FUDGE-5G

FUlly DisinteGrated private nEtworks for 5G verticals

Deliverable 1.1

Technical Blueprint for Vertical Use Cases and Validation Framework

Version 2.0

Partners

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

Abstract

This document describes the five use cases that are the targets for 5G Non-Public Network (NPN) developments within the FUDGE-5G project. The use cases addressed are: (i) Concurrent Media Delivery, (ii) Public Protection and Public Relief (PPDR), (iii) 5G Virtual Office, (iv) Industry 4.0, (v) Interconnected NPNs.

List of Authors and Reviewers

1.1. Authors

Author	Partner
Carlos Barjau, Josep Ribes, Borja Iñesta, David Gomez-Barquero	UPV
Kashif Mahmood (Editor), Pål Grønsund, Ole Grøndalen, Andres Gonzalez	TNOR
Daniele Munaretto, Marco Centenaro, Nicola di Pietro	ATH
Jose Costa, Mika Skarp	CMC
Pousali Charkaborty, Marius Corici	FHG
Peter Sanders	O2M
Thanos Xirofotos	UBI
Luis Cordeiro, André Gomes, António Borges	ONE
Manuel Fuentes, Andrés Meseguer, Teresa Pardo, David Martín-Sacristán	5CMM
Sebastian Robitzsch, Kay Hänsge	IDE
Zoran Despotovic, Artur Hecker, Dirk Trossen	HWDU
Filippo Rebecchi	THA

1.2. Reviewers

Reviewer	Partner
Erik Vold	NRK
Waqas Ikram	ABB
Kennet Nomeland	Norwegian Defense Materiel Agency (NDMA)
Karl Øyri	Oslo University Hospital (OUS)
Steve Appleby	British Telecom (BT)

Executive Summary

FUDGE-5G is the first 5G-PPP project that focuses solely on 5G private networks, known as Non-Public Network (NPN) in 3GPP terminology. Five use cases for 5G-NPNs have been identified featuring diverse range of network and radio requirements, deployment, and configurations options, representing a very high innovation and business impact for the private 5G network market. The five use cases and their corresponding stakeholders are:

- **Concurrent Media Delivery** – stakeholder *NRK.*
- **Public Protection and Disaster Relief (PPDR)** – stakeholder *Norwegian Defense Material Agency*.
- **5G Virtual Office** – stakeholder *Oslo University Hospital.*
- **Industry 4.0 Network** – stakeholder *ABB.*
- **Interconnected NPNs** – stakeholders *Telenor, Fraunhofer FOKUS* and *Universitat Politecnica de Valencia.*

The use cases target five vertical sectors encompassing Media & Entertainment (M&E), PPDR, eHealth, Industry 4.0, and education. It needs to be highlighted that 5G Virtual office will be realised in a hospital in Oslo, while the interconnected NPN use case will be realised by connecting several campuses, hence the mention of the eHealth and education, respectively, as typical concerned vertical sectors. Note that the same two use cases could be applied to different verticals.

This document is a cornerstone for the project, since it describes the technical blueprint about how each use case will be implemented across the 5G-VINNI facility site managed by Telenor Research in Norway, including the specific deployment option of the FUDGE-5G Platform (e.g., public cloud, on premise, hybrid). The use case blueprints have been defined by considering the inputs from the vertical stakeholders.

FUDGE-5G will follow a methodology structured in six steps to bring forward the innovative 5G key technologies and technology components. The methodology steps are: (*i*) Definition of Blueprints for the Use Cases, (*ii*) Technology Design, (*iii*) Agile Prototype Development, (*iv*) Platform Integration, (*v*) Deployment in 5G Infrastructure, and (*vi*) Product Validation in Real Environments.

As well as describing the actual use cases, the document outlines the validation framework based on requirements and Key Performance Indicators (KPIs) specific to the use cases. The architectural blueprint to realize the different use case will be documented in deliverable D1.2 [1].

Table of contents

1. Introduction

The use of 5G for private networks has seen an increased interest in industry and standardization alike with an expected increase of that market in the coming years [2]. This is also evident in the activities within the 3GPP (3rd Generation Public Partnership), which leads the standardization activities with respect to 5G in cellular telecommunications technologies, which positions the study of Non-Public Networks (NPNs) in the second phase of 5G networks (3GPP Rel-16 and beyond). Also, associations such as the 5G-ACIA have identified a number of NPN use cases [3].

A Non-Public Network enables deployment of 5G networks for non-public use. NPNs are physically or logically isolated from the public network by using different hardware, virtual machines or network slices. From this principle, a clear and immediate advantage arises from the isolation in terms of securing infrastructure and devices behind corporate networks. There may be two types of deployments: Stand-alone Non-Public Network (SNPN), operated by an NPN operator and not relying on network functions provided by a PLMN, or a Public Network-Integrated NPN (PNI-NPN), an NPN deployed with the support of a PLMN.

With the SNPN, the network is completely isolated from public networks, uses dedicated spectrum and all network functions are located inside the logical perimeter of the defined NPN operator premises. With the PNI-NPN, there are many options to how it can be provided. Services may be purchased as a virtual network application on a commercial PLMN or sharing the PLMN infrastructure as a closed/private sub-network, either under specific contract arrangements or as a preferential subscriber with suitable assigned priority. There is also the possibility of a hybrid solution for the PNI-NPN, where the NPN, owned and operated by a private institution, resides alongside a commercial PLMN, where, under negotiated contract arrangements, such a private institution gets preferential treatment with suitable assigned priority.

Since NPNs are dedicated to private user groups, the network can be designed, optimised and dimensioned to the groups' needs like coverage areas, network capabilities and mobility scenarios. Furthermore, the NPNs can be customized to serve different needs of enterprise and industrial verticals. For instance, it can be conceived to provide high availability and reliability, to support LAN-type services, to deliver stringent end-to-end synchronization for deterministic packet delivery or to fulfil high uplink and downlink minimal speeds. An NPN can also use dedicated spectrum (i.e., without any potential interference), in new bands beyond the designated ones for specific services (e.g., Programme-Making and Special Events (PMSE)). This further strengthens the motivation behind the need for NPNs to exist beyond the context of PNI-NPNs.

Beyond utilizing the advancements brought about by 5G technology and the emerging ecosystem of cloud solution providers, NPNs will bring the additional benefit of enabling the infrastructure owners to fully control deployment, core components, and coverage for their networks as well as integration into existing backend and communication infrastructure. This removes any dependency from nationwide operator rollouts, while

enabling the NPN operator to carefully optimize the deployment, e.g., for delivering the Quality of Service (QoS) requirements of their interested use cases. Overall, the NPN concept allows for designing, deploying, and interconnecting capabilities for the specific needs of the use cases motivating the NPN deployment in the first place.

Against this background, the FUDGE-5G project has carefully selected five NPN use cases, shown in Figure 1, which will be designed, developed, and tested in FUDGE-5G, covering both types of NPNs, presented before:

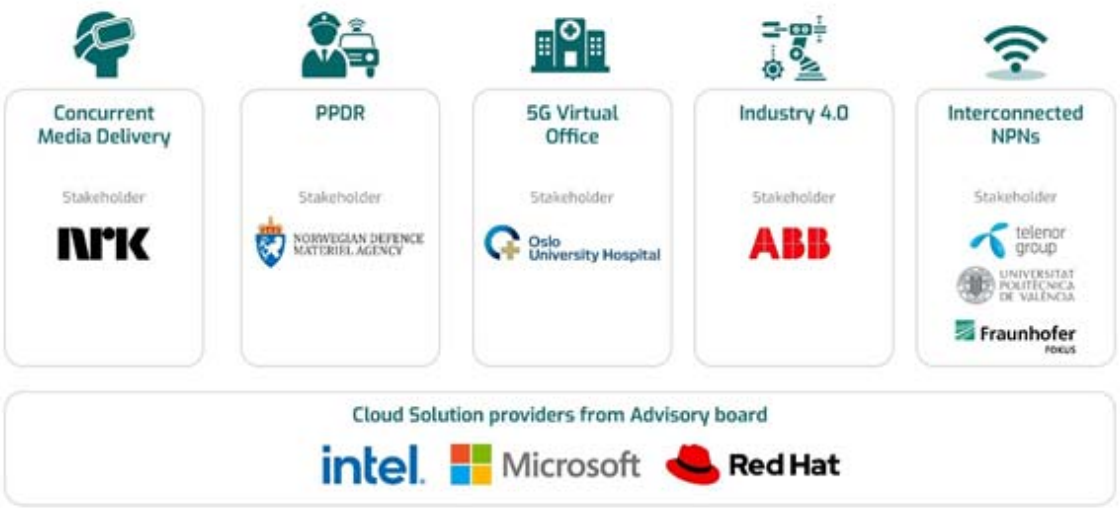


Figure 1: FUDGE-5G use cases along with the stake holders.

All five (5) FUDGE-5G use cases will be hosted in Norway, leveraging the 5G Radio Access Network of 5G-VINNI, except for the "interconnected NPN use case", which will be deployed between the following three locations:

- Fraunhofer FOKUS campus in Berlin (Germany).
- UPV university campus in Valencia (Spain).
- Telenor campus in Oslo (Norway).

This document provides the technical blueprint and the validation framework for the FUDGE-5G use cases. Each use case is being championed by an appointed partner to steer the realization of the use case within the overall efforts of the project partner. The use case champions are: Universitat Politecnica de Valencia (Concurrent Media Delivery), Thales (PPDR), OneSource (5G Virtual Office), Fivecomm (Industry 4.0) and Fraunhofer FOKUS (Interconnected NPNs).

The description of each of the five use cases (denoted as 'X' in the following) follows the same pattern of description in Chapters 2 (Concurrent Media Delivery), 3 (PPDR), 4 (5G Virtual Office), 5 (Industry 4.0) and 6 (Interconnected NPNs):

- The motivation for the use case is provided in Section <X>.1.
- Section <X>.2 covers the scenario description with the different realisations of the use case.

- Section <X>.3 outlines the key components of each use case and high-level topology.
- This is followed by functional and performance requirements of each use case in Section <X>.4.
- The ecosystem in Section <X>.5 describes the different partners and their role in the respective use case. It also presents foreseen future actors when the use case may become commercially available.
- The test cases are introduced in Section <X>.6. This information is further detailed in Chapter 7.
- The expected outcome of each use case is presented in Section <X>.7.
- Finally, the risk assessment is outlined in Section <X>.8.

Chapter 7 provides a detailed description of the validation framework, including the test cases, test tools and validation KPIs.

1.1. Use Case Realisation Methodology

The FUDGE-5G project use case realisation methodology is illustrated in Figure 2. It involves *Technology Design* and *Agile Prototype Development* phase at the individual partner's premises, after which the *FUDGE-5G platform integration* will happen at the InterDigital's premises in the UK. After successful integration, the FUDGE-5G platform will be integrated with the *5G infrastructure* hosted by Telenor at the stakeholders' locations in Norway. The deployment in stakeholder's location will allow extensive FUDGE-5G product validation in a realistic environment. It needs to be highlighted that Telenor will reuse 5G infrastructure from the 5G-VINNI project as much as possible to expedite the realisation of the 5 use cases, after which the focus will be on the validation framework.

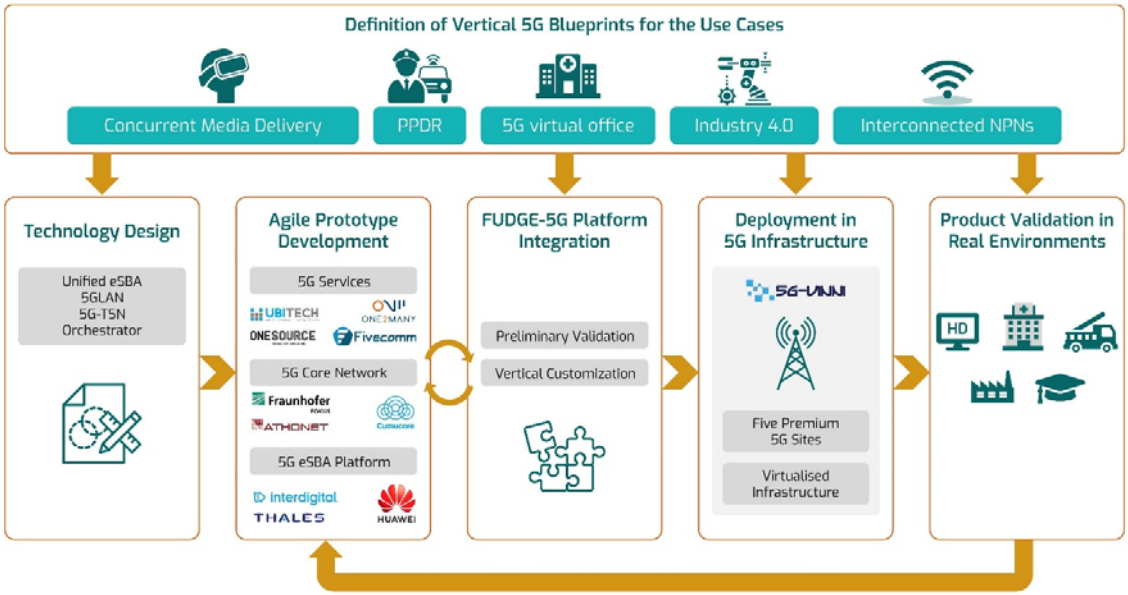


Figure 2: FUDGE-5G use case validation strategy follows DevOps based strategy.

This validation framework will be the means to validate the innovations introduced in each Use Case and prove that the associated KPIs are met. The details of these target KPIs are discussed and detailed in each of the individual use case description and Chapter 7.

To deliver on the promise to showcase the FUDGE-5G innovations in trials, the project is going to follow a DevOps pipeline based on a Kanban strategy. This strategy allows a continuous and more fluid methodology to develop, integrate, experiment, and eventually trial the various technology components. This agile approach is being organised and monitored via FUDGE-5G-internal Gitlab project allowing the degree of freedom an EU project requires to deliver on the project goals while respecting each organisation's business and technology roadmap. Thus, the DevOps pipeline envisaged for a successful conduction of trials is illustrated in Figure 3,serves as the baseline for integrating all FUDGE-5G components and platform, and creates delivery milestones which must be achieved before entering the next level. As can be seen on the very left, all components are expected to be developed in-house by each partner following the architecture and interface specifications provided in D1.2 [1] and D2.1 [4]. While FUDGE-5G encourages each partner to follow agile workflows for code development, it is expected that each partner can provide their components using a versioning system. The Technology Readiness Level (TRL) of components that arrive at the integration testbed are expected to have TRL 4 (technology validated in lab) or above, ensuring they have been tested in an in-house laboratory environment.

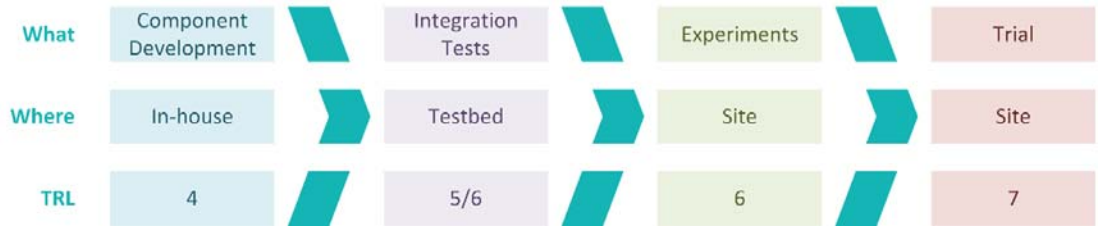


Figure 3: DevOps pipeline for integrating FUDGE-5G components for conducting trials.

The integration testbed then conducts pre-defined system tests ensuring a successful interworking of all components for a particular use case. The envisaged system tests will be developed as part of T2.5 and documented in D2.1 [1]. If a system test is passed successfully, the components involved can be classified as TRL 6 (technology demonstrated in relevant environment - industrially relevant environment in the case of key enabling technologies) given the relevant environment the London testbed provides (OpenStack-based multi-tier compute infrastructure with an SDN-based switching fabric, a 5G SA base station and a range of different 2020 flagship 5G phones).

The next phase of the DevOps pipeline is the execution of pre-defined experiments to test the behaviour of all FUDGE-5G and 5G-VINNI components that are part of a use case on site. The objectives of all experiments are KPI-driven based on the requirements defined in each use case. The validation framework described in the next sub-section forms the baseline for them. If experiments succeed, all components can be tagged with TRL 6.

The last step is the execution of trials demonstrating the innovations of FUDGE-5G in an operational environment, which allows all components involved to reach TRL 7 (system prototype demonstration in operational environment).

1.2. Overview of FUDGE-5G Innovations

In this section, the innovations of the FUDGE-5G project are described briefly to provide a complete list of advances over currently deployed, standard-conform systems. The innovations will be leveraged across all use cases in full or as a sub-set based on their applicability. FUDGE-5G classifies a particular functionality or feature as an innovation, if it fulfils at least one of the following items:

- A definition of a system functionality that, in order to become usable (i.e. both deployed and interoperable) requires standardization.
- Demonstration of a system functionality in a lab or as part of a FUDGE-5G trial, which is not fully standardised or derives from the current standardised methods and procedures. FUDGE-5G defines this functionality as an innovation if there is a clearly expressed desired in a standardisation body, e.g. 3GPP, IETF or ETSI.
- System demonstration of a recently or currently standardised functionality, e.g., Release 16/17 or an IETF draft, in an NPN setting tuned towards a particular use case.
- Integration and demonstration of **multi-vendor systems** beyond the current state of the art, especially in the 5G core domain.

As FUDGE-5G is operating in 5G-VINNI that provides the RAN across all use cases, the access network is seen as out-of-scope for potential FUDGE-5G innovations. However, it is expected that FUDGE-5G can conclude on specific challenges and/or shortcomings with Release 15 or 16-based RANs based on the project's innovations. It is expected to utilise 3GPP Release-16 features provided by 5G-VINNI around uplink enhancement technologies such as supplementary uplink or uplink-friendly frame structure as new RAN features that are not commercially deployed at the time this deliverable is being written. Additionally, FUDGE-5G will utilise and demonstrate the protection against IMSI (International Mobile Subscriber Identity) catching techniques via the 5G SUCI (Subscription Concealed Identifier). This allows improved privacy and disallows tracking end-users even during a first-time connection to a visited network.

1.2.1. Service-based Architecture

The FUDGE-5G platform is composed of the functional blocks; service routing, resource scheduling, system slicing and orchestration capabilities, offering a unified Service-Based Architecture (SBA) for both control and user planes. The platform will be described in detail in Deliverable D1.2 [1].

