Up 6 days                         80/tcp, 0.0.0.0:8020->8080/tcp, :::8020->8080/tcp
                                                                                                                                                              maestro_swagger
977e1717418d   consul:1.6.1                                                       "docker-entrypoint.s…"   6 days ago   Up 6 days
                                                                                                                                                              maestro_consul_1
290ccab86ae4   registry.ubitech.eu/maestro/maestro/virtualization-manager:1.6.0   "/bin/sh -c 'java -j…"   6 days ago   Up 6 days
                                                                                                                                                              maestro_virtualization-manager_1
6adfdfbe9429   landoop/fast-data-dev:1.1.0                                        "/usr/bin/dumb-init …"   6 days ago   Up 6 days                         0.0.0.0:2181->2181/tcp, :::2181->2181/tcp, 0.0.0.0
:3030->3030/tcp, :::3030->3030/tcp, 0.0.0.0:8081-8083->8081-8083/tcp, :::8081-8083->8081-8083/tcp, 0.0.0.0:9092->9092/tcp, :::9092->9092/tcp, 3031/tcp   maestro_landoop_1
```

Figure 26: VAO deployed microservices over London Testbed

4.4.2. Deployment of the VAO with Continuous Integration

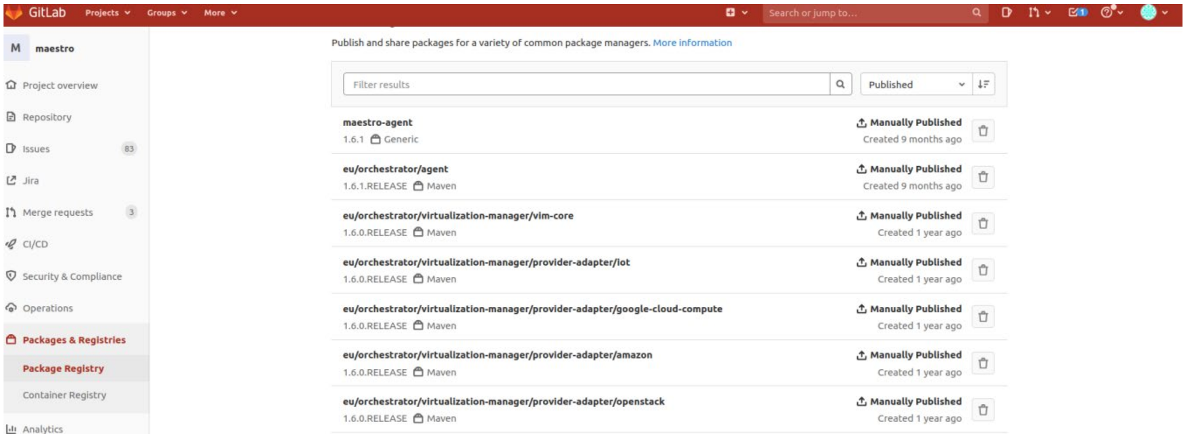
The deployment of VAO is based on a Continuous Integration process. Specifically, the whole deployment process is automated except one basic manual step. The manual intervention is the starting point which requires by the person who performs the deployment to specify the specific release of the code and the involved artifacts/microservices (Figure 27, Figure 28). After that githooks are configured to fetch the specified artifacts and start the Automated Build through ansible playbooks.



```
# Define the publicly accessible IP of the managed server
maestro_server_ip: ""

maestro_repo_version: "1.6.1"
maestro_commit: "769b5abb"
```

Figure 27: Specifying the code commit and the release for automatic deployment through Gitlab.



Publish and share packages for a variety of common package managers. More information

maestro-agent
1.6.1 Generic
Manually Published
Created 9 months ago

eu/orchestrator/agent
1.6.1.RELEASE Maven
Manually Published
Created 9 months ago

eu/orchestrator/virtualization-manager/vim-core
1.6.0.RELEASE Maven
Manually Published
Created 1 year ago

eu/orchestrator/virtualization-manager/provider-adapter/iot
1.6.0.RELEASE Maven
Manually Published
Created 1 year ago

eu/orchestrator/virtualization-manager/provider-adapter/google-cloud-compute
1.6.0.RELEASE Maven
Manually Published
Created 1 year ago

eu/orchestrator/virtualization-manager/provider-adapter/amazon
1.6.0.RELEASE Maven
Manually Published
Created 1 year ago

eu/orchestrator/virtualization-manager/provider-adapter/openstack
1.6.0.RELEASE Maven
Manually Published
Created 1 year ago

Figure 28: Gitlab Artifacts

5. Integration of Vertical Applications

Regarding the Vertical Applications integration, two different apps have been on-boarded into FUDGE-5G nodes and components. Inside the consortium, Onesource has provided their Remote Monitoring application, which has been integrated into the 5G System and trialed in the Virtual Office. The other application was provided by Nemergent and part of a cross-project collaboration between Affordable5G and FUDGE-5G. They are detailed below.

5.1. Nemergent MCX

Nemergent PTT MCX [11] is a popular push-to-talk solution that can be integrated into 5G standalone cores as an additional service. This solution provides a wide range of features that are designed to enhance communication in industries such as transportation, construction, and logistics. Some of the key features of Nemergent PTT MCX include:

- Support for multiple users: Nemergent PTT MCX supports a large number of users, making it ideal for organizations with many employees or team members.
- Group communication: With Nemergent PTT MCX, users can be organized into groups, allowing for easy communication between team members.
- Instant call initiation: Users can initiate a call with just one button press, providing fast and efficient communication.
- Location tracking: Nemergent PTT MCX provides location tracking of users, which can be useful for organizations that need to keep track of the whereabouts of their employees or team members.
- Interoperability: Nemergent PTT MCX is interoperable with other communication systems such as DMR, Tetra and other traditional PTT systems, this allows your organization to upgrade gradually and to keep using your legacy communication systems

Nemergent PTT MCX is also easy to deploy and manage, making it a great choice for organizations that want to enhance their communication capabilities with a 5G standalone core. This solution can be integrated with other core network elements such as PCF, AMF, providing a seamless and efficient communication experience for the users.

By integrating Nemergent PTT MCX into a 5G standalone core, organizations can provide their employees and team members with fast and efficient communication capabilities, which can help to improve productivity and collaboration.

5.1.1. Deployment of the PTT application

The FUDGE-5G project aims to showcase the versatility of the service-based core architecture by integrating the Nemergent 5G PTT application into the Athonet standalone

5GC network. To achieve this, the MCX application was deployed as a virtual machine (VM) on a small server running CentosOS 7. The computational requirements for the service are substantial, with 8 virtual CPUs, 16GB RAM, and 12GB of hard disk space required.

The VM was configured with three interfaces - N5, management, and N6 - to connect to the PCF, enable management, and facilitate RTP and SIP traffic over the N6 interface. On the UE side, three APKs were deployed for the PTT client: a provisioning APK for configuring the application client, an SDK APK, and a GUI APK for the actual application interface.

Once the VM is activated and the clients are provisioned, users should be able to make both private calls and group calls. The deployment of the Nemergent 5G PTT application as an additional service in the Athonet core demonstrates the flexibility of the Fudge-5G architecture and provides a functional example of the potential for further service integrations in the future.

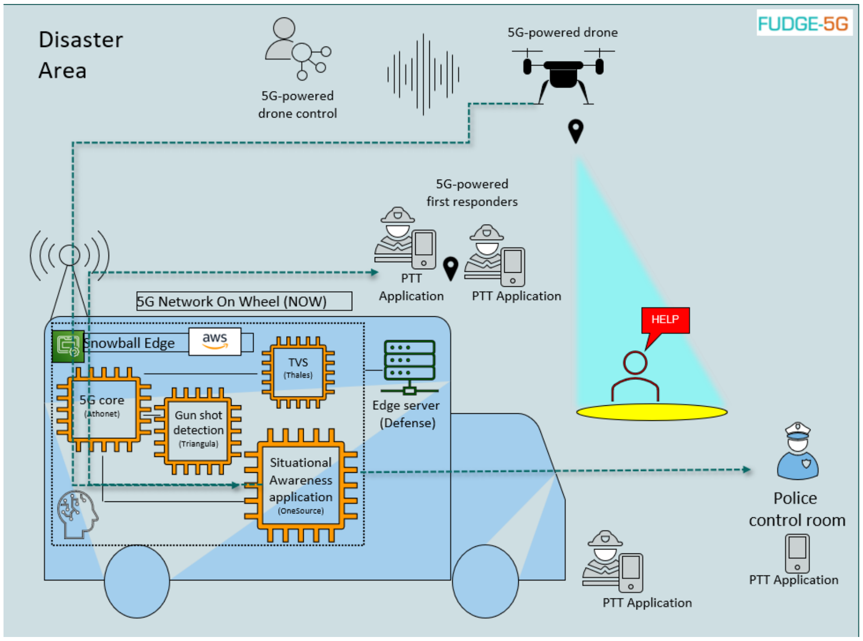
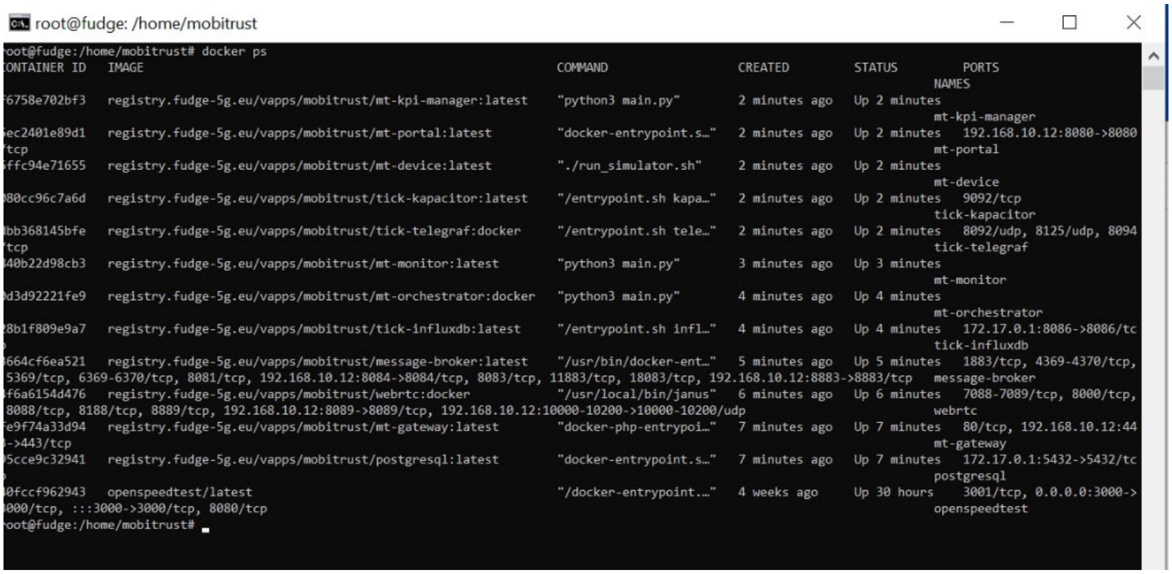


Figure 29: Nemergent components on-boarded on the NoW.

5.2. OneSource Application for remote monitoring

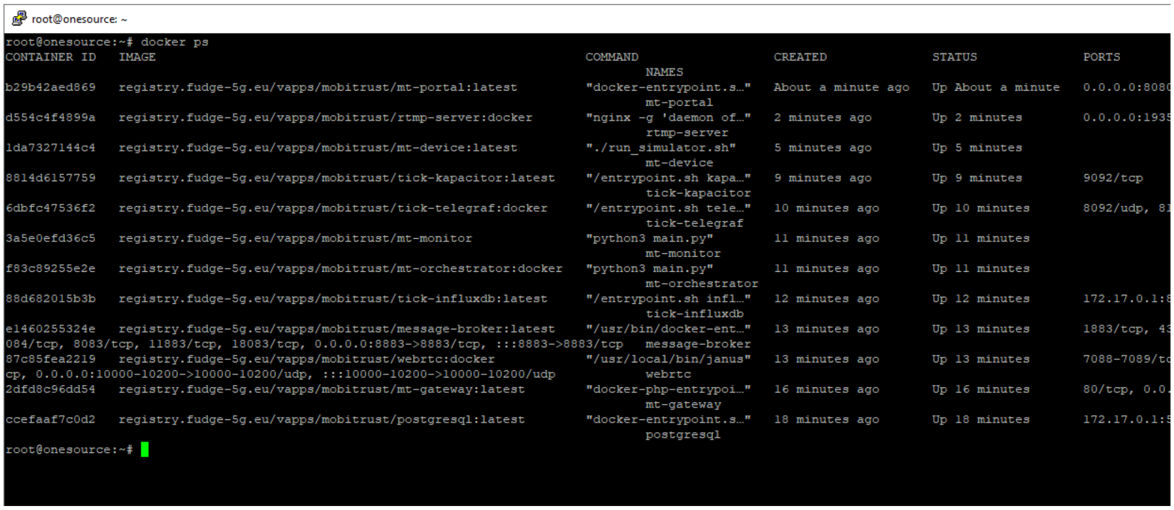
The remote monitoring application from OneSource, also known as Mobitrust, has two different variants. The application can be used both for hospital patient monitoring and for field operations in a PPDR scenario. Given both possibilities, in the context of FUDGE-5G the application was integrated with the 5G Network on Wheels for UC2 and with the 5G NPN from Oslo University Hospital for UC3.