FUDGE-5G brings in **architecture unifications** along several dimensions. **Unified architecture which applies to both control and user plane** comes first. The goal is here to apply the same cloud native and service centric concepts and architectural principles to

services that implement the logic for either plane. The FUDGE-5G platform adopts cloud native and "as-a-Service" paradigm shifts that have originated from the cloud world and ultimately enforces how (control and user plane) services must be designed from an architectural and software engineering perspective.

Practically, given the current status of FUDGE-5G service routing and resource scheduling (see next paragraph), this means working out appropriate solutions for their application in the user plane. 5GLAN enhancements of FUDGE-5G will enable **unified access** by realizing all-Ethernet virtual networks that integrate devices served by diverse access technologies and allowing Ethernet-like communication between them. Towards the end of the project, we will push these unification principles to the limit and come up with their generalizations, e.g. **unified infrastructure**, which may serve as guidelines for future, probably 6G, architecture.

Since Release 15, the existence of a **Service Communication Proxy** (SCP) is optional, enabling the communication among 5GC Network Functions (NFs) that implement a Service-based Interface (SBI) and are realised in a Cloud-Native Network Function (CNF) fashion. FUDGE-5G innovates on the concept of SCP with novel **service routing** and **resource scheduling** advances across all NFs, allowing a full separation of responsibilities between consumers' and producers', and the objective to route traffic among them in a resource-aware manner and to select the most appropriate instance. FUDGE-5G resource scheduling balances the load among NF instances, achieving thus more efficient usage of the infrastructure. It dispatches incoming requests to NF instances at runtime, complementing thus the cloud-native orchestration (described below).

The FUDGE-5G project distinguishes between infrastructure, platform and 5G services on top of the platform; the 5G services implement 5GC as well as vertical applications. In order to offer truly end-to-end slices for a user plane communication (UE to another UE or a vertical application in a DN) which includes the control plane communication for managing the user plane, FUDGE-5G offers **end-to-end secure slicing** allowing differentiated access to specific services and the ability to programmatically slice the wholesale resource (slice) received from the infrastructure and splice (merge) existing slices at run time. The objective is not only to deliver a complete end-to-end solution capable of providing unified slice management over the different orchestration domains (e.g., user entity, radio access, edge, core), but also to be able to showcase differentiated security levels for on-the-fly deployments (deployed as NF both on the user and the control plane). The ultimate goal is to have a separation of information per slice with potential changes at run-time, without reducing security or compromising required access restrictions.

In order to foster multi-vendor deployments (potentially including NFs of the same type) FUDEG-5G innovates on a **unified location-aware cloud-native orchestration** approach, entitled **Service Function Virtualisation (SFV)**, allowing 5G Core (5GC) vendors to orchestrate (deploy) and lifecycle-manage the state of their instances using Service Level Agreements (SLAs) similar to current public cloud offerings.

In addition to SFV, a **Vertical Applications Orchestrator** (VAO) performs deployment and runtime management of 5G-ready vertical applications. The VAO on-boards the vertical

application and evaluates a provided set of requirements (e.g., Quality of Service QoS and Quality of Experience QoE constraints, computational requirements), handling the deployment and lifecycle management of higher-layer application components. The following VAO capabilities are explored:

- Data monitoring mechanisms, which collect feeds from application-level and network metrics.
- Strict enforcement of end-to-end QoS requirements through context awareness engine (policy engine) that makes inference over the acquired data.
- Resource utilization monitoring and correspondent scale-in/scale-out implementation.
- Deployment closer to the UE location, when there is infrastructure available.

As part of the SFV and VAO operations, the FUDGE-5G platform offers an integrated monitoring for unified reporting, processing and analytical tasks across vendors and technologies.

1.2.2. 5G Core Innovations

With the move within 3GPP towards a service-based architecture for control plane services, the monolithic realisation of NFs and their static relationships (as in interfaces) have changed significantly by adopting cloud-native communication and realisation methods. Combined with the ambition to foster multi-vendor deployments based on the advances that SBA provides, FUDGE-5G aims at introducing meaningful disintegration criteria of the existing NFs in order to demonstrate cloud-native scalability and reliability advances as well as to perform multi-vendor trials, where the NF of the same type within the same 5GC is offered by more than one vendor.

Public clouds offer cost-effective access to infrastructure with global coverage of the deployed applications. In this context, FUDGE-5G will leverage the Amazon Web Services (AWS) public cloud to host the virtualized 5GC NFs that are not processing user plane traffic. This approach allows a minimal on-premise hardware set-up, consisting of, e.g., gNB, UPFs (User Plane Functions) and data networks, therefore lowering CAPEX and OPEX for the infrastructure owner, while increasing availability and reliability of control plane services using a stable internet connection towards the public cloud.

5GLAN enables integration with fixed networks (e.g., Ethernet, Wi-Fi, etc.) moving towards an "all-Ethernet" abstraction in unified access. Enhancing 5GLAN allows for all-Ethernet virtual networks, seamlessly integrating devices served by different access networks and allowing direct Ethernet procedures between them. Additionally, such enhancement enables a new approach of specific service access and group management without the need for any higher layer protocol, e.g. IP.

In 5GLAN, the Ethernet traffic flow classification must be based on Ethernet headers – Source and Destination MAC address, VLAN tags including VLAN ID and PCP, in addition to the existing fields used in Traffic Flow Templates (TFT). Thus, packet filtering and choice of 5QI should be based on Ethernet header information. The 5GLAN Group may be dynamically

created by an operator or possibly requested by Application Function via service exposure. When creating the group of devices part of the 5GLAN, the UE includes the GPSI (General Public Subscription Identifier) or SUPI (Subscriber Permanent Identity) of all UEs that are supposed to use this 5GLAN-type service. This requires an AF named Group Management Function (GMF) in the NEF (as per 23.501 section 6.2.5.0), responsible for 5GLAN Group management, including creating, modifying or removing a 5GLAN Group, according to an authorised request from the UE or the AF. The GMF is also responsible for authentication/authorization of UEs for accessing 5G LAN-type service. This GMF is part of the novel 5GLAN supported functionalities such as:

- **Private Data Network Name (P-DNN) for 5GLAN group communication:** A private DNN uniquely identifies a 5GLAN group, since all the members of the same group must establish a PDU (Protocol Data Unit) session towards the same private DNN for 5GLAN group communication. This feature will be used to define User Equipment (UE) group memberships.
- **Communication between Ethernet type 5GLAN and Ethernet:** To support communication between Ethernet type 5GLAN and Ethernet network in a data network.

In scenarios where the same service is being offered at multiple locations, the **interconnection** of the individual **Standalone NPNs (SNPNs)** is required and enables the ability to offer roaming among SNPNs. Different from the current inter-operator roaming scenarios is the deployment itself. A very large number of own administrated networks are interconnected using best effort/non-dedicated backhaul networks, resulting into a conglomerate of a huge number of small size networks with own policies. Albeit such a use case is not yet included in the standardization, it is expected that its necessity will become obvious with the increase in NPN deployments and the dynamic exchange of devices. In this context, the discovery of potential visited networks and the authorizing and authenticating devices across SNPNs is essential. FUDGE-5G will innovate on a **distributed authentication framework** to enable the roaming of UEs without requiring a strong binding between the network providers i.e. the interconnection is realized only when needed. This interconnection will be realised through an innovative Session Border Controller (SBC) enabling the exchange of control plane messages with privacy and security for the different administrative domains and with reliable inter-domain message exchange as well as through a controlled backhaul management to enable a coherent data path for home routed services. The implementation of Security Edge Protection Proxy (SEPP) will enable roaming between Public network integrated NPN (PNI-NPN) and SNPNs to facilitate seamless connectivity for end users, when moving between private and public networks.

Mobile networks currently use best-effort IP networking in the backhaul, which delivers a flat network for best effort traffic management between the radio access network and the UPF. FUDGE-5G will incorporate **5G-TSN (Time Sensitive Networking)** into its platform, via pre-provisioning resources for URLLC (Ultra Reliable Low Latency Communications), both for IP and non-IP transport. FUDGE-5G will prototype the required NFs for integrating 5G as part of an end-to-end TSN-capable network, in addition to:

- Extending the 5G SBA for adding new TSN modules.
- Utilizing SDN for network slicing in the 5GC.
- Ensuring of accurately delivery time synchronization for TSN transport.

5G Multicast is the first 3GPP technology that enables point-to-multipoint communications inside the 5G Core Network and 5G RAN. Currently being standardized in Rel-17, it is enabled by modified versions of existing 5GC Network Functions (Multicast/Broadcast User Plane Function, MB-UPF; and Multicast/Broadcast Session Management Function, MB-SMF) and an optional service layer to manage and control the multicast streams. 5G Multicast reuses existing protocol stack for User Plane communications, providing point-to-multipoint communications between the MB-UPF and several gNBs, improving network resource efficiency.

Opportunistic Multicast (OMC) defines the ability to reintroduce multicast packet delivery behaviour for unicast protocols, such as HTTP, transparently to any IP endpoint for a one-to-many communication within a 5GLAN group or across 5GLAN groups. Opportunistic Multicast is being introduced into the user plane relying on an L2-based networking fabric between UEs and UPFs. This innovation allows *n* clients that request the same HTTP resource, at roughly the same time, to receive the HTTP response as a multicast delivery through the network over L2. If all clients of the same 5GLAN virtual group are synchronised in their sending of HTTP requests and, therefore, being placed into the same OMC group for receiving the HTTP response, the cost savings over conventional IP equal the number of clients in relation to the actual UPF topology and the location of UEs. A conceptual demonstration of the opportunistic multicast capability for HTTP video delivery over a non-3GPP-integrated WiFi-based access network can be found in a video from MWC 2018 [5]. Within FUDGE-5G, OMC will be brought to the 3GPP user plane and integrated with the 5GC NF Session Management Function (SMF) for the very first time.

High Availability (HA) of the 5GC is required, when information needs to be conveyed, upon which human lives and property depend (e.g., PWS). In current public mobile networks, availability is provided by deploying systems in a redundant way, mitigating the single point of failure risk by said redundant systems. However, cloud native system architectures and services provide high availability and scalability natively, removing the need for the deployment of redundant systems. The FUDGE-5G project will demonstrate, how HA can be provided in a cloud native environment for the Cell Broadcast Centre Function (CBCF) which is used in the PPDR use case.

2. UC1 Blueprint – Concurrent Media Delivery

2.1. Motivation

5G represents a very big opportunity for the professional production industry due to its capabilities in terms of increased bandwidth, reduced latency, and guaranteed quality of service. It is also expected that standardised 5G-based solutions could bring down the costs and increase the flexibility of production workflows [6]. The media industry is engaging well with the 3GPP standardization body. The 5G Media Action Group (5G-MAG) that represents major stakeholders in the production and distribution of audio-visual media content and services has been recently appointed as a Market Representation Partner (MRP) in the 3GPP project. FUDGE-5G will introduce 5G-NPN solutions for remote production i.e., multi-camera production occurring outside of a studio context.

Several research initiatives showcased 5G as the enabler for emerging immersive media services [7], [8], [9], [10]. 5G-NPNs are also suitable to deliver immersive media services in different type of venues such as auditoriums, sports stadiums, museums, etc. to reduce and avoid the traffic bottleneck that these types of events introduce into public mobile operators. FUDGE-5G will leverage the 5GC innovations alongside the low-latency and high bandwidth throughput to provide innovative media applications such as virtual or augmented reality. Segmenting and allocating deterministic resources to services via slicing as described in section 1 ensures the coexistence of diverse type of applications under the same 5G-NPN. This catalogue of coexisting media services is the basis for the Media Showroom concept which will be implemented in the project.

UC1 Concurrent Media Delivery will showcase the viability of FUDGE-5G technologies, innovations and components **to simultaneously serve remote production and media showroom services within the same 5G-NPN deployment**.

2.1.1. Use of Non-Public Networks

The advantages of using 5G-NPNs for professional content production are [11], [12]:

- Quality of service, permitting the 5G-NPNs owner to customize their core deployment and radio modes for the different type of traffic flows inside content production.
- Public operators may not provide a suitable or affordable service for content production stakeholders. Cost and all deployment costs for SNPN are controlled by the NPN owner, including devices, RAN and 5GC components. The SNPN can be upgraded into a PNI-NPN if additional coverage or bandwidth resources are needed.
- Liability, the NPN owner is the only responsible for the 5G connectivity of their devices.
- Spectrum, allowing the use of dedicated spectrum (i.e., without any potential interference) in new bands beyond the designated ones for Programme-Making and Special Events (PMSE).

In the context of **media showroom** in venues, 5G-NPNs benefit the Venue Entity Manager (VEM) (i.e., the stakeholder in maintaining the wireless connectivity of the venue) by

complementing the existing WiFi deployment on unlicensed spectrum with dedicated 5G connectivity in IMT bands [13]. It should be noted that the same 5GC is able to serve both 5G and WiFi access points simultaneously. In the same way as existing WiFi deployments, the venue can leverage a SNPN 5G deployment for two different types of communication: enterprise or private communication services, and the other being a 5G service for their guests or attendees. It is critical that these two different types of 5G communications are isolated from each other. Guests and attendees to the media showroom connect to the local 5G network to receive an immersive media service, such as ultra-high-quality video, multi-view of a live event, or low-latency Virtual Reality (VR), etc. The 5GC forming the transport network can be customized to efficiently deliver each service separately, something not possible in a public 5G network. Additionally, the VEM can gather metrics such as location of the attendees inside the premises, interest and time spent in booths or other activities, and leverage this information to keep iterating and optimizing their service catalogue.

For both remote production and media showroom, if the vertical requires additional coverage or bandwidth, an arrangement can be done with a public mobile operator, interfacing the SNPN with the public mobile operator network and thus, transforming a SNPN into a PNI-NPN.

2.1.2. Key Pain Points

The two realizations of the Concurrent Media Delivery use case (Remote Production and Media Showroom) impose their own set of stringent requirements into the 5G system, remote production being characterized with strict user plane requirements; and the media showroom requiring additional control plane and service routing functionality. The successful integration of these intermediate phases is vital to ensure the feasibility of the use case as a whole. The key pain points are detailed next:

- Noticeable changes in video quality: this problem can appear in Variable Bitrate (VBR) situations, in which the bitrate of audio or video streams sent by the camera and received by the professional user are not constant, and depending on the end-to-end connection quality may not be enough to accommodate the bursts in required bandwidth.
- Intermittent signal: if the user bandwidth is intermittent, or the computational resources used by the core network are shared between different services, media can stop playing at some points of the stream. Reliable isolation tools for network slicing are required so each service keeps running without interruption or degradation. SNPN solves this as the network owner has full control on the resources that each service is taking, provided by the FUDGE-5G service routing feature.
- 5G-NPN deployments are dimensioned and built to specifically fulfil the network owner needs. The local spectrum regulator will restrict the 5G coverage in SNPNs (by limiting the transmitting power) to avoid interference. However, for PNI-NPN deployments, the availability of public 5G coverage close to the premises and need for commercial arrangements if public MNO segments are used may not be suitable for the private network stakeholder needs.

- 5G lacks scalability in terms of number of devices attached to an access point. There is not standardized way to deliver point-to-multipoint communications in NR. With an increase of mobile viewers in a venue, physical radio and networking resources are limited, even if private 5G spectrum is available. The network resources required to deliver the service should not grow linearly with the number of users consuming it, even if the content is very popular or the audience is concentrated under a limited area. A network level multicast solution will be explored and tested in this use case.
- Guest access management (credentials, UE configuration, network config, information service/notification portal, optional application installation, etc.).
- Parallel usage of the 5G-NPN and the usual public network; smartphone requirements. How to implement the venue 5G-NPN and let the users in? The 5G-NPN can provide roaming service and books the user into his home network. How to achieve service separation, how to manage a set of private DNS on the 5G-NPN correctly in parallel to public network.
- Trust and security issues surrounding 5G-NPN. For example; how to verify the network owner, how to authenticate the network and its components, how to protect guest data in the visited 5G-NPN, etc.
- Effort for 5G-NPN deployment and operation versus a traditional WiFi deployment; including topics as radio surveying, operations and management, costs, competences, maintenance, updates, etc.

2.2. Scenario Description

The Concurrent Media Delivery use case is composed of two differentiated parts: a Remote Production, where the captured source content from one or several 5G wireless cameras, attached to a 5G-NPN, is delivered to a remote production studio; and a Media Showroom where the realized video is offered and delivered to the audience. The use case is about combining the remote production and the media showroom in a simultaneous 5G-NPN realization. The innovation of FUDGE-5G Platform to ensure isolation between different services, while still meeting the respective KPIs and service degradation avoidance will be put to test. The rest of this section describes the two parts of the use case.

5G Remote Production

Remote production relies on collecting loss-less or almost loss-less video content from several cameras and delivering it reliably to a remote professional content production studio. These video flows must be kept in sync as much as possible to avoid discrepancies in swapping source video streams or composing the final video source. In addition to the uplink dominant camera streams, a robust downlink communication needs to be in place to carry camera equipment control information. A progressive approach from single camera to fully multi-camera remote production trial will be taken to validate the realization of 5G remote production.

5G Media Showroom

Media Showroom will showcase and validate the ability of the FUDGE-5G platform and its components to deliver immersive services featuring efficient transport network transmission techniques and dynamic service routing to many users in the same venue. The project will demonstrate a massive video and audio streaming venue room, hosted in Telenor premises with a deployed SNPN. Inside the SNPN, the media service vertical application that prepares the multimedia data (either based in HTTP formats like DASH or HLS) is installed. The packet stream is delivered to different type of displays, including smartphones, VR headsets or smart TVs. The multimedia streams are delivered using service routing at the user plane, selecting between 5G or WiFi depending on the end device capabilities. The devices will have installed a special video application to parse and display the multimedia packets coming from the vertical application. The 5GC used in this realization features components from several vendors.

2.3. Key Components and High-Level Topology

The use case aims to illustrate a typical remote production and media delivery scenario at the same time, but in this case, using 5G technology. As such, it is firmly built into the system slicing innovation of the FUDGE-5G platform. One system slice for remote production and another system slice allocated to the media showroom. Both system slices are enabled by a single FUDGE-5G platform orchestrated via the Network Function Virtualization Orchestrator (NFVO) of the infrastructure. Figure 4 shows the topology of the use case. The 5G radio is provided by 5G-VINNI featuring both sub-6-GHz and mmWave radio infrastructure. Not shown in the figure is the fact that the 5GC for the media showroom is a multi-vendor deployment.