```
root@fudge: /home/mobitrust
```

```
oot@fudge:/home/mobitrust# docker ps
ONTAINER ID   IMAGE                                                      COMMAND                  CREATED          STATUS         PORTS
                                                                                                                            NAMES
f6758e702bf3   registry.fudge-5g.eu/vapps/mobitrust/mt-kpi-manager:latest    "python3 main.py"        2 minutes ago    Up 2 minutes
                                                                                                                            mt-kpi-manager
ec2401e89d1   registry.fudge-5g.eu/vapps/mobitrust/mt-portal:latest         "docker-entrypoint.s…"   2 minutes ago    Up 2 minutes   192.168.10.12:8080->8080
/tcp                                                                                                                        mt-portal
ffc94e71655   registry.fudge-5g.eu/vapps/mobitrust/mt-device:latest         "./run_simulator.sh"     2 minutes ago    Up 2 minutes
                                                                                                                            mt-device
80cc96c7a6d   registry.fudge-5g.eu/vapps/mobitrust/tick-kapacitor:latest    "/entrypoint.sh kapa…"   2 minutes ago    Up 2 minutes   9092/tcp
                                                                                                                            tick-kapacitor
bb368145bfe   registry.fudge-5g.eu/vapps/mobitrust/tick-telegraf:docker     "/entrypoint.sh tele…"   2 minutes ago    Up 2 minutes   8092/udp, 8125/udp, 8094
/tcp                                                                                                                        tick-telegraf
40b22d98cb3   registry.fudge-5g.eu/vapps/mobitrust/mt-monitor:latest        "python3 main.py"        3 minutes ago    Up 3 minutes
                                                                                                                            mt-monitor
d3d92221fe9   registry.fudge-5g.eu/vapps/mobitrust/mt-orchestrator:docker   "python3 main.py"        4 minutes ago    Up 4 minutes
                                                                                                                            mt-orchestrator
8b1f809e9a7   registry.fudge-5g.eu/vapps/mobitrust/tick-influxdb:latest     "/entrypoint.sh infl…"   4 minutes ago    Up 4 minutes   172.17.0.1:8086->8086/tc
                                                                                                                            tick-influxdb
664cf6ea521   registry.fudge-5g.eu/vapps/mobitrust/message-broker:latest    "/usr/bin/docker-ent…"   5 minutes ago    Up 5 minutes   1883/tcp, 4369-4370/tcp,
5369/tcp, 6369-6370/tcp, 8081/tcp, 192.168.10.12:8084->8084/tcp, 8083/tcp, 11883/tcp, 18083/tcp, 192.168.10.12:8883->8883/tcp   message-broker
f6a6154d476   registry.fudge-5g.eu/vapps/mobitrust/webrtc:docker            "/usr/local/bin/janus"   6 minutes ago    Up 6 minutes   7088-7089/tcp, 8000/tcp,
8088/tcp, 8188/tcp, 8889/tcp, 192.168.10.12:8089->8089/tcp, 192.168.10.12:10000-10200->10000-10200/udp                          webrtc
e9f74a33d94   registry.fudge-5g.eu/vapps/mobitrust/mt-gateway:latest        "docker-php-entrypoi…"   7 minutes ago    Up 7 minutes   80/tcp, 192.168.10.12:44
->443/tcp                                                                                                                   mt-gateway
5cce9c32941   registry.fudge-5g.eu/vapps/mobitrust/postgresql:latest        "docker-entrypoint.s…"   7 minutes ago    Up 7 minutes   172.17.0.1:5432->5432/tc
                                                                                                                            postgresql
0fccf962943   openspeedtest/latest                                          "/docker-entrypoint.…"   4 weeks ago      Up 30 hours    3001/tcp, 0.0.0.0:3000->
000/tcp, :::3000->3000/tcp, 8080/tcp                                                                                        openspeedtest
oot@fudge:/home/mobitrust# _
```

Figure 30: Vertical Application components deployed at the UC3 trial site as Docker containers



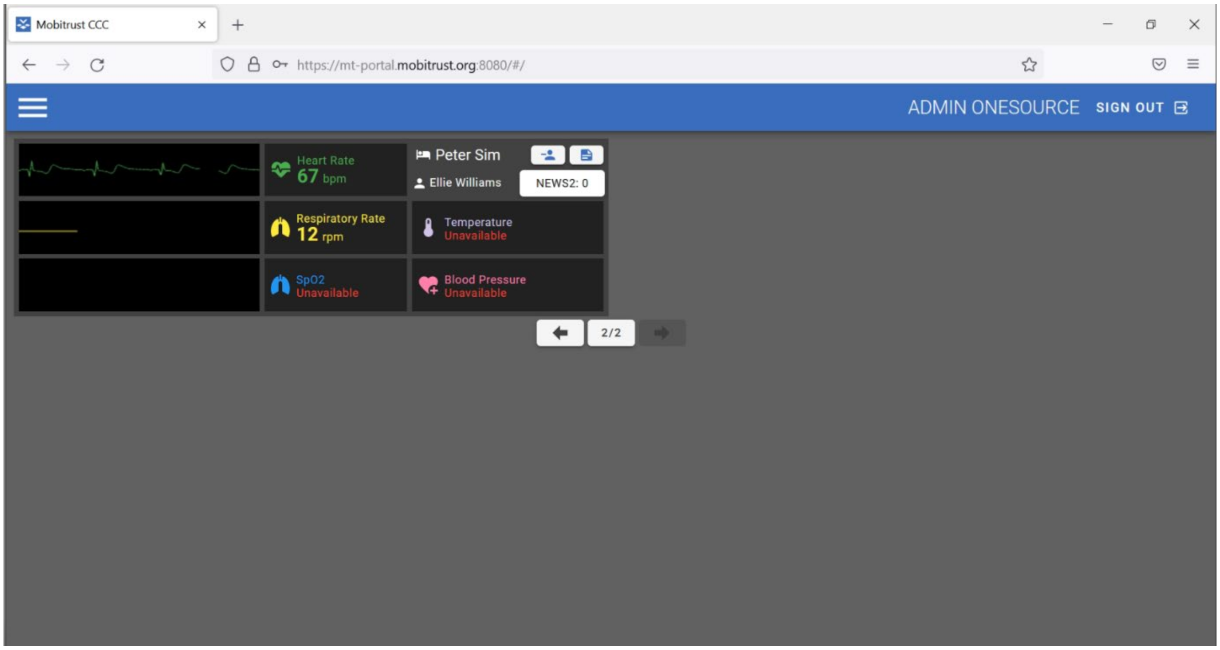
```
root@onesource: ~
```

```
root@onesource:~# docker ps
CONTAINER ID   IMAGE                                                         COMMAND                  CREATED              STATUS               PORTS
                                                                                       NAMES
b29b42aed869   registry.fudge-5g.eu/vapps/mobitrust/mt-portal:latest            "docker-entrypoint.s…"   About a minute ago   Up About a minute    0.0.0.0:8080
                                                                                       mt-portal
d554c4f4899a   registry.fudge-5g.eu/vapps/mobitrust/rtmp-server:docker          "nginx -g 'daemon of…"   2 minutes ago        Up 2 minutes         0.0.0.0:1935
                                                                                       rtmp-server
1da7327144c4   registry.fudge-5g.eu/vapps/mobitrust/mt-device:latest            "./run_simulator.sh"     5 minutes ago        Up 5 minutes
                                                                                       mt-device
8814d6157759   registry.fudge-5g.eu/vapps/mobitrust/tick-kapacitor:latest       "/entrypoint.sh kapa…"   9 minutes ago        Up 9 minutes         9092/tcp
                                                                                       tick-kapacitor
6dbfc47536f2   registry.fudge-5g.eu/vapps/mobitrust/tick-telegraf:docker        "/entrypoint.sh tele…"   10 minutes ago       Up 10 minutes        8092/udp, 81
                                                                                       tick-telegraf
3a5e0efd36c5   registry.fudge-5g.eu/vapps/mobitrust/mt-monitor                  "python3 main.py"        11 minutes ago       Up 11 minutes
                                                                                       mt-monitor
f83c89255e2e   registry.fudge-5g.eu/vapps/mobitrust/mt-orchestrator:docker      "python3 main.py"        11 minutes ago       Up 11 minutes
                                                                                       mt-orchestrator
88d682015b3b   registry.fudge-5g.eu/vapps/mobitrust/tick-influxdb:latest        "/entrypoint.sh infl…"   12 minutes ago       Up 12 minutes        172.17.0.1:8
                                                                                       tick-influxdb
e1460255324e   registry.fudge-5g.eu/vapps/mobitrust/message-broker:latest       "/usr/bin/docker-ent…"   13 minutes ago       Up 13 minutes        1883/tcp, 43
084/tcp, 8083/tcp, 11883/tcp, 18083/tcp, 0.0.0.0:8883->8883/tcp, :::8883->8883/tcp   message-broker
87c85fea2219   registry.fudge-5g.eu/vapps/mobitrust/webrtc:docker               "/usr/local/bin/janus"   13 minutes ago       Up 13 minutes        7088-7089/tc
cp, 0.0.0.0:10000-10200->10000-10200/udp, :::10000-10200->10000-10200/udp              webrtc
2dfd8c96dd54   registry.fudge-5g.eu/vapps/mobitrust/mt-gateway:latest           "docker-php-entrypoi…"   16 minutes ago       Up 16 minutes        80/tcp, 0.0.
                                                                                       mt-gateway
ccefaaf7c0d2   registry.fudge-5g.eu/vapps/mobitrust/postgresql:latest           "docker-entrypoint.s…"   18 minutes ago       Up 18 minutes        172.17.0.1:5
                                                                                       postgresql

root@onesource:~# █
```

Figure 31: Vertical Application components deployed at the NOW as Docker containers

For the integration of the application on both Use Cases, a set of containers was deployed in the servers of each trial site. Such containers, represented in Figure 30 and Figure 31, consist of the various microservices responsible for the features of the application. In Figure 32 it is possible to observe the application running on the servers of UC2 and UC3, respectively.



Heart Rate
67 bpm

Peter Sim
Ellie Williams
NEWS2: 0

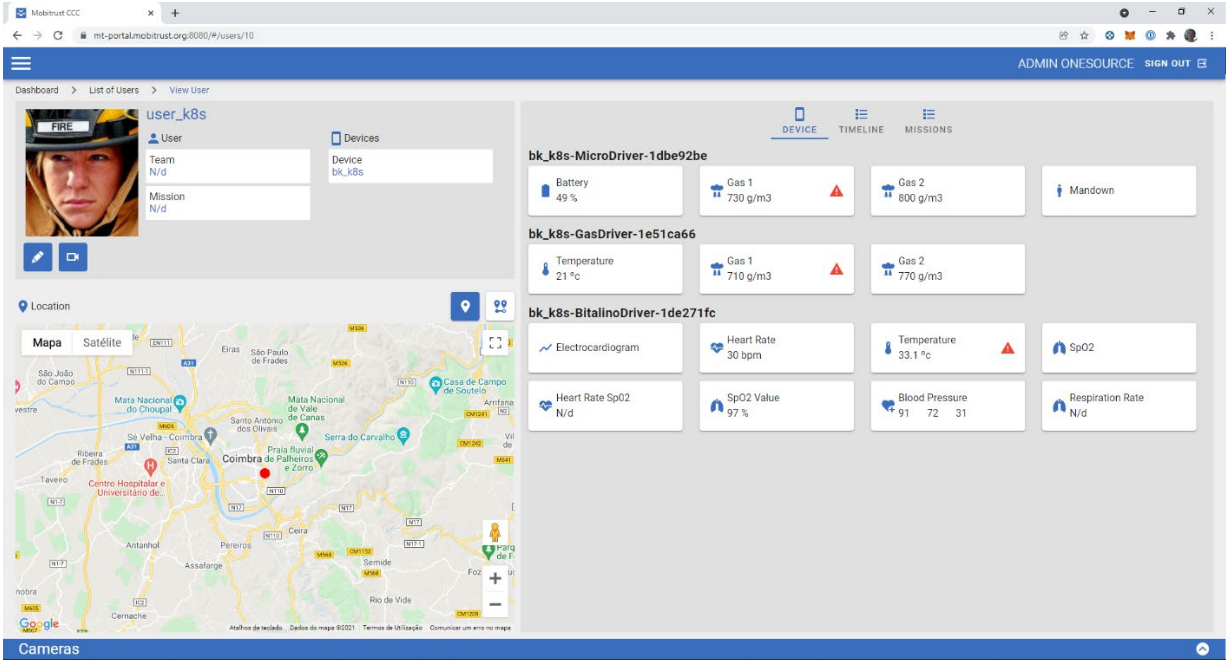
Respiratory Rate
12 rpm

Temperature
Unavailable

SpO2
Unavailable

Blood Pressure
Unavailable

Figure 32: Vertical Application for patient Hospital monitoring deployed at UC3 trial site



user_k8s

User

Team
N/d

Mission
N/d

Devices

Device
bk_k8s

bk_k8s-MicroDriver-1dbe92be

Battery
49 %

Gas 1
730 g/m3

Gas 2
800 g/m3

Mandown

bk_k8s-GasDriver-1e51ca66

Temperature
21 °c

Gas 1
710 g/m3

Gas 2
770 g/m3

bk_k8s-BitalinoDriver-1de271fc

Electrocardiogram

Heart Rate
30 bpm

Temperature
33.1 °c

SpO2

Heart Rate Sp02
N/d

SpO2 Value
97 %

Blood Pressure
91 72 31

Respiration Rate
N/d

Figure 33: Vertical Application for PPDR scenarios deployed in the NOW

6. Integration of Technologies

The last part of the FUDGE-5G ecosystem are the technologies and features developed during the project duration, including the integration between components from different consortium partners and the interoperability tests to verify their correct behaviour. In detail, six different technology and component integration have been carried out during the project duration, and they are described in consequent subsections.