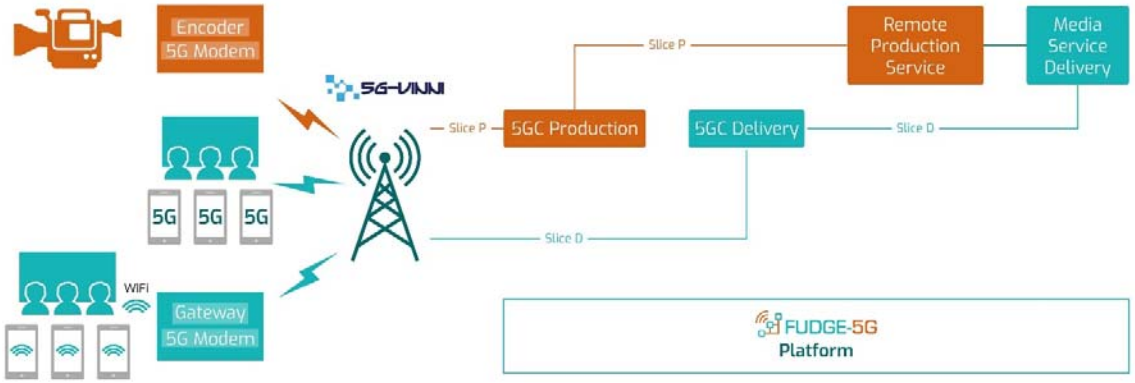


Figure 4: Concurrent media delivery high-level topology.

The remote production service also manages the timing and synchronization and distributes it to each contribution device, taking appropriate action if these values exceed certain thresholds. To enable multi-source content production, all the media equipment must be time-synchronized with the same timing source, wirelessly. Providing such time reference to all the devices needed is challenging, and the network should also be a time-aware system, so it does not interfere with the synchronization process.

5G Remote Production

The key components for remote production are shown in Figure 5. It consists of a professional camera featuring a video encoder, with a built-in 5G modem, or connected to an external one. The scenario emulates a Public Network Integrated NPN (PNI-NPN), where the professional video camera is attached into a public operator network that shares RAN nodes with a broadcaster. The remote location is where the event is taking place and it is assumed to be far from the master control room and the production gallery (these two must be interconnected). A video processing function acts as the master control room; it will be hosted next to the 5GC to process the video feed from the camera and to monitor the KPIs. Then, the video captured by the 5G camera is sent from the public 5G network into the FUDGE-5G platform, featuring on-premises 5GC. The components inside the 5GC are the minimal required to ensure end-to-end connectivity and include the Access Mobility and Management Function (AMF), Service Management Function (SMF) and the User Plane Function (UPF).

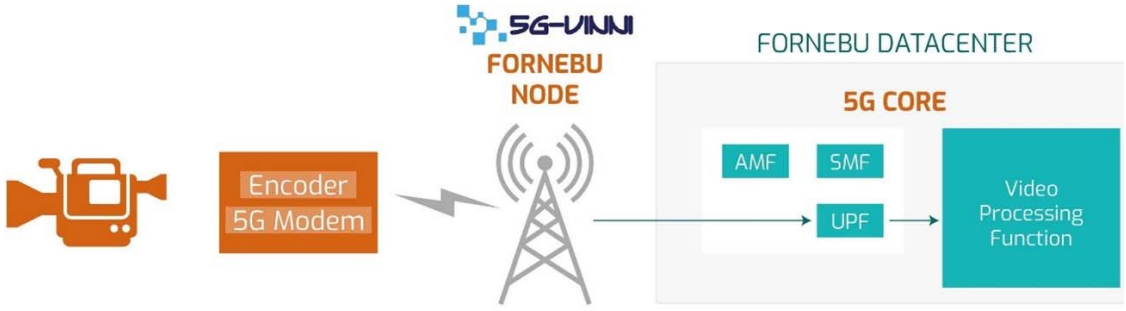


Figure 5: Content production realization topology.

Interoperability experiments with different 5GC vendors are planned for this use case. The 5GC network will have a multi-vendor setup with different vendors providing the 5GC network functions. The first multi-vendor trials include an on-premise 5G core deployment providing the user plane, interfaced with a public cloud deployment of the control plane as illustrated in Figure 6. These trials will be expanded to include additional components from different vendors and hybrid public-private cloud based on-boarding, to evaluate the full flexibility in 5G-NPNs deployments; they act as a validation in realistic environments for the components involved.

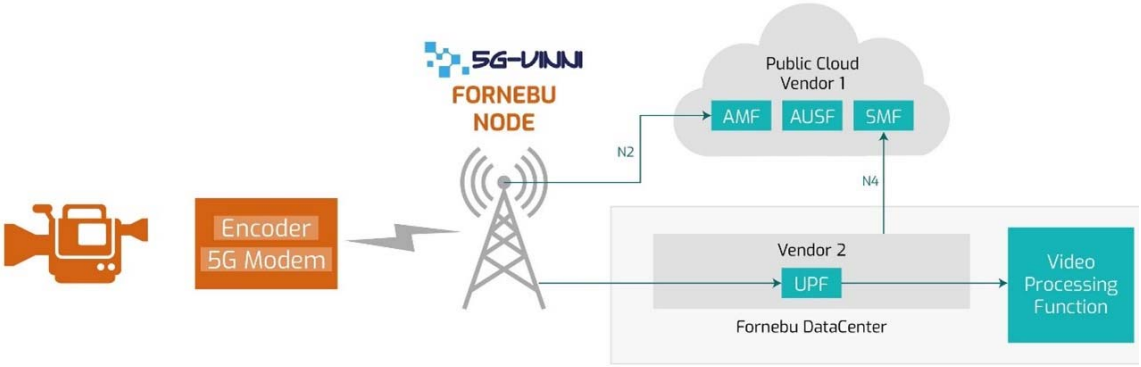


Figure 6: 5GC in the public cloud for content production.

5G Media Showroom

This realization is enabled by FUDGE-5G platform featuring service routing on the user plane with a UPF and UE implementing Name-based Routing (NbR). Furthermore, a multi-vendor SMF will be featured supporting the NbR-based UPF in its service routing capabiltiy. Name-based routing on the user plane allows the re-introduction of multicast for HTTP responses without any changes on either IP endpoint (client/server); TLS-based HTTP communication is suported too. This Opportunistic Multicast (OMC) capability requires a link local broadcast medium with packet switching capabilties implemented in software only, enabling packet delivery cost savings of up to the number of clients that request content over HTTP. In other words, for *n* clients requesting the same content over HTTP at roughly the same time, the savings over conventional IP could be *n*-fold in terms of number of packets being sent.

The service routing capabilities on the user plane comes in two modes: the infrastructure mode (UPF-to-UPF only) and the UE-mode (UE-UPF and UPF-to-UPF). Figure 7 illustrates the topology for the media showroom with a multi-vendor 5G core, distributed UPFs and two Data Networks (DNs) for hosting the vertical applications. Additionally, the Vertical Application Orchestrator (VAO) and Service Function Virtualization Orchestrator (SFVO) is illustrated enabling the orchestration of the 5GC and vertical applications.

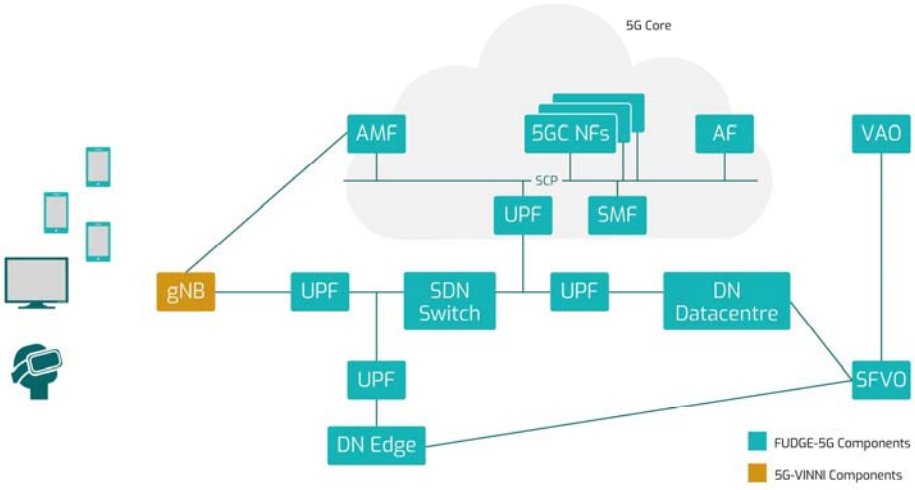


Figure 7: Media Showroom high-level topology.

The SMF is decomposed into sub functions allowing two vendors to provide the complete SMF functionality as specified in the standard, but allowing the integration of service routing on the user plane. The vertical application is a video live streamning service leveraging MPEG DASH over HTTP to allow a range of end devices to view the same video stream. As illustrated in the figure above, two DNs (data centre and edge) are available to host the vertical application allowing the geographical scaling of the service endpoints and utilising the service routing capabilties on the user plane to seamlessly switch endpoints without any interruption to the content retrieval on any UE. Also, this use case demonstrates an Service Based Interface (SBI) enabled UPF, which communicates with other NFs via the Service Communication Proxy (SCP) of the FUDGE-5G platform. Depending on which mode the UPFs are operating in the service routing capabilties can be extended

to the UEs, where all end devices require an additional software component mimicking procedures that should take place in the UE modem in a commercial product. Due to the pure softwarised realisation of the service routing capabilities, a change in the communication stack on the UE can be realised as an APK. This effort allows the conceptual demonstration of opportunistic multicast between the UPF serving a DN down to the UE for HTTP-based video delivery.

2.4. Requirements

2.4.1. Functional Requirements

This use case requires a robust and efficient network slicing implementation to ensure that the QoS is not degraded across the two services (Remote Production and the Media Showroom) which will be operating simultaneously.

Regarding the remote production, good quality in uplink transmissions is a must to meet the requirements to deliver almost lossless quality over the air. Having low latency on top could enable remote production of TV programs where the operators can control and monitor the equipment in real time. The overarching goal of this realization is to prove and validate the concept of a “mobile 5G network on demand” for remote production.

For a media showroom to deliver very high-quality content to many users while avoiding network congestion, a point-to-multipoint transport technology is required for scalability purposes. Currently, 3GPP is working in Release-17 to include 5G-Multicast support at both RAN and 5GC. The media showroom will feature Opportunistic Multicast technology, i.e., the ability to send the same HTTP response to more than one UE; and use of other access network technologies such as Wi-Fi to offload as much traffic as possible from the 5G network.

2.4.2. Performance Requirements

5G Remote Production

3GPP analysed the requirements that the next generation broadcast production standards in [14]. However, these requirements are future-looking and not feasible with existing 5G technology (Release-15 and Release-16).

Remote production operates in a delicate balance between bandwidth, latency and reliability. In detail:

- The end-to-end latency is defined as the time from the moment that an event is being captured by the camera until the video stream reaches the production. For production environments, especially for live events, the media content should be perceived in near real-time on the production facilities so that producers can make adequate editorial decisions, have direct communication with the staff in the field and provide a good viewing experience to the final clients. This parameter is also key for equipment control, such as camera focus, tally lights, etc. This parameter composed of several

terms, including video encoding latency, air interface latency and transport network latency. Overall, the sum of these terms should not exceed **100 ms**.

- Reliability is mostly affected by the air interface transmission configuration parameters and controlled dynamically in a closed-loop by the 5G UE and the gNB. Notwithstanding faulty equipment, the transport network is assumed to be error free and capable of delivering 100% of the radio packets to the 5GC. Target KPI for reliability is **Quasi Error Free (QEF)** or 1 uncorrected error event per hour at the input of the video decoder [15].
- Bandwidth for media content, especially video in contribution scenarios is very little compressed and thus requires very high bandwidth that the network uplink from the remote location to the production network should be able to handle. The required bandwidth is extremely dependant on the output of the video encoder and the added air interface error correction (which derives into reliability). The resultant throughput is multiplied by each video camera involved in the remote production. In conclusion, the air interface bandwidth should manage to handle **100 Mbps per camera** for remote production and **200 Mbps for a single 4K camera** in remote news gathering.

5G Media Showroom

Media Showroom will feature MPEG-DASH based video delivery [16], [17]. As such, the target KPIs are listed below.

- Data Throughput. It is needed to ensure high-quality user experience and constant video service. The average bit rates per programme type are specified: **8 Mbps** average for HDTV stationary device; **5 Mbps** average for portable TV; and **15-50 Mbps** for Virtual Reality Headsets (4k 360 video). Data throughput should not drop below these levels.
- Latency. **The end-to-end delay for DASH delivery should be below 10 seconds**. This value includes the time when the client has sent off the request for a DASH segment until the HTTP response has arrived with the DASH segment. DASH clients require buffering to adapt properly, and this creates an inherent delay in the content presentation (in order of seconds). All clients base their prediction, on which stream quality to choose, on the achieved throughput, latency and jitter of the connection, similarly to how TCP determines its window size. When pre-rolling the video and at run time, the DASH clients are very sensitive to time gaps in HTTP requests sent off for a video chunk and the HTTP response arriving at the UE independently from where the client is in the playout. This observation has been verified with a range of different DASH realisations (VLC, gstreamer, dash.js). On top of this, different software clients showed different behaviour depending on which stream is being displayed.

2.5. Ecosystem

The vertical stakeholder of this use case is the Norwegian public service broadcaster NRK, which will provide professional broadcaster equipment and will be involved in the

deployment and execution of the remote production and concurrent media delivery trials. Other Advisory Board (AB) stakeholders will provide cloud infrastructure. The table below summarizes the ecosystem including partners and stakeholders. Each column represents a different point in the business chain.

Table 1: Ecosystem of the media use case.

Device Application	5G Modem	Media Devices and Equipment	5G Radio & Spectrum
InterDigital	Fivecomm	NRK	Telenor (5GVINNI)

Cloud Infrastructure Provider	5G Core Network Provider	Platform Provider	Application Provider
Microsoft Intel RedHat	Cumucore Athonet InterDigital	InterDigital Ubitech	NRK

The following list details each step in the chain and the partner involvement:

- **Device Application.** Involves the associated software that a device needs to receive and parse video data. InterDigital's Android APK, which can decode name-based routing packets, will run on commercially available smartphones for the Media Showroom.
- **5G Modem.** Involves the associated hardware that an equipment needs to receive and send wireless 5G data. Fivecomm will provide their small factor 5G modem for remote production.
- **Media Devices and Equipment.** The device that captures or displays multimedia content. Remote production will explore both several types of video encoders with different codec outputs such as JPEGXS [18] and VC-5 [19] with embedded 5G modems and encoders with external 5G modem. In the media showroom, commercially available Android smartphones and Smart TVs will be used.
- **5G Radio Infrastructure.** The radio equipment and related backhaul transport network the 5G user data to the 5G user devices. Telenor will provide the 5G sites with the gNBs already deployed as part of 5G-VINNI.
- **Infrastructure Provider.** All the related computational servers, virtualization technologies, and software solutions who manage these resources. Telenor datacentre is equipped with Intel virtualization hardware. RedHat will provide operating system level solutions for containerization of the FUDGE-5G platform.
- **5G Core Network Provider.** This concept includes all the 5GC NFs required to support an end-to-end 5G communication. For the media showroom, Cumucore will provide the AMF, SMF, Authentication Server Function (AUSF), Unified Data Management (UDM), Network Slice Selection Function (NSSF), Network Exposure Function (NEF)

and Network Data Analytics Function (NWDAF), while the SMF and UPF will be provided by InterDigital. For the interoperability testing, ATH will provide all the 5GC control plane functions deployed over Amazon Web Services.

- **Platform Provider.** The platform will host all the network functions and provide the lifecycle, orchestration and service routing to manage them. Concurrent Media Delivery will make use of the name-based routing innovation and slicing as part of the platform features. The two main components forming the platform are provided by InterDigital Rel-16 Service Communication Proxy (SCP); and Ubitech's Vertical Application Orchestrator allowing the stakeholders to orchestrate their applications.
- **Application Provider.** The user plane endpoint that processes the data coming from the devices and equipment. For the remote production, it will be provided by NRK. For the media showroom, a 5GPPP cross-project collaboration is being explored to provide an HTTP-based video streaming service for a range of end devices.

2.6. Test Cases

The validation framework consists of a battery of test cases. A more detailed description of the test cases can be found in Chapter 7.

Table 2: Remote Production validation test cases.

Test case	Description	Target KPIs
1	Network Slicing Provision	QoS, Isolation
2	Delivering of realization control to the cameras	E2E latency, Reliability
3	Video streaming of professional cameras via 5G	UL bandwidth, DL bandwidth, E2E latency
4	Interoperability testing	UL bandwidth, DL bandwidth, E2E latency

Table 3: Media Showroom validation test cases.

Test case	Description	Target KPIs
1	Mass multimedia delivery	DL Bandwidth, E2E Latency, Scalability
2	Mass File Delivery (e.g. Application update)	DL Bandwidth, Scalability

Table 4: Concurrent Media Delivery validation test cases.

Test case	Description	Target KPIs
1	Video streaming of professional cameras via 5G	UL/DL bandwidth, E2E latency

2	Mass Video Delivery of live content	DL Bandwidth, Scalability
3	Network Slicing Provision	QoS, Isolation

2.7. Expected Outcome

The two realizations of this Concurrent Media Delivery use case (Remote production and media showroom) will produce results and findings in different fields. Remote production innovations reside in the User Plane, while media showroom outcomes will be related to Control Plane novelties. In detail:

Remote production does not require big innovations in the control plane, nevertheless the stringent requirements on the user plane will solidify 5G-NPNs solutions as a competitor to expensive wired deployments between outside broadcasting vehicles (OB van) and the site of interest. The execution of the remote production trials will provide the experience and insight to transform 5G into the new de-facto standard in contribution equipment for professional content production and its adoption by broadcast stakeholders. The components showcased within this use case will be proven to be capable of handling content production scenarios.

Similarly, the media showroom trials will demonstrate a 5G cellular telecommunication system utilising 5G NR. However, it must be noted that with no broadcasting capability available on the access network and with GTP-U in place between the UPF and gNB, the FUDGE-5G platform cannot demonstrate the OMC innovation on the physical medium, as FUDGE-5G has inherited a unicast access network which it is unable to change. However, the OMC benefits can be directly measured and demonstrated on N6 and N9 and on N3 and the access network when only looking at the payload of PDU sessions.

2.8. Risk Assessment

Table 5: Risks of the media use case.

Risk description	Likelihood (L / M / H)	Impact (L / M / H)	Risk Mitigation
5G-Multicast radio solution is not standardized	L	H	The FR_MBS Work Item has been approved in Dec 2020. FUDGE-5G will explore non-3GPP multicast solutions in case the Work Item experiences delays
NR uplink capabilities not enough for Content Production	M	M	If the use of default NR cannot meet Content Production requirements; advanced and optimized radio technologies like Bandwidth Parts and SuperUplink will be used.
Devices for mmWave 5G are not stable	M	L	In case stable mmWave devices are not available, sub-6 GHz equipment will be used
Concurrent Media Delivery is not possible due to service degradation	L	H	The isolated network slices brought by cloud-native FUDGE-5G platform can ensure that each component demanded resources will not be violated.

3. UC2 Blueprint – PPDR

3.1. Motivation

ICT (Information and Communications Technology) represents today one of the essential components for coordinating and handling PPDR (Public Protection and Disaster Relief) operation. The complexity of these operations is such that typically several entities are involved, with **a diversity of actors deployed for different types of events – sometimes in isolation, other times in a coordinated fashion**. Thus, the capability of exchanging information quickly in such complex theatres represent a decisive factor for first responders and deployed forces. ICT solutions must enable their efficient coordination at operational, strategic and tactical level. **Communication is the key enabling factor for coordinating different entities, such as information sources and actuators, towards a common set of goals, in order to fulfil the mission objectives.**

Successive evolutions in telecommunications standards have enhanced the means to exchange information faster, further and with lower failure rates. At the same time, advances in computing capabilities have allowed new kinds of information sharing, ranging from live audio/video, image recognition, and real-time telemetry. Combined together, telecommunications and computing represent the keystone to improve the capability of first responders and law enforcers to collaborate. In Europe, today's prevailing communication technology for PPDR is TETRA (TErrestrial Trunked RAdio) which falls short of satisfying the requirements for broadband. Thus, the PPDR community has investigated the transition to 4G (LTE) in order to leverage its broadband capabilities. Nevertheless, unlike legacy systems natively designed for PPDR services (TETRA, TETRAPOL, P25), **4G was originally not designed for PPDR**. Therefore, the 3GPP initiated specific standardization activities for PPDR, via the definition of several "enablers" and the creation of a dedicated group SA6 for Mission Critical applications. This materialized first in Rel. 13, with a first version of MC-PTT (Mission Critical Push to Talk) and continuously enhanced up to Rel. 16 addressing Mission Critical Services (MCS), i.e., Mission Critical Data (MC-Data) and Mission Critical Video (MC-Video).

Future PPDR systems aim at establishing a rapidly deployable broadband infrastructure on the field. Hence, PPDR systems shall meet the demands for **voice** (e.g., 1-to-1, push-to-talk, conference), real-time **video** communications (including video broadcasting), **tracking** of deployed forces (e.g., vital signs and positioning) and sensors (e.g., fire, water, gunshot detection), together with high-speed **data transfer** for dealing with natural and man-provoked disasters. Unlike commercial networks, PPDR systems must guarantee the **prioritization** of traffic (including the implementation of different priority classes, queuing, congestion management and protection strategies). One key capability is the dynamic **pre-emption** of (possibly) already allocated resources in case of high network load to steer them towards fulfilling the higher priority services (e.g., higher priority slices). Moreover, **security** needs to be ensured from the end-to-end perspective, including network management, user/control planes, and up to devices. This will allow creating **situational awareness**, that is, the digital re-construction of the interaction between individuals, objects and the

environment within a limited geographical perimeter, which is instrumental for PPDR forces to plan and engage action in a precise and timely manner.

The main challenge for FUDGE-5G is to provision mission-critical services transparently to the end-user and independently of the underlying telecommunication infrastructure. One additional technical challenge is to ensure that mission-critical voice communication is as robust as in current TETRA systems. Another challenge is to ensure first responders to be able to access critical information and communicate with each other during crises, even when commercial 5G networks are down or likely crowded by many individuals attempting to use them.

3.1.1. Use of Non-Public Networks

In this UC, we consider a 5G NPN deployment conforming alternatively a SNPN and a PNI-NPN, where the PNI-NPN is owned and managed by the PPDR agency but resides alongside with a PLMN. The standalone option increases coverage in the form of a mobile 5G connectivity bubble deployed during catastrophes, such as hurricanes or wildfires destroying infrastructures, or terrorists taking hostages. Here the goal is to provide quickly and independently from other networks, local connectivity, with specific access control policies to specific business applications with dedicated performance, QoS settings, as well as isolation. A hybrid scenario is then envisioned to extend the capabilities of the PPDR NPN when the situation is stabilized. Network slicing enforced by orchestration allows retaining the same set of KPIs and performances as in the standalone case.

Regardless of the selected approach, an NPN suitable for PPDR operations, when compared to PLMNs will have to guarantee always higher levels of availability for incident management, the support for deployable base stations, dynamic prioritization of traffic, congestion management and an enhanced security. While for some cases, the use of a PLMN complemented by specific prioritization policies might be sufficient, most PPDR users prefer retaining full independency of their network due to **security and availability levels consideration** and the need to **fine-tune coverage** according to their needs.

3.1.2. Key Pain Points

Mission critical communications for PPDR require being specifically reliable, resilient, secure, and easy to deploy and manage. Existing key pain points are the following:

- Difficulty in having as much as possible zero touch automation and setup of the network and related PPDR services. Typical end users are not technology experts, thus they expect that the communication system just work when needed, with a special focus on uptime.
- Stringent deployment latency and fast-response systems due to the specific operational environment.
- Need for lightweight solutions, with reduced complexity that could yield various points of failure or bottlenecks in the system. In addition, the system should be as much as possible autonomous, local, and independently from the availability of a backhaul.

- Deliver increased reliability requirements when compared to commercial networks, supporting both legacy TETRA functionalities (e.g., push-to-talk, group communications, direct mode), and next-generation ones (mainly broadband) at a lower TCO than current tailor-made solutions.
- Customize and enforce the required characteristics, priority levels, and pre-emption for a plethora of critical services in an easy way.
- Lack of interworking and interoperability between NPNs and public networks, and even between multiple NPNs deployed by different agencies.
- Privacy/security of information exchanged has to be enforced in any situation due to the critical nature of communications involved.
- Handle possible disconnections, unavailability of parts of the network. Ensure that communications can continue, even in case of network partitioning (e.g., PACE, local communications).
- Having one hardware solution size (that includes the antennas, power amplifiers and supplies, the computing equipment) for different missions is a strong limitation in terms of operational efficiency. Thus, the solution must be adaptable to different hardware footprints.

3.2. Scenario Description

The PPDR use case developed in FUDGE-5G aims at evaluating and demonstrating whether the advancements brought by 5G networks and their evolutions are fit the purpose of being deployable during relevant PPDR operations. In this context, the use case plans to: 1) **identify current technological limiting factors**; 2) **quantify** how much public safety organizations can **benefit from 5G networks**; and 3) provide **useful hints and roadmaps** for adopting and adapting 5G technologies to PPDR systems.

The scenario foresees a group of first responders deployed in a fictional theatre of operations. The scenario involves using **voice on-demand** (including 1-on-1 and group calls) for coordination between participants on the field, simultaneous **streaming** of multiple high-definition videos for situational awareness, and **data exchange** (e.g., maps, locations, messages, sensors and other relevant information). Each flow is subjected to strict **QoS requirements** and **security policies** in terms of traffic isolation and available resources. Depending on the type of data exchanged, communications can be either exclusively local - between group participants only - or remote - between the group and external entities, such as a remote command and control post or an application server deployed in the cloud.

FUDGE-5G foresees the use of very compact and portable solutions, which can be carried in various forms according to the envisioned use case, e.g., a backpack or a box in a vehicle, and just need to be powered on by the end users to start working. Therefore, the key features included in this equipment should be **the access radio cell and the core network components, possibly virtualized in the same box with other mission-critical applications**.

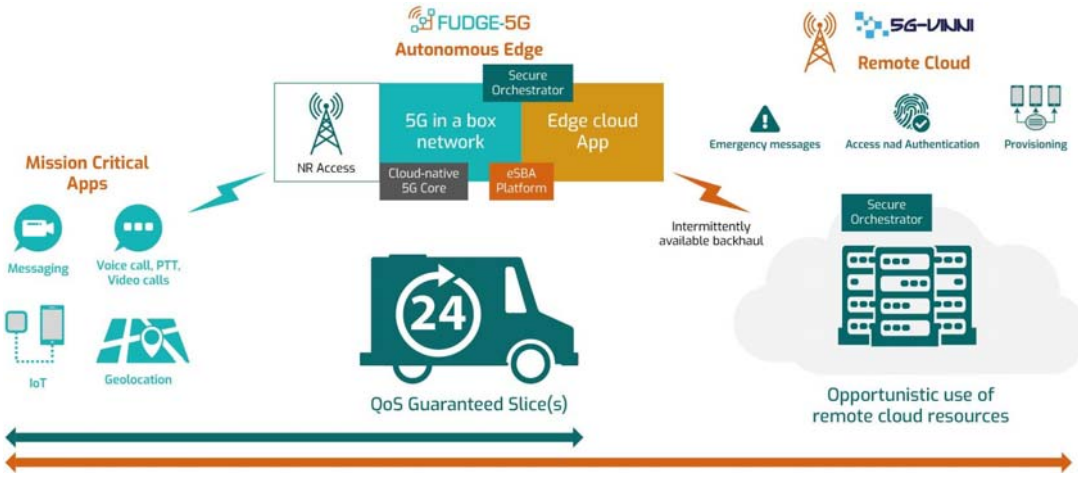


Figure 8. High-level vision of the PPDR use case.

Figure 8 proposes the high-level architecture for the use case, including the main building blocks and their intended locations. It highlights the capability of creating self-contained and mobile 5G connectivity bubbles, with both communication and local computing capabilities. The 5GC realization consists in the integration of an **autonomous 5G edge** platform capable of hosting a radio head, a gNB, and a computing platform running a cloud-native 5G core alongside several edge cloud applications, all of them deployed in a van. The autonomous edge hosts a service orchestrator agent as well, to take care of automation, lifecycle management and dynamicity. The use case also considers the **interworking between the autonomous edge and a remotely connected cloud site**. This use case will employ custom differentiated traffic processing in terms of traffic priorities, availability of computing and radio resources, redundancy, security levels such as for MC-PTT, MC-Video and MC-Data.

Within this high-level vision, we further break down the PPDR UC in three sub-scenarios, with each one of them highlighting different technical challenges and operational aspects.

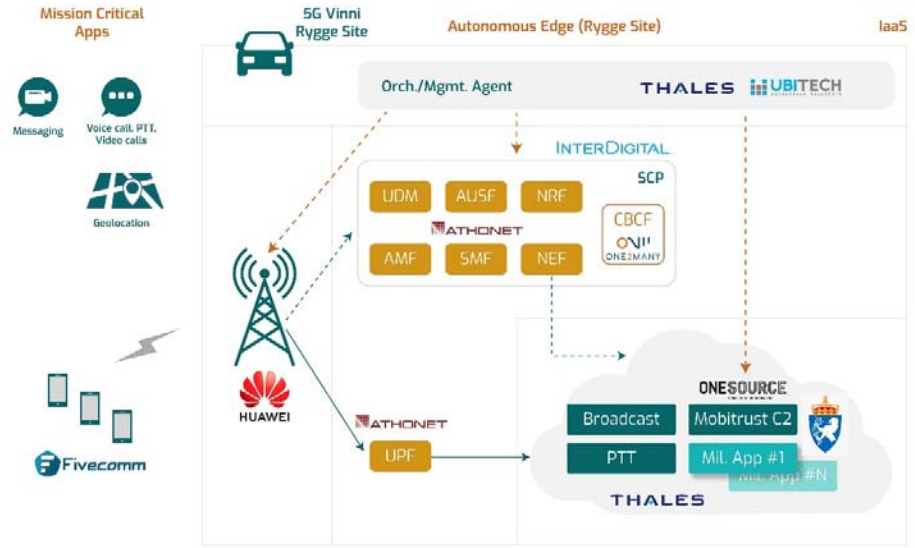


Figure 9: PPDR use case Topology of Scenario 1.

PPDR Scenario 1: 5G core and cloud applications deployed in FUDGE-5G mobile autonomous edge

This scenario focuses on the **integration of the mobile autonomous edge** to deploy a tactical bubble providing a fully autonomous and deployable non-public 5G network. The autonomous edge shall be deployed and set up in a reduced time to ensure 5G coverage around a specific mission-critical field of operations such as terrorist attack, war or natural disaster. The tactical bubble is aimed for up to few hundred users from the emergency services and the military. By providing a fully functional 5G network embedded in a mobile edge, FUDGE-5G will offer broadband communication capabilities to first responders and Special Forces even in the case of remote deployments. This realization will highlight the ability of delivering non-public 5G networks anywhere, as well as supporting PPDR operations with the most flexible deployment possible. The objective of this scenario is to demonstrate the simplicity of setting up, configure, and provision an all-in one 5G system utilizing local instantiations of a 5G RAN, core and cloud applications based on cloud-native principles in a standalone node. Via the capability offered by the FUDGE-5G Platform, the cloud application components of the system can also adapt to the current conditions (e.g., local scale-up, scale-down). The provisioning of local users' databases is made effortless via the orchestration layer.

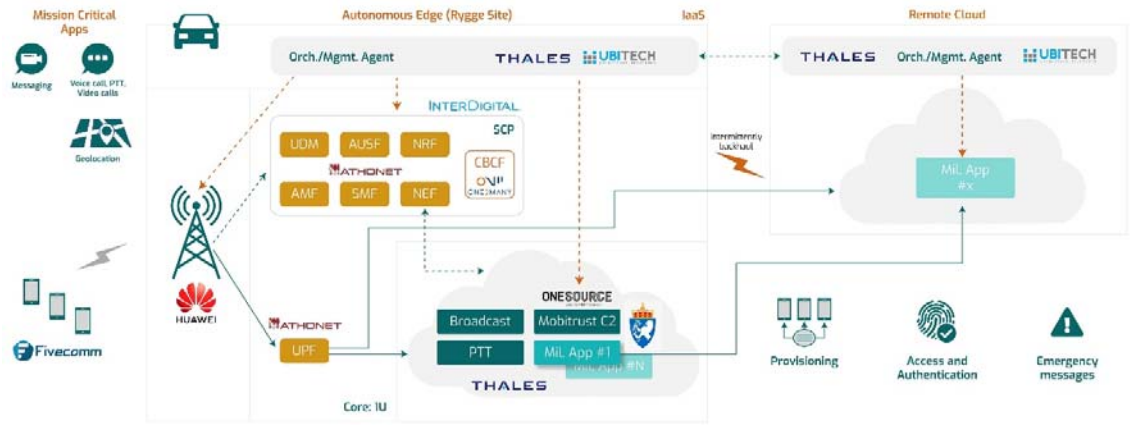


Figure 10: PPDR use case Topology of Scenario 2.

PPDR Scenario 2: Intermittent backhaul connectivity and heterogeneous deployment

This scenario demonstrates the flexibility of the FUDGE-5G solution to enable opportunistic use of an intermittent backhaul link between the autonomous edge and a possibly remote cloud. Indeed, cloud applications, once instantiated on the autonomous edge, are intrinsically constrained by the limited availability of resources (e.g., in terms of available cores or RAM). For this reason, in this scenario we explore the possibility of leveraging a remote cloud to provide additional processing capabilities. By integrating a common orchestration framework, it is possible to extend the reach of the non-public 5G network on the autonomous edge up to a remote cloud, where replicated, or totally different, instances of cloud applications may have fewer resource constraints. This implies first deploying and managing one or more PPDR-specific logical slices connecting the

autonomous edge to remote cloud. Additionally, the orchestrator is tasked with balancing the use of local resources (always available at the autonomous edge) when in fully standalone mode, and cloud resources (opportunistically available at the remote cloud), when a backhaul connectivity is available. Switching between these two modes must be as automated, transparent, and seamless as possible for the user. One specific example of already identified cloud application benefiting from this process is gunshot detection in federated learning scenarios. It has to be noted that this kind of arbitration, while in principle possible for all virtualized functions, should be limited to non-critical ones. For this reason, in this scenario, we do not consider shifting 5G core functions, and we limit ourselves to cloud applications on the user-plane.

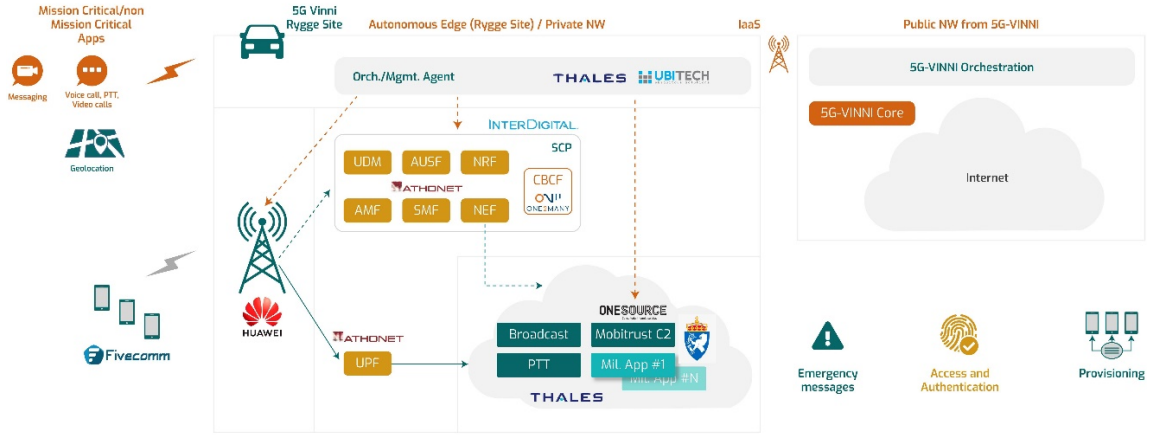


Figure 11: PPDR use case Topology of Scenario 3.

PPDR Scenario 3: Coexistence of public and non-public networks

In this scenario, we focus on **the coexistence of multiple public and non-public networks that offer different services (mission critical or not) to PPDR users**. This is a very common operational scenario, where PPDR end-users might benefit from using their terminal for non-mission critical services for their mission (for example carrying out a web search, or accessing a global mapping service). In this case, we consider the case where a single PPDR device can connect to a network (or multiple networks) serving multiple slices. One slice gives access to a public macro cell offering best-effort Internet access. The other slice is served by the FUDGE-5G autonomous edge, providing local connectivity to specific mission-critical services and applications deployed at the autonomous edge. A terminal configured and authorized to access the mission critical slice can work with specific mission critical applications by exploiting the proximity to the autonomous edge and the specific guarantees provided for the mission critical slice (e.g., Improvement of security, prioritization). On the other hand, the same terminal shall also be able to access the public slice, to accomplish less critical tasks, such as browsing the web and scraping information. For such specific case, the scenario requires the terminals to support secure enclaving of applications, in order to avoid cross poisoning among slices having different security properties.

3.3. Key Components and High-Level Topology

3.3.1. Key Components

Autonomous Edge Platform. The edge platform allows running the virtualized core and the cloud applications close to the user. It is composed by a hardware-based edge-computing device in 1U rack-mounted server hosting multiple server-grade CPUs, memory and disk resources. It also hosts a hypervisor and a local orchestration system for automating the management of deployed VMs and containers.