6.1. Integration of CBCF and AMF

One2Many-Everbridge developed a 5G based Cell Broadcast Control Function (CBCF). This function allows an operator to massively send Commercial Mobile Alert System (CMAS) over a controllable geographical area, and it is based on special SMS messages. Everbridge CBCF was delivered from O2M to the Cumucore laboratory as a microservice. The CBCF micro services are running in Docker containers that is setup using docker-compose. From the Cumucore perspective CBCF is an Application Function that communicates with the AMF. Cumucore AMF was modified to support Cell Broadcast feature. The write-replace warning message and PWS-cancel messages were initiated by executing python scripts provided by O2M. The python scripts were run on the same server where the 5G core and CBCF system is setup.

Integration between One2Many-Everbridge SW and Cumucore 5GC was done in Cumucore laboratory. Cell broadcast also requires support from the gNB. In the Cumucore laboratory the system was tested with Nokia RAN and Nokia XR20 and Huawei P40 UEs using test and private network PLMNs. Huawei P40 was tested with PLMN ID 001-01. Warning message state of the Huawei P40 can be reset by switching the phone off and on. Nokia XR20 was tested with PLMN ID 999-98.

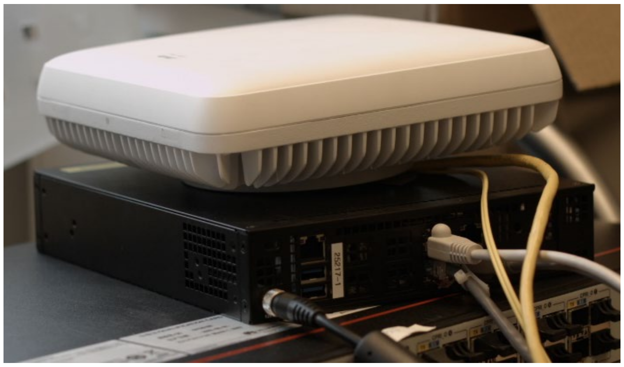


Figure 34: One2Many-Everbridge CBCF on-boarded in Cumucore 5GC box connected to a Huawei LampStation (White box)

In the second stage of Cell Broadcast integration, Cumucore 5GC plus One2Many-Everbridge CBCF was delivered into Telenor on-boarding laboratory in Fornebu; where the PPDR stakeholder brought devices and the solution was integrated with a Huawei LampStation, as shown in Figure 34. More details can be found in D4.2 [12] and upcoming D4.3.

6.2. Integration of NEF

The goal of this integration was twofold: first, to validate the decomposed NEF developed by OneSource, and second to allow the AFs from the PPDR and 5G Virtual Office use cases to request the desired QoS profile for each UE. By communicating through NEF, the requests from the AFs can reach the PCF and other NFs from the 5G Core with the required security and transparency.

Integration work has been performed in two different testbeds. A controlled setup between Fraunhofer FOKUS premises and OneSource's, prioritizing the integration with the 5G Core, and a setup in the eSBA platform located in London. In Figure 35, it is depicted the controlled test setup, where the 5G Core and a simulated UE were deployed at Fraunhofer FOKUS, and the NEF with an AF deployed at OneSource.

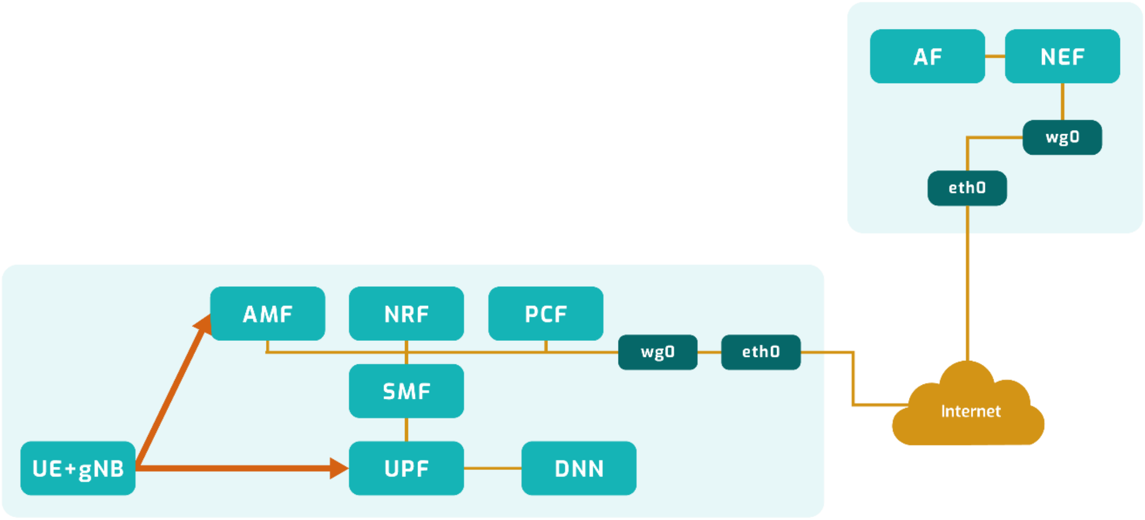
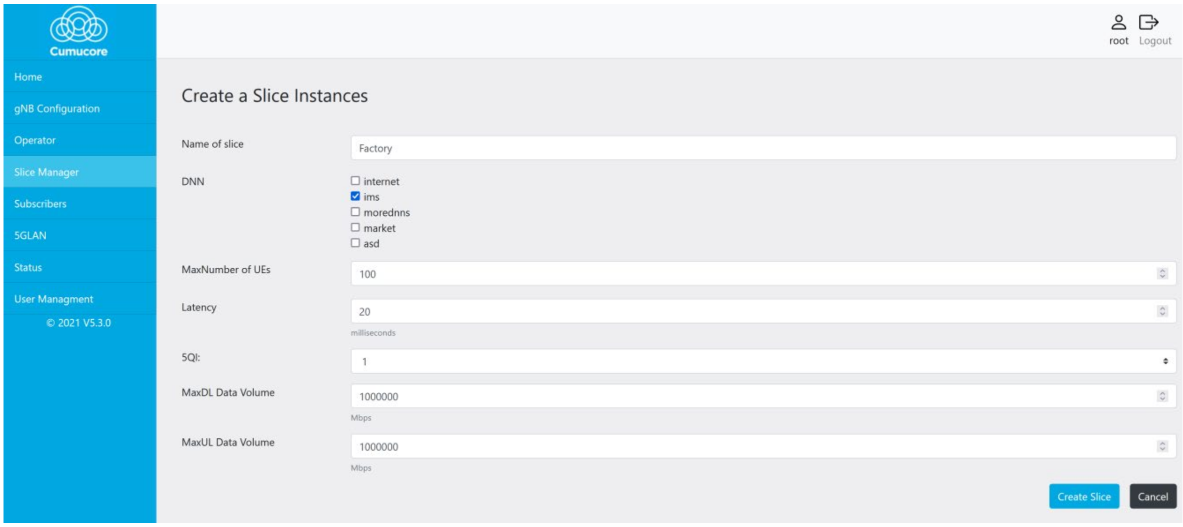


Figure 35: Controlled test setup for NEF integration with 5G Core

The test consisted in connecting a simulated UE to the 5G network followed by a request from the AF to create a Policy Authorization for the same UE. The request is sent to the PCF through the NEF. By receiving a status code of 201, and validating the creating of the Policy Authorization, the integration was successful. At the 5G core network side after receiving the request from NEF, PCF sends a Policy update notification to SMF. Upon receiving the request and validating it, SMF creates rule and push that to UPF. SMF also forward rules and information about the flow towards gNodeB and UE via AMF, in order to configure them in RAN and UE. More information of the validation test performed can be found in D4.2.