Network and Service Orchestrator. Two orchestrators work together providing the end-to-end orchestration at cloud, core, edge, RAN levels:

Ubitech Vertical Application Orchestrator (VAO). The Vertical Application Orchestrator (VAO) is a sophisticated platform that enables distributed applications composition and cloud services orchestration. It is an advanced developer framework for cloud orchestration and infrastructure automation that gives you the power to design, deploy, and manage cloud-native containerized components in both public and private cloud environments. It comes with advanced off-the-shelf features to support extensive monitoring, security enforcement, elasticity management, and operational analytics.

InterDigital's Service Function Virtualisation Orchestrator (SFVO). The SFVO offers location-aware cloud-native SLA-driven orchestration of 5G services, e.g., a 5G core or a vertical application, is an integrated part of the FUDEG-5G platform, and is utilised by the 5GC vendors as well as the VAO to orchestrate services.

Thales Secure Slice Orchestrator. The secure slice orchestrator is in charge of automating both the deployment and the runtime management of the lifecycle of end-to-end slices. Its main role is to provide a unified view and management of the deployed end-to-end services and to guarantee the differentiated SLAs of each slice. The orchestrator interacts with the RAN, the core, the transport, and to the cloud components via specific adapters (mostly based on REST APIs). Runtime decisions follow a policy-based approach driven by a telemetry layer.

5G Radio Access - Huawei gNB. Radio access implements the radio access technology.

5G Core components. The core network components are composed of software instances deployed over the autonomous edge. They are:

- **Athonet Mobile Core.** A full on-site core network solution transportable and interoperable, specifically tailored for the deployment of mission critical 5G networks. The Athonet mobile core delivers an agile, secure, reliable, and highly performing mobile networks for critical environments. Additionally, it is field-friendly, meaning that operators and IT personnel in the field can manage it without requiring specific telco knowledge and training. Moreover, the solution can be adapted from small field areas to nationwide coverage and supports a large set of applications, including group calls, audio/video dispatch, critical alerts etc.

- **Public Warning System – One2many Cell Broadcast Centre Function (CBCF).** The public warning system solution consists of a portal (deployed as cloud), on which warning messages can be created and delivered to the Cell Broadcast Centre Function (CBCF) NF deployed in the 5G Core.
- **SBA – InterDigital Service Communication Proxy.** The Service Communication Proxy (SCP) provided by IDE enables fast and adaptive service routing among 5GC NFs following the description of D1.2 [1]. IDE's SCP is one of the three deployment options mentioned in TS23.501 and implements Name-based Routing, an Information-centric Routing approach transparently allowing a change in consumer – producer instance relationships. This ability enables seamless change in lifecycle management states of producer instances without affecting the consumer assuming all NFs have been implemented as CNFs.

Cloud Applications. Cloud applications represent the endpoint processing. They can be deployed either at the autonomous edge or at the remote cloud. We envision utilizing the following:

- **MC-PTT Server.** Push to talk is a feature used in group communications where the same communication can be received in many devices originated from one source. Communication groups can be formed freely under the network. Communication can be text, voice or video. Since point-to-multipoint radio transmission is still in the study phase for 5G, and eMBMS has elements not compatible with 5G, the MC-PTT feature will be initially implemented based on unicast communications.
- **OneSource Mobitrust platform.** Situational awareness Command & Control (C2) platform for monitoring, accessing and processing data from different types of sources. These include GPS positioning, man-down detection (and body position) with accelerometers and gyroscopes, ECG and RR via wearable devices to control vital signs, environment sensors (e.g. gases, temperature, etc.) to quickly detect hazardous environments and conditions, and also a communication channel with on-demand video and audio in real-time.
- **Thales FeedSync server for chat and positioning application.** FeedSync platform provides a professional, modular and secured chat + positioning application for first responders, focusing on group communications. FeedSync is capable to manage disconnections and interruption, specifically designed to deploy new servers close to the users (e.g., on the autonomous edge) and allowing D2D communication opportunities.

NDMA Military Application Services

- **HERMOD.** Application with DNS/Registry function to keep track of military HERMOD nodes in the 5G network. When a new HERMOD node is attached to the 5G network, it should be possible for the nodes to communicate directly. HERMOD is already running as an application Function in the 5G-VINNI network today. When there is connectivity between FUDGE-5G and VINNI networks, the HERMOD nodes should be able to find each other across the two networks.

- **BMS Message Hub.** Blue Force tracking/Battle Management System (BMS). BMS Message Hub will also run in the 5G_VINNI network. Users in both VINNI and FUDGE network should be able to see each other (BFT), when there is connectivity between the two networks**.**
- **Gun Detection System (Triangula).** Crowd-sourced gunshot detection application running on at least three end-devices actively listening for gunshots. When a gunshot is detected the GDS service returns position (triangulation) of the shooter and weapon type (via AI/ML processing). GDS service will also run in the 5G-VINNI network. When backhaul connectivity is available between the two networks it will also be possible to do triangulations on the smartphones attached to different networks (5G-VINNI and FUDGE-5G) with better precision.

5G UEs. The 5G UEs represents the set of devices used by PPDR users to communicate. In this UC, we will use the following**:**

- **Fivecomm 5G modem.** The 5G modem to be used in the PPDR use case is a hardware-based device that provides sub-6 GHz connectivity. The modem can be used in a long range of frequencies (n1, n3, n28, n41, n77, n78 or n79, among others) and supports both non-standalone (NSA) and standalone (SA) modes (option 3x, 3a and 2 network architectures). Additionally, 5G connectivity can be shared locally via Ethernet using time-critical hardware, with the objective of fulfilling the required low-latency requirements. External or integrated antennas can be selected, according to the specific needs of the use case.

3.3.2. High Level Topology

The Autonomous Edge in a van will host most of the components of the UC. The baseline topology for all three scenarios is common to the three scenarios.

A 5G Core, composed of both Control- and User-plane functions will be deployed as an all-in-one software solution on the Autonomous Edge alongside with multiple cloud edge applications (including the C2, communications, and specific applications). On top of that, a CBCF function will be employed to broadcast public warning messages. The 5G core will be connected to the local RAN, which is provided as softwarized gNB and integrated on the van as well. PPDR team members will use 5G modems on the n78 band to connect with the Autonomous Edge and will have on their device mission critical applications (e.g., PTT, chat, video, map, …). Then, depending on the specific scenario under test, the topology will be enriched as follows.

Scenario 1: **5G core and cloud applications deployed in FUDGE-5G mobile autonomous edge**

Scenario 1 focuses on the capabilities of the autonomous edge deployed at the FUDGE-5G Rygge site. Initially, both 5G core and cloud application components are instantiated locally via common IT automation tools (e.g., Ansible) and without any lifecycle management strategy in place. At a later stage, the orchestrator agent will be integrated into the autonomous edge allowing adaptation and scaling of deployed components at runtime.

Scenario 2: Intermittent backhaul connectivity and heterogeneous deployment

This scenario will focus on the interconnection of the user plane with a remote cloud data centre. In this case, the topology also includes the connection with a remote cloud data centre managed by an orchestrator agent. The orchestrator is in charge of providing end-to-end service-level guarantees on the user-plane. The remote cloud runs a replica of a service application that represents the endpoint for the user plane.

Scenario 3: Coexistence of public and non-public networks

This scenario will focus on the coexistence of multiple public and non-public networks that offer different services (mission critical or not) to PPDR users. In this case, the topology includes an alternative to the FUDGE-5G NPN, represented by the 5G-VINNI PLMN providing non-critical services, which can be accessed by PPDR users alongside the critical services provided by the autonomous edge (which in turn is dedicated to critical services).

3.4. Requirements

3.4.1. Functional Requirements

Table 6: PPDR use case functional requirements.

Scenario	Requirements
Scenario 1.1	#1 The system shall be able to deploy a full 5G network in the FUDGE-5G autonomous edge. The platform shall be dimensioned for running RAN, core VNFs, and edge applications in a fully standalone configuration
	#2 Devices and antenna shall be capable of using the same sub-6 GHz frequency bands
	#3 The system shall be able to automate the provisioning of RAN configuration, core functions, and cloud applications
	#4 The system should be easy to configure and run for a user, including primitives for zero touch deployment
	#5 The system shall support PTT service, localization (BFT), chat, vital parameters monitoring (IoT-like) applications, public warning broadcast, and video processing deployed as local cloud applications
	#6 The system shall have the capability to issue public warning messages to all devices in radio coverage
	#7 The system shall be able to define and configure end-to-end slices via the allocation of radio, network and cloud resources to the critical applications with different capabilities (including radio bearers, expected bandwidth, availability, priority, etc.)
	#8 The system shall have the capability to route specific application-related traffic over their correct slice
	#9 The system shall provide an access control for the mission critical slices to guarantee that only authorized users can access them
	#10 The system shall guarantee the appropriate level of security and privacy to data in transit, preventing both passive and active eavesdropping and tracking of user identifiers

	#11 The system shall guarantee security between deployed NFs and between the user and the application instances by using mandatory security mechanisms such as TLS and OAuth
	#12 The system shall be able to pre-empt already deployed resources from low-priority slices to reliably serve higher priority slices
	#13 The system shall be dimensioned to deploy an orchestrator layer at the autonomous edge on top of RAN functions, core NFs, and edge applications
	#14 The system shall keep track of the resources used and the load per function/application
	#15 The system shall be able to autonomously scale up and down NFs and applications as function of the observed load. It has to be capable to enforce different redundancy levels depending on service characteristics
	#16 The system shall be able to migrate existing traffic flows over the different instances of NFs and applications as function of the observed load
	#17 The system shall enforce dynamically network slices requirements (expected bandwidth, availability, priority, etc.)
	#18 The system shall provide an access control for the creation of slices, by taking into account the available resources at radio, core and application domains and the relative priority levels
Scenario 2 (Delta wrt. Scenario 1)	#1 The system shall have the capability to provision cloud applications over a remote cloud (e.g., ML learning applications for video processing)
	#2 The system shall monitor in real time the availability and performance of backhaul link(s)
	#3 The system shall have the capability to steer user traffic dynamically to different DN programmatically (in this case depending on the availability of a backhaul link)
	#4 The system shall have the capability to enforce end-to-end slices terminating either at the autonomous edge, or at the remote cloud
	#5 The orchestration of application instances at the autonomous edge shall allow maintaining the operability when the backhaul connection is unavailable.
Scenario 3 (Delta wrt. Scenario 1 & 2)	#1 A device shall be able to connect to be served by multiple slices from different networks at the same time
	#2 A device shall be able to support multiple slices over different RANs and core networks (e.g., having different PLMN ids)
	#3 A device shall be able to securely isolate applications whose traffic is served by different slices
	#4 The system shall be able to define and enforce different slices over different networks
	#5 The system shall be able to separate network traffic over PPDR (mission-critical slice routed to the autonomous edge) and public networks (best effort slice routed to the 5G-VINNI macro)

3.4.2. Performance Requirements

Table 7: PPDR use case KPIs and application-related performance requirements.

Application	KPI name	Description	Measurement unit

Voice	Mouth-to-ear latency	The time between an utterance by the transmitting user, and the playback of the utterance at the receiving user's speaker (both for PTT and group calls)	ms
	Late call entry time	The time to enter an ongoing group call measured from the time that a user decides to monitor such a group call, to the time when the UE's speaker starts to play the audio	ms
	Access time	The time between when a PTT user request to speak and when this user gets a signal to start speaking.	ms
	Concurrent calls	The maximum number of concurrent person-to-person and PTT calls that the system can handle	number of concurrent calls
	Users in a group call	The maximum number of users in a PTT group call	number of users
Video	Throughput	The measured average data rate to support highest resolution video formats	Mbps
	Latency	The time between when a video stream is captured and when the user receive the stream	ms
	Late stream entry time	The time to enter an ongoing MC-Video stream measured from the time that a user decides to monitor such a MC-Video stream, to the time when the UE's scree, starts to play the video	ms
	Concurrent streams	The maximum number of concurrent MC-Video streams that the system can handle	number of concurrent videos
Messaging / Facsimile	Latency of distribution	The time required to distribute a message to all members of a distribution group	ms
	Delivery failure	The number of messages that were not delivered after the delivery deadline	number of times
Location	Localization latency	The time between the localization reading by a user device and the visualization over a remote C2 screen	ms
Public warning broadcast	Coverage	The maximum distance where a device to receive the public warning message	km
	Initialization time	The time to setup the public warning message network service before it being operational	min
	Public warning latency	The time required to distribute a public warning message to the last device receiving it	ms
Vital signs monitoring / telemetry	Monitoring latency	The time between the vital signs readings by a user device and the visualization over a remote C2 screen	ms

Data	Data Rate	The speed at which data is transferred between the source and its destination device	Mbps

Table 8: PPDR use case KPIs and platform-related performance requirements.

KPI name	Description	Measurement unit
Autonomous edge installation time	The time to provision and install autonomous edge, including, HW, SW, interconnection of components, configuration (all of day -1 operations)	days
Management framework footprint	The minimum (recommended) HW requirements for all the management (VIM, orchestrators) to run properly	CPUs GB of RAM GB of storage
Service establishment time	The elapsed time to setup a specific network service before it being operational (from the deploy command)	min
Orchestrator discovery time	The time required to discovery a new orchestrator entity	sec
Single touch orchestration	Minimum number of workflow interventions to setup the autonomous edge software stack	number of interventions
Scale-up latency	The time before a scale-up operation is completed in case of a lack of resources	sec
Number of slices	The maximum number of slices concurrently supported by the system	number of slices

3.5. Ecosystem

The hardware blueprint of the autonomous edge platform is composed by a radio access gNB and the NFVI edge. For the particular use case realizations of FUDGE-5G, we will make use of a 5G gNB from Huawei Norway and of a NFVI edge platform to be provided by Advisory Board stakeholders. Initial integration and validation activities will be realized on both OpenStack and Kubernetes-based platforms. Athonet supplies the core network functions, while One2Many provides the public broadcast function. The service-based platform is enabled by Interdigital in the form of service routing capabilities among 5G core functions. Thales and Ubitech focus on the automation and dynamic management of deployed slices via their orchestrators (specific to Scenario #2).

On the other hand, Telenor acts as premise provider in Fornebu, hosting the equipment for the remote cloud (for Scenario #2) and the macro 5G network (for Scenario #3) through its 5G-VINNI platform node (currently based on a Microsoft Azure PaaS solution). End devices will be either COTS 5G smartphones or computing devices (PCs) connected to 5g modems supplied by Fivecomm. At application level, One Source provides the Mobitrust platform as a C2, Thales deploy the FeedSync chat and location server, NDMA provide multiple defence-related applications and notably a gunshot detection application. Cumucore provides the

application stack for PTT communications. Depending on the scenario, application services can run either at the autonomous edge or at the remote cloud.

3.6. Test cases

There are multiple test cases, each one of them focusing on the requirements of one or more scenarios. The test cases are presented below, and detailed in Chapter 7.

Table 9: PPDR test cases.

Title	Description
Basic connectivity test (Scenarios 1-2-3)	The team deployed on the theater can ping an applicative server deployed either at the autonomous edge (Scenario 1), at the remote cloud (Scenario 2), or on the public network (Scenario 3)
Push-to-talk communications between a group of (locally) deployed forces (Scenarios 1 - 2)	The team deployed on the theater has the capability to stay in contact during the operation via PTT communications over 5G. The PTT application is deployed either at the autonomous edge (Scenario 1) or at the remote cloud (Scenario 2).
Group video call between deployed forces and a C2 operator (Scenarios 1 - 2)	A member of the deployed team can stream video from the field to the other member of the team and back to a C2 operator. The C2 application can be deployed either at the autonomous edge (Scenario 1) or at the remote cloud (Scenario 2).
Group chat with BFT and situational awareness update (Scenarios 1 - 2)	Deployed forces can share their live position and situation awareness data (captured photos, videos, and audios) in order to help reconstruct the hostile environment. The BFT server can be deployed either at the autonomous edge (Scenario 1) or at the remote cloud (Scenario 2).
Live tracking of health data from deployed forces (Scenarios 1 - 2)	All the sensors on the people in operation are connected to the C2, so it is possible to subscribe to alerts from sensor readings and to evaluate the status of each team component. The C2 application can be deployed either at the autonomous edge (Scenario 1) or at the remote cloud (Scenario 2).
Broadcast warning messages to all end-devices in coverage (Scenario 1)	The staff on the C2 can send a warning message (audio, text) to warn the population of an ongoing operation.
Crowd-sourced gun-detection system (Scenarios 1 - 2)	The team can use their end-devices as a triangulation mechanism to discover the orientation and position of a gunshot. The devices continuously overhear and use a triangulation server to discover the position and the type of weapon. The application can be deployed either at the autonomous edge (Scenario 1) or at the remote cloud (Scenario 2).
Intermittent connectivity with remote cloud (Scenario 2)	A non-mission critical vertical application (e.g., gunshot detection or messaging server) is instantiated at the autonomous edge. Once connectivity is restored with a remote cloud, the orchestrator agents negotiate and automate the provisioning of the same vertical application on the cloud shifting traffic there. In case of disconnection, local traffic is immediately re-routed back to the autonomous edge instance by the local orchestrator.

Simultaneous use of NPN and PLMN (Scenario 3)	The same component of a deployed team is capable of using a mission-critical service provided via the FUDGE-5G autonomous edge (e.g., MC-PTT communications), but also a non-critical service provided over a PLMN (e.g., web browsing).

3.7. Expected Outcome

The first scenario will validate the concept of a fully standalone "Mobile Autonomous 5G Edge" proposing localized 5G NPNs that can be used by emergency teams in their operations, usually deployed in vehicles. Main technical realizations consist in providing the integration of different components (including control-, user-plane functions, and cloud applications) developed in the FUDGE-5G consortium and integrated together in a low-footprint form-factor.

The second scenario will extend the reach of the Mobile Autonomous 5G Edge, validating its interconnection and interoperability with remote cloud. By putting stringent requirements on orchestration and user-plane traffic, the platform must be able to opportunistically handle connections and disconnections of intermittent backhaul links without affecting user-perceived KPIs. This scenario also opens up for the collaboration of PPDR agencies with third parties or with each other in coalition scenarios.

Finally, the third scenario will validate the simultaneous coexistence of multiple public and non-public telecom services enabling to access multiple slices, each one with different requirements. This scenario unlocks the capability for a deployed team member to use the same device to access different network types (e.g., NPN or public) with the assurance that the expected requirements, including security and privacy levels, are in line with the type of traffic exchanged (best-effort or mission critical).

3.8. Risk Assessment

Table 10: PPDR use case risk assessment.

Risk	Description	Likelihood (L / M / H)	Impact (L / M / H)	Mitigation
1	PTT not standardized as part of 5G	H	M	The partners will explore alternative options (e.g., applicative only with out of band signalling) for providing PTT-like features
2	Unavailability of 5G frequencies	L	H	Frequencies have already been secured (n78 band) and are employed both at the RAN and end devices
3	Under-dimensioning of the compute platform (Autonomous edge)	M	M	Collection of computing requirements has started, the low footprint of the selected edge makes it possible to extend the platform on the van

4	Missing interfaces for integrating partners' contributions	M	M/H	Common interface points and APIs are defined in WP2 and will be developed in WP3
5	Footprint of the orchestrator too high	M	M	Related to risk #3. In case of too large footprint, the capabilities of the orchestrator will be streamlined in order to comply with available processing power.
6	Impossibility to connect to multiple slices provided via different PLMN ids	M	L/M	In principle, multiple options allow this: Dual SIM devices, eSIM approaches are the most promising.

4. UC3 Blueprint – 5G Virtual Office

A 5G Virtual Office provides secure access to a specific set of corporate services. This means that a 5G device can communicate with any other device member of the 5G Virtual Office, if there is any type of 5G coverage, including both indoors and outdoors. In an assumed hospital environment, a group of heterogeneous individuals, from different teams and with distinct responsibilities (doctors, nurses, paramedics), share a set of office resources and have the need to communicate both with each other, and with the hospital physical resources in a reliable way.

For the specific context of a hospital as considered in this use case, the main application is that hospital staff is not bound by location to access medical devices, electronic health records, or any office equipment, allowing the flexibility to work remotely (e.g., paramedics accessing patient health on the go, video conferencing diagnosis, remote operation of medical equipment), including from a patient premise or another off-site location.

In the next sections, the blueprint for this use case is described. This includes the motivation behind it, detailed scenarios, deployment topology, technologies and innovations, as well as the target achievements and how they will be assessed.

4.1. Motivation

This section will proceed with the description of the use case, introducing the motivation behind the use case and its scenarios, the rationale for Non-Public Networks (NPNs) in those scenarios as well as key pain points for its implementation.

The COVID-19 pandemic brought a new set of challenges to the healthcare infrastructure. To keep up with the demand for beds, a lot of hospitals opened additional wards to improve their capacity and to provide isolation, but human resources did not expand at the same rate. 5G can play a fundamental role in this scenario by providing transparent remote access to medical devices (e.g., ventilators, infusion pumps), office equipment, electronic health records and patient-attached bio sensors, thus allowing the flexibility to work remotely. With these capabilities, remote consultation, monitoring and evaluation will be possible, enabling the optimization of human resources by decreasing time loss on movements across different sites and by providing additional isolation between patient and doctor, reducing health risks and the need for protective equipment. This virtual office concept can also be extended to ambulances or other medical vehicles working remotely. With additional network capabilities (edge integration, CN slices, guaranteed QoS), 5G allows medical crews to remotely start the patient's evaluation, as soon as paramedics encounter the patient.

4.1.1. Use of Non-Public Networks

In this use case both SNPNs and PNI-NPNs are relevant. The PNI-NPNs are used by ambulances and paramedics and remotely deployed staff to have a continuous connection to the hospital's network, enabling access to the same devices and information as if present

at hospital premises. The standalone NPNs are more relevant at the hospital campus to provide non-public coverage. Here, the goal is to provide seamless connectivity, resilience, dedicated performance and QoS settings, as well as isolation, thus ensuring that only authorized individuals have access to the network and that both access to confidential electronic health records and remote monitoring personal data is secure, reliable and real-time.

4.1.2. Key Pain Points

The implementation of this use case faces a number of challenges that are mostly due to the limitations of current technologies. We expect to overcome these with FUDGE-5G innovations. These key pain points are detailed below:

- Time-sensitive alerts (very low SpO2 level or blood pressure drop) requires reliable and deterministic latencies. State-of-the-art networks are not able to offer low enough latency to assure that alerts get to the destination fast enough and that decisions (via video/audio) on a patient can be performed in a safe way.
- Non-public networks need to be accessed transparently and securely, even when supported on public networks. This requires isolation from the rest of the network and the capability to execute NF instances within the provider premises securely.
- Nowadays there are few instances of remote patient monitoring due to privacy concerns, so hospitals avoid having sensitive information moving across untrusted public networks. This removes the possibility of remote medical exam. The SNPN closed system, internally controlled and completely separated from the public infrastructure mitigates these privacy concerns on the hospital premises.
- It is not always possible to have a health professional in front of a health monitoring computer terminal or next to the patient, so most times diagnosis and treatment are delayed until that can happen. A SNPN 5G network that removes the location factor could help to mitigate this issue, while satisfying privacy concerns due to its internal management and isolation.
- The information exchanged between the hospital NPN and the emergency response vehicle is personal information. The privacy and security of that information needs to be enforced during communication and storage.

4.2. Scenario Description

The 5G Virtual Office use case has a complex scenario, depicted in Figure 12. This scenario can be split into three sub-scenarios that make it easier to comprehend: Ward Remote Monitoring, Intra-Hospital Patient Transport Monitoring and Ambulance Emergency Response. In this sub-section, a detailed description of each of these is provided to create an overall view of the use case.

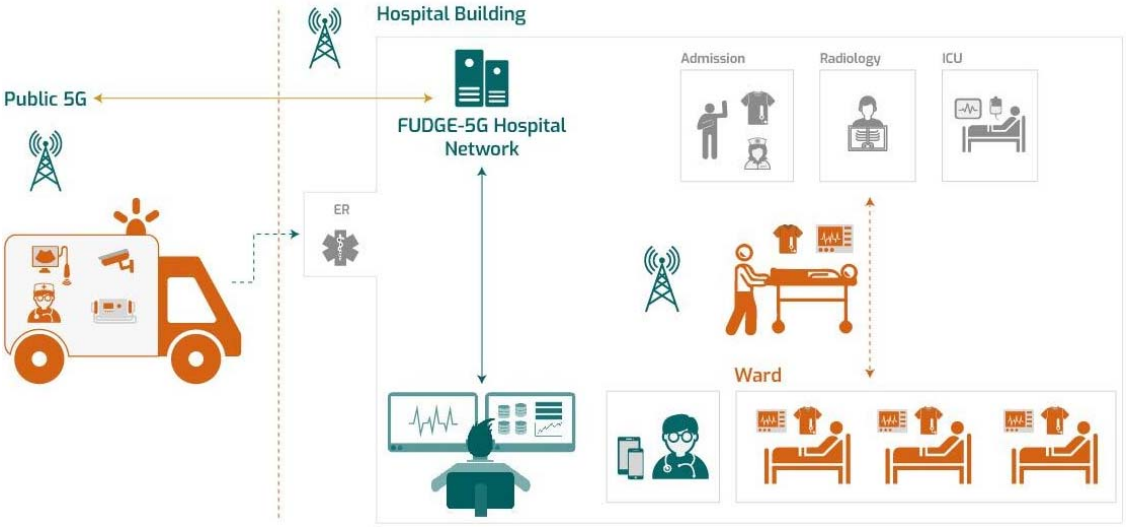


Figure 12: 5G Virtual Office Scenario.

Ward Remote Monitoring

Unlike Intensive Care Units (ICUs) where monitoring of patients is continuous and hospitals tend to have better equipment and more qualified staff, hospital wards have the capacity to accommodate big quantities of patients, and the amount of time that the medical staff has to monitor each of the patients individually is very short. Another important aspect is that wards have sparser monitoring resources. This leads to additional delays in the detection of symptoms, some of them life threatening, which increase the overall mortality rate. Thus, if more sophisticated monitoring can be expanded to wards and if it can be done with less human interaction/less need for qualified staff, the overall quality of healthcare can improve and mortality can decrease.

In the 5G Virtual Office use case, every time a patient enters the ward (either from admission or from ICU), it receives a smart shirt to monitor cardiac and respiratory functions. All the data collected by sensors is centralized in the hospital network and sent over the 5G non-public network. This collection and the fact that it is done in real-time over 5G has multiple benefits: first, it has no wires and does not depend on sketchy Wi-Fi coverage, meaning the patient can be easily moved to another location without monitoring disruptions (see the next sub-scenario); second, it enables centralized data fusion and processing with machine learning algorithms that detect abnormal readings and dispatch alarms to the relevant staff. The latter benefit is extremely important towards an effective monitoring, and it further reduces the need for qualified staff to be constantly monitoring each patient. In fact, human intervention is reduced and only exists either when an abnormal reading is automatically detected or when a consultation is given to the specific patient.

While the patients are undergoing medical care at the ward, qualified staff can also remotely access all information and interact with patients in real time, even performing diagnostic tests and complex procedures (for example, ventilator configuration). This means that qualified staff and specialists do not need to move within the hospital at all

times, reducing wait times, increasing efficiency and also reducing the probability of spreading contagious conditions.

Intra-Hospital Patient Transport Monitoring

A large percentage of patients need to be moved across the hospital building to perform exams, sometimes covering distances close to one kilometre. These patients are heavily monitored by multiple equipment types with wires, thus moving them around is complex.

This becomes a challenge when patients need to be monitored at all times, in particular ICU patients due to their underlying conditions and invasibe monitoring equipment. Additionally, some of the sensors (including ECG, blood pressure, SpO2, respiration rate) may require very high sampling rates (> 100Hz) and will generate huge quantities of data that needs to be transmitted in real time.

With the 5G non-public coverage across the entire hospital, moving patients around when necessary becomes easier as coverage is highly dependable. Moreover, as it lacks wires and supports high bandwidths/low latencies, it is also a great alternative to existing wired solutions. As in the ward, such patients can have greater quality of monitoring delivered by the network solution, but also a better care overall because even if a qualified person is not monitoring vital signs at all times, an automated system is always performing a real time analysis to detect abnormal patterns and will send alerts as soon as that happens.

Ambulance Emergency Response

An ambulance is dispatched to an emergency call and uses an NPN on top of public 5G networks to remain connected, thus obtaining seamless connectivity with the required security and performance.

When an ambulance is called on site, paramedics provide assistance to the patient, where they usually receive only a brief report from the emergency call centre, identifying the patient with information obtained from the emergency contact. The paramedics can now check the patient’s medical history and information regarding underlying conditions (for example, medication being taken by the patient, allergies, recent hospital visits, chronic illnesses, etc.) from the emergency response vehicle. The information is readily available during the journey to the patient's location. Based on this patient information, paramedics apply the appropriate procedure to stabilize the patient and start moving towards the hospital. Along this path, the patient is monitored with cameras, microphones and biosensors. This information is uploaded, stored and viewed at the hospital to prepare for the patient's arrival. Still, additional diagnostic tests can now be performed to save time. If necessary, the doctor can instruct paramedics to apply specific procedures or medications.

This is particularly relevant as, typically, an ambulance has a crew of two paramedics, one being the driver, the other staying with the patient. The problem arises, when there are some tasks (bureaucracy, monitoring, reporting to the hospital), for which both are necessary. When having a doctor intervene remotely with the ambulance, as described above, the driver will be responsible only for making the journey to the hospital. The remote

support of the doctor allows the driver to focus on a specific task, enabling the redistribution of qualified paramedics to new ambulances to use resources more efficiently.

Upon arrival at the emergency room, everything is ready for the patient and the connectivity of any remaining monitoring equipment is assured by the hospital's non-public 5G network.

4.3. Key Components and High-Level Topology

In this section we give a description of the key technological components and how they interact to provide the required platform for this use case.

4.3.1. Key Components

5G Core

- Open5G Core with enhanced Service Based Architecture (eSBA) implementation.

Cloud Applications

- **5G Virtual Office Vertical Application** - consisting of a situational awareness application platform for monitoring, accessing and processing data from different types of devices, including:
  - Patient's bio-sensors (e.g. ECG, SpO2, respiration rate).
  - Internal communication system.
  - Medical records databases (*will be simulated*).
  - Office equipment (e.g. printers, computers, scanners).
  - Shared services (e.g. private websites or shared folders).
  - Vehicles (e.g. ambulances).
  - Deployed medical staff (e.g. on the patient premises).

Network and Service Orchestration

- **End-to-end secure slice orchestration** - for the purpose of providing isolation for biosensors from external devices.
- **Vertical Applications Orchestrator (VAO)** - to ensure high availability of the Virtual Office application, irrespective of where it is being accessed.
- **Service Function Virtualisation Orchestrator (SFVO)** – an integral part of the FUDGE-5G platform offering location-aware cloud-native orchestration for 5G services, e.g. 5GC and VAO, based on SLAs.

5G NR

Implements 5G E2E with the ability to validate 5G KPIs, supporting the execution of vertical use case tests, demonstrating the value of 5G solutions and ultimately fostering the widespread adoption of 5G technologies.

- **Radio components** (3.5 GHz and 26 GHz), reaching a TRL (Technology Readiness Level) of 7 or higher.
- **Quectel RM500Q-GL –** 5G Sub-6GHz Module optimized to IoT and eMBB applications and with an integrated GNSS receiver that provides an accurate and dependable positioning capability.
- **5G End User Equipment.**

4.3.2. High Level Topology

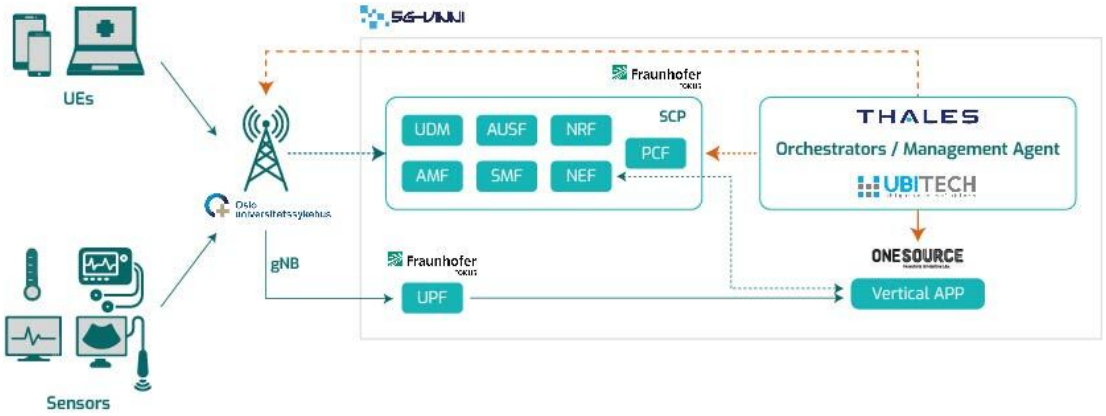


Figure 13: 5GVirtual Office High Level Topology.

The high-level topology of the 5G Virtual Office use case is depicted above in Figure 13. End user equipment, regular UEs, sensors or any other type of devices connect to the gNB and use the provided 5GC. Although some functionalities are directly provided by the 5GC and its NFs, both orchestration and vertical applications are external to the 5GC and must interact with it. The orchestrators follow the path of SCP, while the vertical application of the use case interacts with NEF to perform the required operations (e.g., policy control requests to PCF).

4.4. Requirements

This section includes the functional requirements of the use case and the key performance indicators targets to be met.

Table below shows the functional requirements of the use case. It represents the target functionalities of the use case that are needed for successful use case realization. It represents what the system is expected to deliver and its behaviour.

Table 11: Functional requirements for 5G Virtual Office.

FR	Title	Description	Type (I-Implement, O-Operate)

FR1	Produce real-time video and audio (important for vertical use cases for patients, e.g., in vital healthcare)	Real time video and audio from the patient room or ambulance transmitted to the hospital monitoring room and, when required, to a specific UE.	O
FR2	Mission and team management	APP to manage the different operations teams, allowing mission distribution, vital health control, for greater security in operations	O
FR3	5G Communication	• 5G modems allowing the connection of the devices used in critical operations to the RAN deployed on the Hospital testbed. • Provide user friendly zero-touch orchestration, operation and management systems. • End-to-end (E2E) facility (performance validation through advanced vertical sector service testing)	O
FR4	Mobile device management	Devices distributed by operations with different functionalities, according to needs	I
FR5	Finding devices involved in operations (hospital and Ambulance scenarios)	The mobile devices for the operations have GPS locators that are viewed in the APP. Indoor positioning is also an alternative (with Bluetooth & Wi-Fi)	O
FR6	Securely Exchange data	THA will provide its secure slicing orchestrator to provide isolation for critical biosensors from external devices	I
FR7	High Availability	UBI will deploy its VAO in order to guarantee high availability and continuous accessibility of the Virtual Office application.	
FR8	Infrastructure	Compute infrastructure in the autonomous edge capable of running RAN, core VNFs, and edge applications	I
FR9	Equipment	Devices and antennas capable of using the same frequency	O
FR10	Connectivity (PNI-NPN)	To have a continuous connection to the hospital network	I
FR11	Communication	The internal network must be unaffected by power failures	I

4.5. Ecosystem

In the Figure 14, the ecosystem of the use case is described. Special highlight is given to the components and the providing partners, Table 12 summarizes it:

Table 12: Ecosystem of 5G Virtual Office use case.

5G User Equipment	Devices and Equipment	5G Radio Infrastructure & Spectrum	Infrastructure Provider	Core Network Provider	Platform Provider	Application Provider
ONE	ONE	TNOR (5G-VINNI)	Microsoft Intel RedHat	FHG	IDE THA UBI	ONE

- **5G User Equipment.** It includes all the hardware equipment to access the 5G network. ONE will provide modems from Quectel, which were already tested and validated in a 5G SA network. ONE will provide commercial smartphones.
- **End User Device.** The gateway device to deliver 5G connectivity to bio-sensors, smart shirts and other patient monitoring devices that, due to size, power and similar concerns cannot connect to the 5G network by themselves. It acts like a bridge between 5G and other communication technologies, and it has edge computing capabilities to handle some local data processing.
- **5G Radio infrastructure.** All the infrastructure, including radio equipment and backhaul transport network, to deliver 5G communications. In a first stage, it will include the deployed 5G infrastructure of 5G-VINNI, including 5G sites and gNBs provided by TNOR.
- **Infrastructure Provider.** Computational resources, virtualization technologies and software tools that enable resources management. At the operating system level, RedHat will provide solutions for containerization of the FUDGE-5G platform components. At the infrastructure level, TNOR datacentre runs Microsoft datacentre software on top of Intel hardware. The infrastructure encompasses a main datacentre and an edge datacentre.
- **Core Network Provider.** The set of core network functions needed to provide the E2E 5G communication. FHG will provide a deployment of Open5GCore, their 5G Core solution, on-boarded in the FUDGE-5G platform and integrated with the 5G Radio infrastructure.
- **Platform Provider.** The platform that will host all network functions and deliver service routing, orchestration and lifecycle management. FHG will provide their platform integrated with the Secure slice orchestrator from THA and the vertical applications orchestrator from UBI.
- **Vertical Application Provider**. The application that processes all data from patient monitoring equipment and biosensors. ONE will provide the vertical application for the 5G Virtual Office use case, which will ultimately be deployed in the stakeholder premises.