6.3. Integration of Slicing

In Industry 4.0 use case 5G network was configured to have an own network slice for 5GLAN traffic. Nokia 5G SA radio was configured with two different slices. First slice was used by the payload with 5GLAN functionality and the second slice was used by TSN traffic.



Create a Slice Instances

Name of slice	Factory
DNN	☐ internet ☑ ims ☐ morednns ☐ market ☐ asd
MaxNumber of UEs	100
Latency	20 milliseconds
5QI:	1
MaxDL Data Volume	1000000 Mbps
MaxUL Data Volume	1000000 Mbps

Figure 36: Slice creation in Cumucore 5 NC

6.4. Integration of TSN and 5GLAN

5GLAN feature was tested first in the Cumucore premises. Integration and testing with Fudge platform was done in Telenor laboratory in Fornebu. Test set-up is shown in Figure 37.

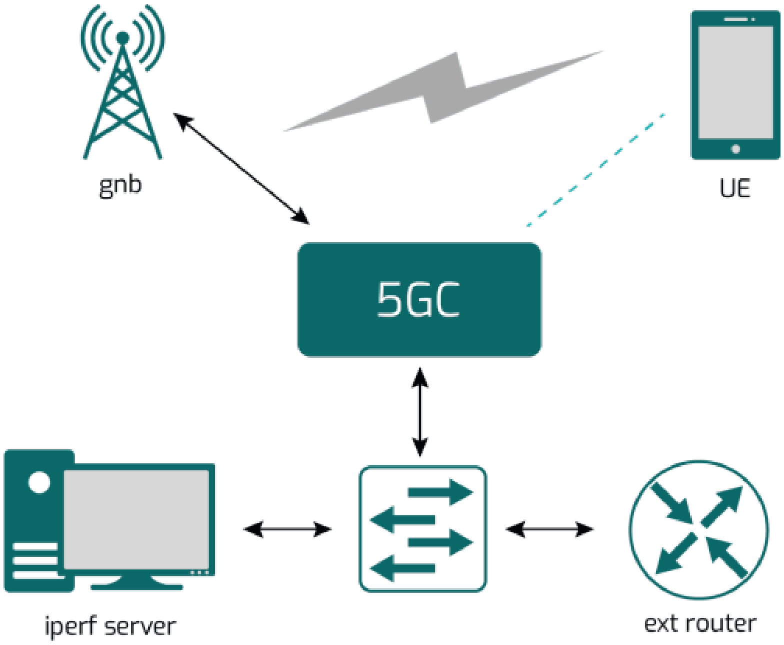


Figure 37: 5GLAN test set-up

FUDGE network with 5GLAN was moved to ABB laboratory in Fornebu. In ABB premises 5GLAN functionality was tested in Industry 4.0 use case. TSN functionality was tested in Cumucore laboratory. TSN testing was done in Cumucore premises using test set-up described in the Figure 38.

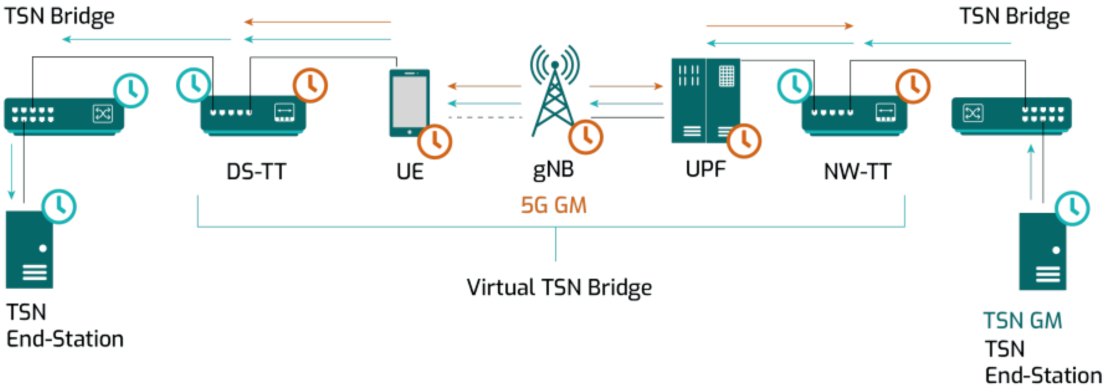


Figure 38: TSN test set-up

TSN feature was integrated with the FUDGE platform in ABB laboratory to be used in industry 4.0 use case.

6.5. Integration of Interconnected NPNs

In section 3.2.4, in order to connect the three INPNs nodes a lightweight containerized Open5GCore deployment is featured. However as these are three separate locations, the connection is performed over public internet link acting as backhaul i.e. a best effort connection. This introduces security risks, as opening a system directly to internet is unsafe for unwanted connections to gain internal access into resources and personal information. Often, organizations are not allowed to open a webport directly. Hence to circumvent this, a Wireguard (WG) system [13] is being used to connect the edges together. WG allows the interconnected nodes to communicate as they are located on the same network. Once Wireguard is setup and the 5G core is up and running, the challenge is to send traffic from the 5G core over these WG interfaces. This is achieved by redirecting traffic from SCP to WG interface. The SCP has two interfaces for connectivity, one interface where it communicates to the deployed core network functions and other interface where it connects to other SCPs. The Berlin node SCP deployed on each node has been modified to accept WG interfaces as possible inputs, so the Berlin SCP binds the interface directly on start-up, enabling the connectivity across geographically distributed SCPs and easing the operation and communication.