Once the use case is commercialized, new partners will come into play enabling a faster spread of the 5G Virtual Office across different business and entities. The new partners belong to the following categories:

- 5G user equipment providers (e.g., Samsung, Apple).
- 5G radio infrastructure providers and operators (e.g., Ericsson, Nokia).
- Infrastructure providers (e.g., HP, IBM, AWS, VMWare).
- Vertical application providers.

The entities' employees will benefit from the 5G seamless integration with fixed networks provided by the NPN and from the PNI-NPNs enabled continuous connectivity to the entity's internal network. Virtually any entity, public or private, regardless of its size or geographical distribution will benefit from the capabilities and innovations showcased by this UC.

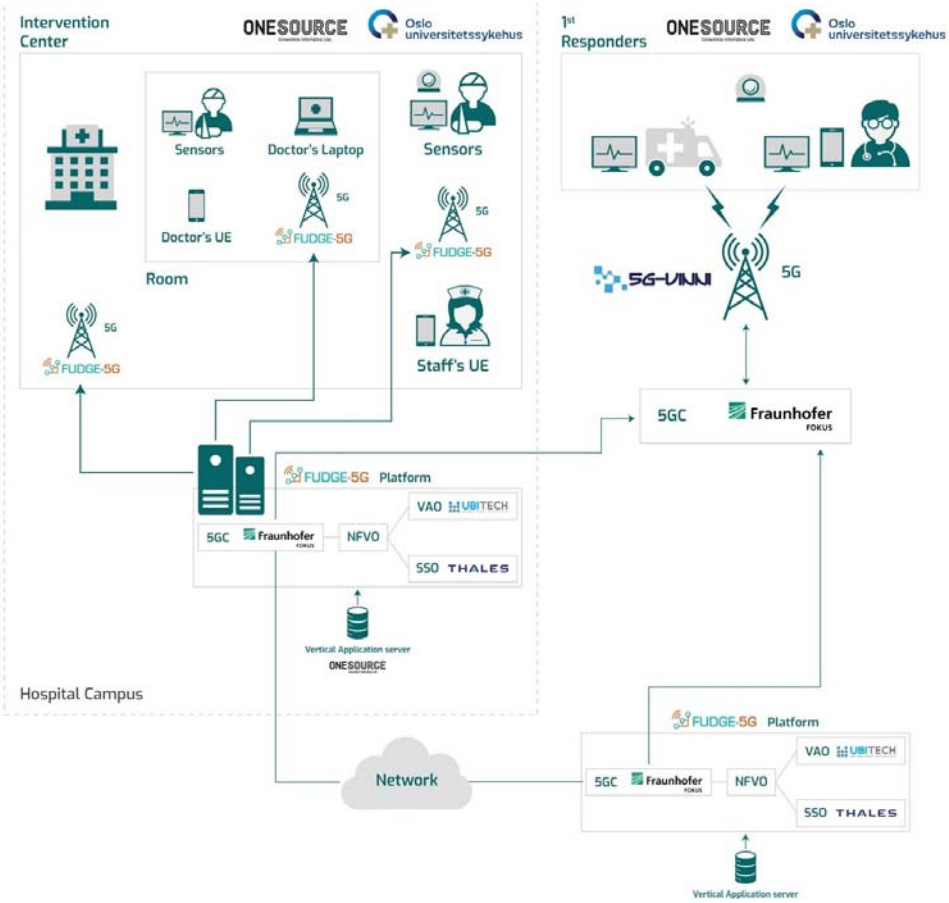


Figure 14: 5G Virtual Office ecosystem components providers.

4.6. Test Cases

Three test cases, one for each sub-scenario of the 5G Virtual Office use case, have been defined: Ward Remote Monitoring, Intra-Hospital Patient Transport Monitoring and Ambulance Emergency Response. They are described in detail in Chapter 7.

4.7. Expected Outcome

The process of office digitalization is expected to generate operational efficiencies and productivity improvements without disregarding security and privacy. In this use case, innovations will allow hospital staff to be able to work in a more effective way and for medical knowledge and expertise to cover a much wider area. This is achieved by remote procedures and remote diagnosis with the latest technologies and innovations in terms of network connectivity and IT security, thus ensuring that patients are not at a risk and that accuracy of diagnosis and treatment is not compromised.

Moreover, with additional advances in office digitalization, it will be possible to have a greener hospital with reduced use of office consumables (printed X-rays, blood tests, patient history, etc.).

Here we list the expected key outcomes of the use case:

- Allow communications between different hospital teams (NPN over the public network).
- Enable the integration of LAN into the 5G network (5GLAN) to allow connectivity to the 5G hospital network regardless of the connection point. It provides local addressing to the user terminal and the capability to access to a set of isolated services (e.g., simulated patient databases) when authorized.
- Deploy the required infrastructure to create a network on the hospital campus even when there is an energy failure or failure on the internet connectivity to the hospital.

4.8. Risk Assessment

The risk assessment for this use case can be found in the table below, including likelihood, impacts and possible mitigation measures.

Table 13: Risk assessment for 5G Virtual Office use case.

Risk	Description	Likelihood (L / M / H)	Impact (L / M / H)	Mitigation
1	No access to Healthcare Information System Interface (HIS).	H	M	Deploy temporary sensors
2	No real-life patients	H	L	Simulate patients
3	Ungranted access to the Electronic health records	H	L	Electronic health records with mock patient information
4	Not enough microcells (two) to test the handover during intra-hospital patient transportation	L	M	Perform the test only on the coverage area of the deployed microcell.

5	No Ambulance available	M	L	Use a private vehicle and remote access to the network
6	Legal issues	L	H	Plan and take care of the legal documents and permits before the tests

5. UC4 Blueprint – Industry 4.0

5.1. Motivation

Nowadays, industrial communications are mostly based on wired industrial Local Area Networks (LAN), a configuration that is inflexible and complex. In the FUDGE-5G vision, components, and machines on the industry floor such as controllers, robots, or automated guided vehicles (AGVs) will be wirelessly connected, replacing some of the wired state-of-the-art alternatives. Currently, a range of wireless technology options are available for the Industry 4.0 [20]. From all these alternatives, 5G is emerging as a key connectivity solution, as many of its features are tailor-made for Industry 4.0 applications. 5G offers some key capabilities that other standards lack partially or completely. 5G allows for ultra-reliable and low-latency connectivity, as well as ultra-high bandwidth, among others. Industry manufacturers will therefore have the opportunity to use wireless critical communications, operating reliably and securely with 5G [21].

This use case aims at demonstrating the applicability of 5G NPNs and their integration with 5GLAN and TSN [22] , replacing fixed and wired alternatives for industrial communications with 5G. An NPN based factory floor will allow engineers to design and manage wireless resources in the plant without external interference.

5GLAN is envisioned as a key technology to be used in this use case. The integration of 5G with the fixed Ethernet network into the same network will certainly bring benefits to the industry. Network administrators in the industry are used to manage enterprise networks and 5GLAN allows them to administrate 5G networks by following the same procedures and with all the benefits from the industry. The integration of 5GLAN in industrial networks means that three important features from enterprise communications will be incorporated, i.e., easy management, interoperability, and reliability [23]. As an example, wireless devices can be seamlessly integrated in the enterprise networks thanks to the establishment of end-to-end tunnels from them to the cloud network.

On other hand, extending TSN networks towards mobile infrastructure requires a set of fundamental enablers to match the features in fixed networks. The primary challenge consists in delivering time synchronization to the industrial mobile devices. This requires either enhancements to the wireless modem to access specific radio signals or radio links with ultra-low delay and high reliability to exchange Precision Time Protocol (PTP) messages. Other challenges are the need of low latency to enable equipment control over wireless connectivity and high bandwidth to enable the use of AR/VR devices for remote control. This will in turn increase site efficiency, lower training cost, and improve Health, Safety and Environment (HSE) aspects.

In addition to latency and reliability, security is one of the most stringent requirements in industrial networks. Most of the industrial infrastructures consist of a large complex system with multiple areas, each of which requires different levels of security. In an industrial network some areas must guarantee restricted access, which is implemented by applying a concept of security zones. Industrial networks follow ISA/IEC 62443 specifications, where

security zones are defined. According to those specifications each security zone consists of a logical grouping of physical, information or application assets sharing a common security requirement. The 5G architecture options should ensure support of security zones when integrated with existing industrial network architecture and network slicing.

5.1.1. Use of Non-Public Networks

5G NPNs provides the following benefits to the Industry 4.0:

- **High security:** Data can be exchanged inside the network without involving the intervention of external networks, meeting the strong security policies of industrial environments, where, for example, access to internal data from the outside world is not allowed, and the management of the network elements is only allowed to authorized personnel.
- **Low latency:** NPNs enable the use of edge computing on premises, which will naturally minimise the latency [24]. This is the case for direct communications between end devices, but also for communications between an end device and storage and computing resources in case they are provided on premises following an edge computing approach.
- **High efficiency and QoS:** Network owners have total control over the network deployment and configuration providing the highest level of efficiency and quality possible.
- **Better coverage:** Indoor coverage by public macro networks is very challenging, as we move higher in frequencies for 5G NR. Local installations can be a game changer. Unlike PLMNs, when using NPNs the industry stakeholder can decide where to place the access points, reaching the required coverage. This is similar to Wi-Fi deployments, but without any interference.
- **High adaptability and scalability:** The network owner can decide the configuration of the NPN, which results in a highly flexible and scalable industry floor. Once this NPN is set, it is possible to adapt the network to get more devices connected and more services running easily given the total control of the owner over the network [25].
- **High reliability:** Industrial networks require a robust infrastructure for critical communication tasks involving the control of end devices remotely. This robustness in NPNs is ensured by integrating time synchronization, having better coverage, and using a dedicated spectrum as required.
- **Non-switching networking:** In large areas, other technologies such as Wi-Fi would trigger the use of several cells to cover a large area. NPNs allow to use the same network, without the need of handovers.

5.1.2. Key Pain Points

The development, integration and demonstration of the Industry 4.0 use case entails a number of issues. The key pain points and their possible solutions are [26] [27]:

- **Information shortage**: In industrial applications, workers may get unprocessed or inaccurate information. Therefore, real time correction will be integrated to ensure that workers have validated data at each moment.
- **Safety hazards**: In industrial environments it is very important to ensure workload safety, which may be hazardous. The proposed use case will enhance safety due to the use of wireless communications provided by 5G.
- **Strict requirements**: Industry 4.0 applications have stringent requirements in terms of security, reliability, or latency that must be fulfilled. This will be ensured by using 5G NR, together with network slicing and edge capabilities, among other alternatives.
- **Seamless integration and compatibility**: One of the obstacles that 5G faces to be deployed in factories is the fact that there are legacy equipment, installations, and devices. Thus, the addition of a new technology is not an easy task to achieve. 5G networks will be adapted so devices that use industrial standards are also connected.
- **Usability**: 5G networks have been designed for consumer traffic with large deployments and complex management systems. Instead, the management of industry 4.0 infrastructures is based on generic tools for managing fixed Ethernet/IP networks. 5G deployments should be planned by considering this aspect.

5.2. Scenario Description

To demonstrate the great advantages of 5G NPNs in industrial environments, FUDGE-5G will implement and validate a use case in which a controller interacts with sensors and actuator devices, located within a small area in a factory environment. Wired connections will be partially replaced by 5G wireless links to provide flexibility for remote reconfiguration (for instance, avoiding the use of cables in places such as hazardous areas or a rotating part in a machine that needs connectivity). Note that the intention is not to replace the whole infrastructure but to integrate 5G with the existent wired infrastructure and use wireless links when needed. The Industry 4.0 use case scenario is shown in Figure 15.

Figure 15: Industry 4.0 use case configuration for the test cases.

The 5G NPN is formed by three main components, i.e., the 5GC from Cumucore, the 5G RAN from 5G-VINNI, provided by Telenor, and the 5G Modem from Fivecomm. In this scenario, end user devices will be connected through the 5G NPN to the end station. 5G TSN will be

implemented in both 5GC and modem sides by using TSN translators and controllers. The specific components and the high-level topology are explained in detail in Section 5.3.

The development, integration and demonstration of this scenario will be divided in **two main phases**, as initially planned in the project proposal. The main difference between phase-1 and phase-2 is the enhancements related to the use of the 5G core (control plane) in the cloud.

- **Phase-1:** The first stage of trials will consist of standalone NPN within a controlled environment. FUDGE-5G partners will integrate their solutions and validate them in ABB's facility located in Oslo, see Figure 16.
- **Phase-2:** Partners will demonstrate in a second stage the FUDGE-5G solution in a cloud-hosted 5GC. The location will be also the ABB premises.

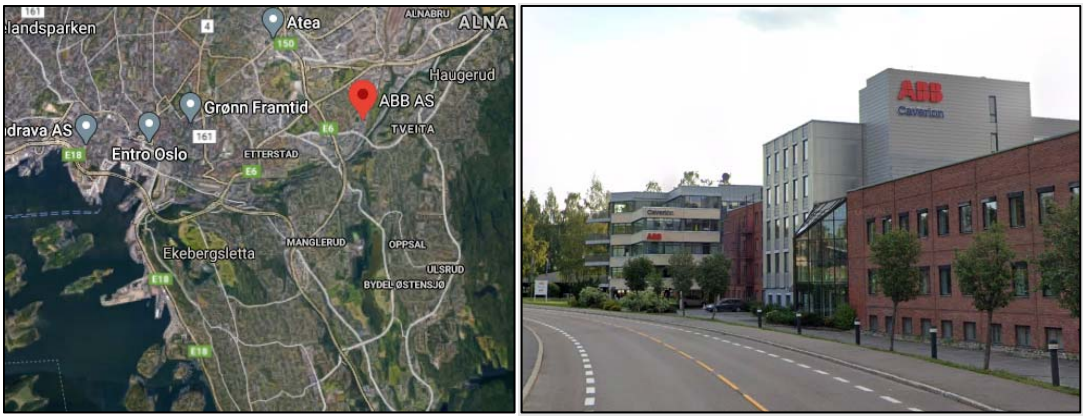


Figure 16: Location for the industry 4.0 use case: ABB facility in Oslo.

Note 1: the second phase of this use case is still under discussion and open to changes.

Note 2: as a potential alternative or third phase, partners will demonstrate the FUDGE-5G solution in an additional/pilot site, to be decided later.

5.3. Key Components and High-Level Topology

5.3.1. Key Components

The following components will be integrated within the use case:

- **Devices and controlling station:** the vertical stakeholder of this use case will bring to the consortium end-user devices and their respective controlling stations to be used in the considered applications.
- **5G Modems:** End-user devices will be connected to the 5G network through a 5G modem. It is a hardware-based product with the necessary electronic components and I/O ports to support the considered applications.
- **5G RAN**: FUDGE-5G will make use of the 5G RAN of 5G-VINNI to support this use case. This RAN component will allow access from 5G devices to the network and the

application itself controlled by the stakeholder. The RAN should support network slicing to provide different performance based on traffic requirements.

- **5G Core Network:** virtualized 5GC based on SBA architecture with support for TSN and time synchronization.
- **5G Core Management**: A management console will be integrated for managing the mapping between network slices assigned to different devices and the IEC 62443 security zones defined in fixed industrial network.
- **TSN-AF**: Application Function required for seamless integration of the 5GS with wired industrial devices such as TSN controllers.
- **TSN Controller**: Such component is developed to ensure high-precision timing synchronization, in addition to flexibility in traffic scheduling with the purpose to reduce latency, hence allowing execution of time-aware application [28].
- **Service Communication Proxy (SCP)**: With a unified FUDGE-5G platform architecture across all use cases, all SBI-enabled 5GC NFs will be communicating via an SCP with each other, which enables transparent service routing for HTTP-based services.
- **Service Function Virtualisation Orchestrator (SFVO)**: The location-aware cloud-native orchestration framework as part of the FUDGE-5G platform is being used to orchestrate all 5GC NFs (SBI enabled or not) driven by unified cross layer analytics for lifecycle management purposes for 5GC NFs.

5.3.2. High Level Topology

Figure 17 shows the high-level topology of the Industry 4.0 use case.

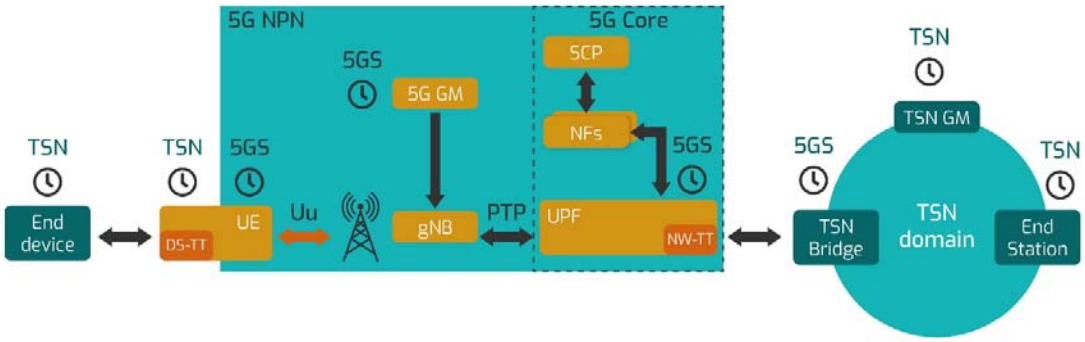


Figure 17: Industry 4.0 use case high-level topology.

The end-user device, e.g., a sensor, actuator, or any type of device that collects industrial information to be sent through the 5G network, is connected to the User Equipment (5G modem) to provide connectivity and time synchronization with its Device-Side Translator (DS-TT) using an owned TSN clock. From this point, the 5G NPN transports any message between the UE and the TSN bridge with a far more precise master clock (5GS), which allows the TSN clock synchronization.

The signals coming from this master clock are received by the 5G RAN, which sends the information through the UPF of the 5GC. The 5GC also offers SCP orchestration and is TSN

compatible by implementing a Network-Side Translator (NW-TT). Note that, for the sake of simplicity, only the most important network functions have been shown in the figure. It is also worth mentioning that all clocks are synchronized using (g)PTP v2 messages handling, in addition to the 5GS clock.

5.4. Requirements

5.4.1. Functional Requirements

Functional requirements in the Industry 4.0 are usually related to security and safety aspects, authentication, or identity management [29]. Time synchronization and positioning are also key aspect to consider. Wireless connectivity must include deterministic communications, ensuring that all the packets being transmitted can arrive to their end-devices and preserve the order. TSN networks will incorporate new 5G wireless devices that require synchronization. Additionally, data transmission might be non-IP, as industrial devices need to exchange IEEE 802.1 addresses, discover mechanisms and broadcast messages over L2 communications. Hence, time synchronization must be applied regardless of the (IP/non-IP) type of message.