The scenario carried out in this Interconnected NPNs is the home-routed roaming. The main feature is the data traffic is also routed via the home network to the data network along with the authentication of the subscribers. This feature was developed and integrated in the 5G core following 3GPP Specifications. More information on home-routed roaming is available in [14] and [15]. In Open5GCore platform the selection of home-routed roaming for a roaming subscriber is data network (DN) based. Both Home SMF (H-SMF) and Visiting SMF (V-SMF) takes part in this procedure to push data path related rules to the Home UPF (H-UPF) and Visiting UPF (V-UPF) subsequently. In Figure 39, data path for home-routed scenario is shown using yellow lines. To configure the setup, each of the domain gets a home network specific DN (such as FOKUS, UPV, OSL for the three locations), and any session establishment request from the roaming subscriber to that DN is home-routed. Once the data path is established between the visited and home network, the data traffic is routed from V-UPF to the H-UPF through the WG interface. Results from this setup can be seen in upcoming D4.3.

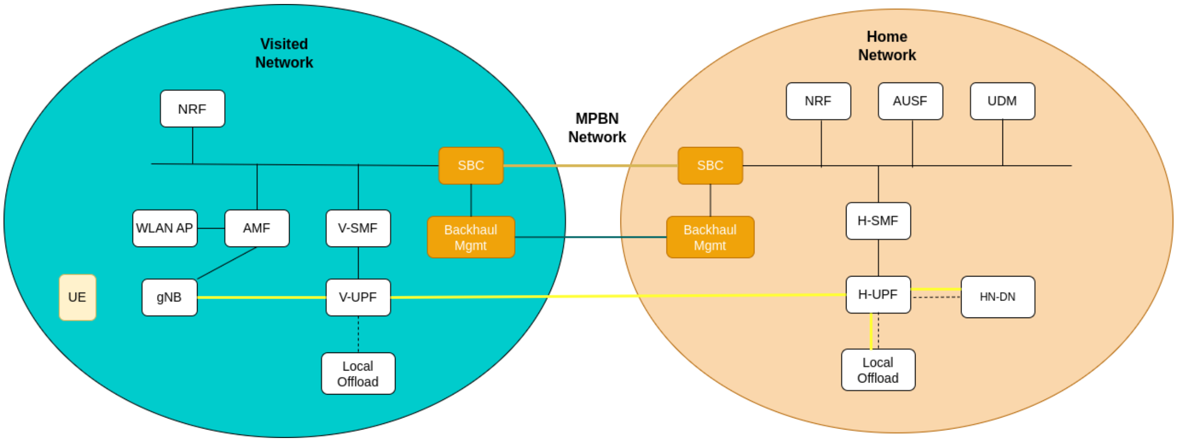


Figure 39: Data Bearer for Home-Routed Roaming

6.6. Integration of Slicing Orchestrator

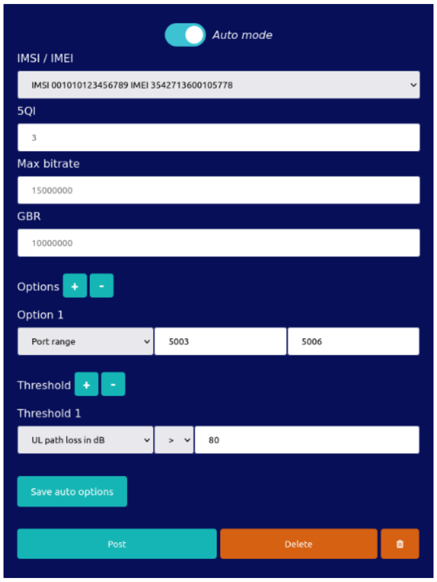
The slicing orchestrator manages the quality of service (QoS) rules on the Amarisoft network, thus allowing a UE to be isolated from other UEs in its slice.

An executable script starts the connection to the Amarisoft base station and starts a web interface (Figure 40) allowing the management of the QoS rules. The QoS rules consist in a set of different values: the UE on which the rule is applied, the wanted 5G QoS Identifier (5QI), the allocated download and upload bitrates and the port range/type of service (ToS) the rule will be applied on. It is possible to send those rules manually or automatically following set rules.

The script accesses the APIs of the Amarisoft RAN and the core network and can send JSON messages to them for two purposes:

- Monitoring statistics from the RAN and the core with the possibility of sending them to a data visualisation like Kibana. It is also used for the Auto mode which will be described below
- Sending the QoS rules to the core

The auto mode allows to send the QoS rules according to a predetermined rule instead of manually. For example, it can activate the rule if the download retransmissions are exceeding a set value.



Auto mode

IMSI / IMEI: IMSI 001010123456789 IMEI 3542713600105778

5QI: 3

Max bitrate: 15000000

GBR: 10000000

Options

Option 1: Port range 5003 5006

Threshold

Threshold 1: UL path loss in dB > 80

Figure 40: Slicing Orchestrator web interface

6.7. Multivendor 5GC configuration

During this period, an integration effort was put into having an interoperable 5GC solution featuring hybrid deployment between cloud and on-premise components. In detail, the solution consists of a multi-vendor integration of the 5GC's Control Plane (CP) from Athonet with the 5G's User Plane (UP) from Cumucore, and namely the integration of Athonet's Session Management Function (SMF) and Cumucore's User Plane Function (UPF). For this activity, the same on-cloud 5GC solution introduced in Section 4.3 was utilized, with the difference that Athonet's UPF was excluded from the overall architecture. Figure 41 below represents the main core network components and highlights the logical exposure of the N4 interface between SMF (CP) and UPF (UP).

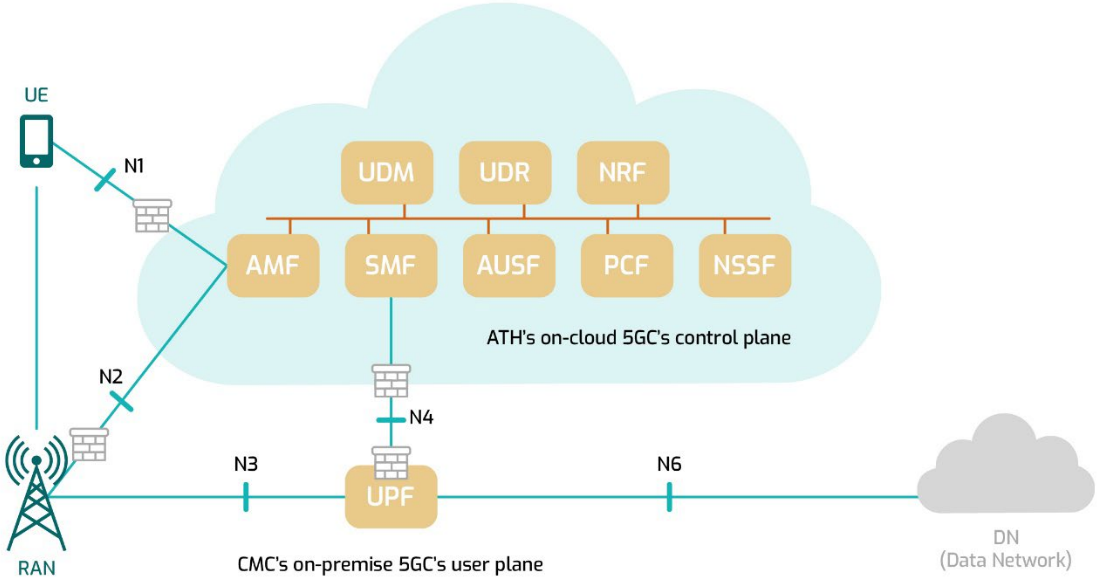

UE
N1
UDM
UDR
NRF
AMF
SMF
AUSF
PCF
NSSF
ATH's on-cloud 5GC's control plane
N2
N4
N3
N6
UPF
RAN
CMC's on-premise 5GC's user plane
DN
(Data Network)

Figure 41: 5G core network architecture highlighting the N4 interface between SMF and UPF.

The N4 interface is implemented following the 3GPP standard specifications. The reader is referred to [16] and [14] for the SMF and UPF endpoints, and to [17] for the PFCP protocol for communication between the two network functions. The release supported for the current integration is Rel-15.

The main scope of exchanges over the N4 interface includes the establishment, modification, and release of the PDU sessions. In an architecture with control and user plane separation, the UPF is responsible for handling user data packet forwarding and reporting the traffic usage data to the SMF.

A VPN connection is established between the local UPF and the remote CP in the cloud to meet security and best-practice recommendations.

The goal of this work item is to configure the SMF and UPF in order to integrate and allow the interworking between the two functions from different vendors. The integration has followed a process split into multiple steps, which can be summarized as follows:

1. SMF and UPF configuration and exchange of common information elements mandatory on the N4 interface.
2. Validation of the PFCP messages exchanged on the N4 interface.
3. Setup of a gNB locally at Cumucore’s premises (where the UPF is located).
4. Provisioning, registration, and authentication of the UEs.
5. PDU session establishment involving all core components.
6. End-to-end validation with traffic flows.

All the previous six steps were validated successfully. We recall that the purpose of the integration was to validate the functional interconnection between the two core network components, and KPI collection and performance analysis was out of the scope in this setup.

7. Conclusion

This document provided the details on the integration of the technological components developed in the tenure of the project and were reported in the WP2 related deliverables. To validate different scenarios of the use cases and to validate the key features developed as part of the project, how different trial sites are prepared were illustrated by this deliverable. The integration work performed to onboard the 5G Cores and VAO on the eSBA platform were also depicted by this document. The deliverable is structured in a way so that it provides an outline of the technologies, preparation of the testbeds on the trial sites and the onboarding of the technologies on the testbeds to perform vertical trials and validate the use cases.

Following the integration work denoted in D3.1, this deliverable gives more information on the integration of technologies to perform trials for different use case scenarios mentioned in D1.1. The preliminary test setup at Fornebu, the preparation of the trial sites for the each of the use cases with the configuration and installation of the 5G cores, RAN, devices, vertical applications were presented by this deliverable. How the eSBA platform can be used to connect multiple trial sites were also showcased with one use case. This project also offers integration between technologies provided by different partners to showcase some use case scenarios. The work done in this direction was also illustrated in this deliverable.

This document was the final release on the integration work performed for the use cases in the project. The validation of the integrated components and the use cases will be done by performing trials in the trial sites. The outcome of the trials will be reported accordingly in D4.2 and D4.3 deliverables.

8. References

[1] Affordable5G, “High-tech and affordable 5G network roll-out to every corner,” [Online]. Available: https://www.affordable5g.eu/.

[2] Cumucore, “5GLAN feature enables the integration of mobile networks,” March 2022. [Online]. Available: https://cumucore.com/whitepapers/5glan/.

[3] N. Finn, “Introduction to Time-Sensitive Networking,” *IEEE Communications Standards Magazine,* vol. 2, pp. 22-28, 2018.

[4] M. Corici, “5G Non-Public Networks Roaming Architecture,” in *International Conference on Network of the Future*, Coimbra, 2021.

[5] nghttpx, "HTTP/2 proxy - HOW-TO," [Online]. Available: https://nghttp2.org/documentation/nghttpx-howto.html.

[6] one2many, an Everbridge company, "WHY CELL BROADCAST IS MORE IMPORTANT THAN EVER FOR EMERGENCY ALERTING!," [Online]. Available: https://www.one2many.eu/_files/ugd/8632b1_73e1fefa063b460799ee7aa52a4e7e97.pdf?index=true.

[7] Cumucore, "FUDGE-5G announces a Cumucore’s 5G core into the OpenShift Ecosystem," [Online]. Available: https://cumucore.com/cumucore-news-and-events/cumucore-has-installed-its-5g-core-successfully-on-redhat-openshift/.

[8] C. Pousali, “FUDGE-5G D3.1: FUDGE-5G Test-bed Continuous Technology Integration,” 31 12 2021. [Online]. Available: https://fudge-5g.eu/download-file/495/4wMXMZc1zPCYuSshevOc.

[9] S. Robitzsch, "FUDGE-5G D1.3: Final FUDGE-5G Platform," August 2022. [Online]. Available: https://fudge-5g.eu/download-file/543/iYIVtTS3SKWmXm6QfdQp.

[10] S. Robitzsch, “FUDGE-5G D2.5: Technology Components and Platform - Final Release,” November 2022. [Online]. Available: https://fudge-5g.eu/download-file/567/Mi9U4WiZAUo4LDk04U8t.

[11] Nemergent Solutions, “Nemergent Solutions: Experts in Mission Critical Services,” [Online]. Available: https://www.nemergent-solutions.com/lang/es/.

[12] J. Fernandes, “FUDGE-5G D4.2: Final Technical Validation of 5G Components with Vertical Trials,” 2022. [Online].

[13] Wireguard, "Fast, modern, secure VPN tunnel.," [Online]. Available: https://www.wireguard.com/.

[14] 3GPP, “TS 23.502: Procedures for the 5G System (5GS) v17.0.0,” [Online]. Available: https://www.3gpp.org/ftp/Specs/archive/23_series/23.502/23502-h00.zip.

[15] 3GPP, “TS 29.502: 5G System; Session Management Services; Stage 3,” [Online]. Available: https://www.3gpp.org/ftp/Specs/archive/29_series/29.502/29502-h00.zip.

[16] 3GPP, "TS 23.501. System architecture for the 5G System (5GS). V17.0.0," [Online]. Available: https://www.3gpp.org/ftp/Specs/archive/23_series/23.501/23501-i00.zip.

[17] 3GPP, "TS 29.244. Interface between the Control Plane and the User Plane nodes. v17.0.0," [Online]. Available: https://www.3gpp.org/ftp/Specs/archive/29_series/29.244/29244-h00.zip.