The following functional requirements have been identified for this use case:

- **Synchronization**: Time accuracy is a critical aspect for TSN. If there are different TSN controllers or 5G TSN systems, it is necessary to keep time synchronization among all of them. End-devices need to be always synchronized to avoid any type of accident. According to [30], these devices are required to have a synchronicity time from 10 µs to 50 ms.
- **Frequency ranges**: Due to local regulations, there may be some issues related to the frequency band to be used and the coverage covered. Selected frequencies must be agreed prior to the implementation of the radio access. Partners will identify alternatives for radio access in this scenario.
- **Positioning**: Mobile devices must provide information about their location. 5G positioning information coming from such devices will be used.
- **Safety**: Safety measures are a key aspect to consider in industrial environments to reduce risks, since accidents can not only harm people, but also the environment [29]. 5G systems applied to the considered use cases need to implement such functional safety measures.
- **Security**: Wired infrastructures are not usually exposed to local and external attacks since they are not connected to the Internet. The 5G network deployed in industrial environment must be protected against them, being authentication of the key measures in this regard.
- **Flexibility**: Flexibility is key to enable new business models and support the envisioned applications in the Industry 4.0. This could be achieved by using edge capabilities and software-based solutions such as network virtualization or cloudification [29].

5.4.2. Performance Requirements

In the factory, a controller will interact with many sensor and actuator devices located within a small area (up to 100 m^2). These applications have high performance requirements such as low latency, high reliability, and deterministic delivery of messages. The following KPIs and performance requirements are expected:

- **End-to-end UL/DL latency**: Latency is measured as the time delay from message generated at source until its arrival at the end node. The 5G NPN delay is considered as part of the E2E latency, with values within 1-2 ms range.
- **Throughput**: In typical 5G consumer use cases, DL throughput is of utmost importance. However, in industrial use cases UL throughput is also important. Control related traffic does not require high throughput in both directions, but condition monitoring, optimization, VR, AR, and CCTV applications require significantly higher throughputs. Expectation is a throughput up to 200 Mbps in the UL and up to 4 Gbps in the DL.
- **Power Consumption**: Controlling energy levels is key in this use case, because of the need to reduce production costs.
- **Transmission power**: Transmission power levels in the gNB must be kept to a lower value to ensure that it is safe to operate the equipment when deployed in a hazardous area in the considered frequency range. Typical Effective Isotropic Radiated Power (EIRP) values are between 2 and 10 W.
- **5G coverage**: Related to the previous KPI. gNB transmission power levels should be enough to provide coverage and support the required communication in the industrial environment. This will be supported for the considered frequencies.
- **Reliability**: Another requirement is to ensure that at least 99.9% of the transmitted packets arrive to their destiny correctly. This can be achieved by using 5G Rel-15.
- **Availability**: This value will vary depending on the outage time permitted in a year, that is, the period of time when the system is unavailable. The following table provides the specific values associated to this downtime.

Table 14: Availability values for the Industry 4.0 use case.

Availability (%)	Outage time in a year
99.8	17h 31m 53s
99.9	8h 45m 56s
99.999	5m 15s
99.999999	0.3 s

5.5. Ecosystem

The table below shows the ecosystem envisaged for the use case, the partners involved, and their components. ABB will offer its premises and end-user solutions to be integrated in the use case. Cumucore will contribute with a TSN controller, TNS-AF and its 5G core network to establish a 5G LAN among devices. InterDigital will support this use case with

their SCP and service function virtualisation. The radio access will be brought by Telenor through 5G-VINNI. Finally, Fivecomm will bring its 5G modem to perform a bridge between the 5G NPN and the industrial end-devices from ABB.

Table 15: Industry 4.0 use case ecosystem.

End devices / stations	5G modem	5G RAN	5GC	TSN-AF
ABB	Fivecomm	Telenor	Cumucore, InterDigital	Cumucore

5.6. Test Cases

The Industry 4.0 scenario has been divided into **five test applications**:

- **Remote monitoring as a service**: Video signals are streamed using network orchestration and traffic handling with priority levels.
- **Remote control as a service with real-time feedback:** Video signals are streamed and processed using control hardware, working in parallel over the same network. TSN and localization services over 5G are applied.
- **5G integration and adaptability in industrial environments**: Continuous monitoring and support of 5G devices and other components for industrial environments.
- **Process control over 5G**: Large amounts of simulated data are used as an input to the 5G network for process control and management.
- **VR/AR control over 5G (optional):** Several IoT devices such as sensors and actuators, as well as VR/AR devices (smart glasses, holographic displays) will be integrated and controlled in a 5G NPN.

Such applications share the same infrastructure and scenario, but they will be demonstrated under unique conditions and with different end user devices. Each of these five test applications will be divided in turn into several test cases, whose description and related requirements are provided in Section 7.8.1.

5.7. Expected outcome

The industry digitalization is expected to generate strong productivity improvements and operational efficiencies within logistics, supply, and manufacturing segments. For example, this use case will enable industrial staff to work smarter, to increase productivity levels per headcount, to accelerate innovation and design cycles, and to improve supply chain relationships. All in all, this use case pretends to transform the way we do business and manufacture goods.

Moreover, integrating wireless communications may be beneficial in terms of eco-sustainability due to the lesser quantity of materials that are required, compared to wired solutions. This naturally will depend on some factors such as the factory stretch, number of connected devices, or data rate expectations, among others.

Another point of view that mixes eco-sustainability and cost saving is power consumption. It has been claimed that with 5G communication the power consumption per bit could be 90% lesser than in 4G [31]. This is an outstanding number, but the density of base stations, antennas, cloud infrastructure and user devices may have an impact. It could be possible that a 5G network uses over 140% more power than a similar 4G network if the components are not properly optimized [32].This point, far enough to be innocuous, may be a key point to reduce production costs and to improve the sustainability of the industry environment.

It is also expected that 5G wireless communications will offer greater flexibility within the factory premises. Nowadays, many manufacturers achieve some of these benefits by connecting to the public 4G network or local on-premises Wi-Fi networks. However, an exclusive and dedicated 5G NPN will bring the performance to a whole new level due to the integration of technologies that permit ultra-reliable and low latency communication, in addition to ensuring the security.

In this context, the following outcomes from individual partners are expected:

- **ABB** will get an NPN in one of its factories with time critical and 5G connectivity features in addition to localization service.
- **Fivecomm** will improve its portfolio, increasing the number of products and services related to the Industry 4.0 that could be applied in future scenarios. Thanks to this use case, the 5G modem will implement TSN, including a DS-TT, which is key for this vertical.
- **Telenor** will be able to meet the performance targets of industry verticals by optimizing the 5G dimensioning.
- **Cumucore** will increment the current portfolio adding new network functions related to 5G-TSN like DS-TT or NW-TT, to get competitive advantage to deliver end to end system required by industry 4.0 customers.
- **InterDigital** will be able to use their SCP in an industry environment, increasing the use cases where they have performed a 5G service-based architecture. Additionally, InterDigital's orchestration technology, Service Function Virtualisation, will be used in this trial to orchestrate the 5G core and demonstrate industry 4.0-related lifecycle management actions of the 5GC NFs that have been decomposed into cloud-native network functions.

5.8. Risk Assessment

Table 16: Risk assessment for Industry 4.0 use case.

Risk	Description	Likelihood	Impact	Mitigation
1	Frequency unavailability for an NPN in Norway	L	H	Partners will ensure that the use case is adapted to the frequency bands available in Norway (for instance, 2.4 GHz). Both the modem and the RAN will

				be compatible with the selected frequency bands.
2	E2E latency not low enough	M	M	Identification of monitoring points and measurement of latency values per component. This will permit to identify the problem and solve it when needed.
3	Coverage issues in the factory	L	M	A proper coverage planning, including visits to the factory, will be done before deploying the RAN.
4	Issues in timing synchronization	M	M	The integration of PTPv2 both in the 5Gmodem and in the 5GC will ensure time synchronization in this use case.
5	Lack of interaction among partners for integration	L	H	The use case champion will coordinate this integration and set up periodic calls to make sure that the progress is correct.
6	Timing in 3GPP standardization	L	M	Most of industry-related services have been considered in Rel-16, including TSN. Special focus was put on URLLC. Partners will implement Rel-16 during the project.

6. UC5 Blueprint – Interconnected NPNs

6.1. Motivation

With the large deployment of smaller size Non-Public-Networks (NPNs), the network ecosystem is changing from large scale networks covering large areas towards a multitude of networks with smaller coverage. To be able to use such an ecosystem in a coherent manner, there is a very large need to interconnect different NPNs. This can be, for example, to interconnect multiple factory floors, multiple event venues, logistics centres, portable 5G units or to connect different educational institutes, like in the case of the well-known WiFi Eduroam coalition.

As mostly it is expected that the communication of the NPNs would be strongly localized with all the devices staying within the coverage area of the network. This would be the case for example of factory robots which will not change the location. However, already there is a very large mobility within these networks. For example, for the logistics and the quality maintenance within factory environments, a very large number of devices are associated and physically connected to product parts or not completed yet elements, packaging, etc. Similarly, for the multimedia content acquisition, multiple families of devices are included from venue logistics, multimedia capturing (e.g. TV stations) and the performing artists' devices coming together only for specific events.

However, the typical roaming mechanisms, currently available, are suitable only for the interconnection between public networks or public network integrated NPN, as they mostly rely on controlled large-scale connections. To interconnect a large number of independently administrated NPNs, there is a need to create different trust and reliability models for both control and data exchanges, especially when related to authentication and authorization control. Furthermore, this multitude of networks is connected across transparent backhauls pertaining to third parties. To be able to make such a use case work, a proper management of the data exchanges, as much as possible, over these third party, independently managed backhauls is needed, including the characterization of the backhaul and the adaptation of the communication to the momentary available resources and to the service requirements.

Also, to be able to reach the expected level of success, the proposed mechanism should function with any two networks and easily scale towards a global conglomerate network composed of a very high number of interconnected NPNs. This could be achieved only by assuring a high administrative independence of each of the networks as well as a set of semi-automatic mechanisms for an NPN to easily join the global conglomerate. Specifically, to be able to participate in the inter-NPN roaming, the administrators of NPNs would have to accept a set of common principles and technology mechanisms which would reduce their independent administration. For this to happen, the mechanisms proposed should be minimally invasive as otherwise the local administrators will not accept such extensions. Even so, the acceptance of the visiting subscribers (this being the main administrative hurdle) is highly dependent on the advantages obtained by the home network users either as reciprocity or by the direct interaction with the visiting devices.

Eduroam (www.Eduroam.org) is a good example of an initial solution for Interconnected NPNs use case with specific WiFi authentication and local data traffic. It is a major part of research and education, as students and researchers can benefit from secure and reliable WiFi access both at their home campus, and when they are travelling to other campuses members of the Eduroam network. It is a roaming service designed for users from a superior educational organization (universities, engineering schools, etc.). Users are authenticated using their own university credentials, whether they are in their local network or in a visiting network, while not requiring a priori relationship between the home authentication functions and the visited network. Still, albeit no relationship is considered, there is still the need to have some peering functionality which includes the support for the authentication procedures (EAP methods) and the RADIUS proxying.

The main motivation of this use case is to further develop the interconnection of separately administrated NPNs, so as to be able to provide a coherent, secure and reliable communication environment across the global conglomerate of NPNs. The goal of this use case is to replicate the success of WiFi Eduroam for interconnecting 3GPP 5G NPNs and to further advance it with the specific mutual authentication, data path privacy of 5G networks as well as with a general managed data exchange across an unreliable backhaul. Specifically, it will concentrate on the authentication and authorization of the subscribers across multiple domains, the access control in visited domains, the establishment of proper control and data plane as well as on the management of the connectivity across the best-effort backhauls.

6.1.1. Use of Non-Public Networks

In this use case, we will be deploying three standalone NPNs in three different locations. This is similar to the current development of NPNs where different verticals and institutions consider the deployment of 5G networks of smaller or larger size to cover the specific area of the use cases.

Also, this represents a simpler use case where the NPNs are separately administered. Each of the networks has its own authentication, authorization and access control policies for the local users and potentially for visited users. A more sophisticated use case would be the one where the NPN is a dedicated termination of a large operator network. In this situation the administration policies of the NPN are shared between the local administrator and the operator. For example, the operator would define how the radio network would be accessed, as being part of the operator spectrum planning while the local administrator may define the access rights. Albeit not implemented within the use case, the feasibility of this version will be also assessed.

In each of the FUDGE NPNs a comprehensive 5G network environment will be deployed based on the 3GPP 5GLAN concept. As of today, these networks are offering services to a set of subscribers, from here on named home subscribers, according to their subscription profiles stored in the local repository. In addition to these subscribers, the use case will concentrate on the provision of service support for subscribers of other networks, from here on named “visiting subscribers”.

It is expected that the visited subscribers will pertain to different networks. They are expected to roam into one network, occasionally. The local network will provide to them some local services (according to the local policies) as well as the possibility to have home services (according to the local and the home policies). For accessing these services, the authentication and authorization mechanisms of 5G will be adapted not to require a pre-knowledge of the existence of the home network. Furthermore, a set of new policies will be defined to protect the local subscriber data traffic and the local services from the visited subscribers, providing an extended privacy to the local services. Additionally, a backhaul support functionality will be added to be able to exchange control and data plane messages in a coherent manner across backhauls pertaining to third parties.

6.1.2. Key Pain Points

The Interconnected NPNs use case has the following challenges:

- Access network discovery and selection – transmitting indications to the UEs, on which NPNs may be available at the location part of the NPN conglomerate where the expected security level of the communication can be achieved.
- Discovery of home NPNs – NPNs will be discovered only when a subscriber from the specific network will join as visited subscriber a local network. This way, there is no binding needed between NPNs prior to having a visited subscriber.
- Federated authentication and authorization – a mechanism to authenticate and authorize visiting subscribers for usage of local services, local data traffic offloading and home services.
- Ensuring secure inter-domain connectivity between the networks deployed in different locations.
- Dynamic establishment of a reliable and secure end-to-end control plane between local and home NPNs.
- Providing dynamic control of the communication across unreliable backhauls.
- Providing data path selection for local services, local data path traffic offloading and home services.

6.2. Scenario Description

This use case proposes a coherent communication support across a conglomerate of independently administered 5GLAN networks based on and extending the concept of the WiFi Eduroam i.e. roaming between a massive number of local networks with no inter-network service continuity and unreliable backhauls. The Interconnected NPNs use case will validate seamless connectivity, security and home users and service isolation across three different NPNs' sites.

The users of the 3NPNs will get access to the network some local services, home services and local offload regardless of their location be it in the home network or within one of the visited networks. In both cases of users either in the home institutions and users as visitors,

the requests should get authorized and access to the resources of the home institution should be provided. For users in their home network and for users in the visiting network, the authorization process will be different and access to the resources may also vary depending on their locations.

Home Subscribers will connect to the local RAN and the authentication request will be sent from the RAN to the 5GC. The Access and Mobility Management Function (AMF), which takes care of the connection and mobility management tasks for the UEs connecting to the 5GC, will receive the request from the RAN. AMF will check for the PLMN of the user identity and, if it matches the home PLMN, will forward the request to the Authentication Server Function (AUSF). In case of home subscribers, the PLMN will be same, so AUSF will receive the request and will query the Unified Data Management (UDM) for subscription information. The UDM will provide the subscriber profile information and chose a 5G authentication procedure to generate an authentication vector, which will be forwarded to AUSF. Based on the 5G Authentication procedures (either 5G-AKA or EAP-AKA), the user will get authenticated. Once authenticated, the home subscriber will have access to the services of the home network.

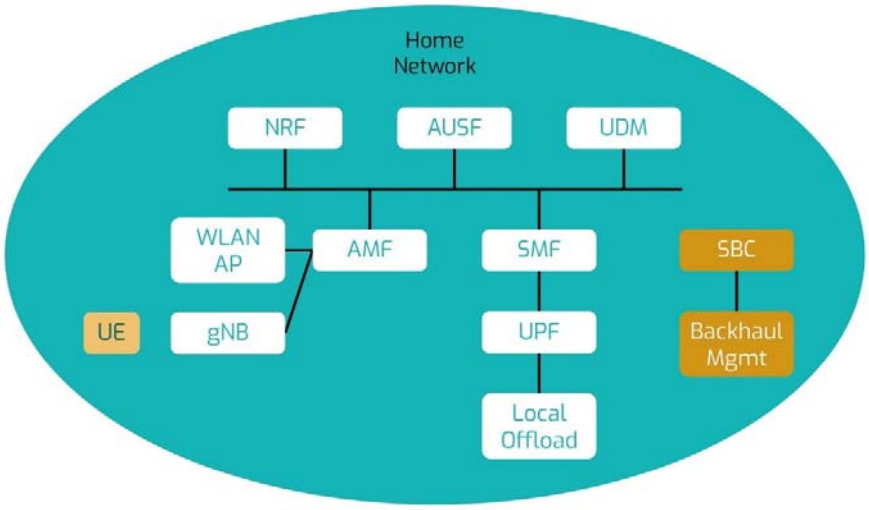


Figure 18: Interconnected NPN home subscriber scenario.

Visiting Subscribers will be using SIM-based steering to connect to the network. Devices will choose PLMN from the EPLMN list provided in the USIM to connect to the network and will try to connect to the Cells with good signals, if rejected by the network will choose another PLMN from the EPLMN list and the procedure continues until the network accepts the connection request. Once the visited subscriber is connected to the RAN, an authentication request will be sent from RAN to 5GC in the visited network. AMF will check the PLMN of the subscriber, in this case, this will not be matching with the PLMN of the home network. So, AMF will forward the request to the Session Border Controller (SBC) (which also serves the functionalities of SCP as control plane proxying) to find out the subscriber details from the other domains. SBC will check from the Network Repository Function (NRF) to find out, which SBC it should connect for the particular PLMN. As the NRF

may not have this information available, a hierarchical discovery process will be performed as in the case of the WiFi Eduroam. Through this process a home network SBC will be discovered. A secure connection between the visited network SBC and the home network SBC will be performed. Through this connection the authentication messages will be transmitted. After reaching the home domain, the home SBC will ask the local NRF for the address of the AUSF. Once it has the address of the AUSF, SBC will forward the authentication request to the AUSF. The AUSF will ask the UDM for the subscriber details. If the subscriber is found, the UDM will generate the authentication vector and forward it to the AUSF. The response from the home network will be sent through the home network SBC back to the visited network SBC. AMF in the visited network will receive the response from the SBC and will continue the 5G authorization procedure. Visited subscribers may have access to the local offload or they may connect to other devices in the same network. Visited subscribers can also be home routed, but that scenario will be covered in the later phases.

In case the subscriber information is not found, or the subscriber should not be allowed to connect to the domain or the authentication cannot be performed, the home network SBC will terminate the connection to the visited SBC as this may be a potential security breach. Same in the case the UE disconnects from the visited network.

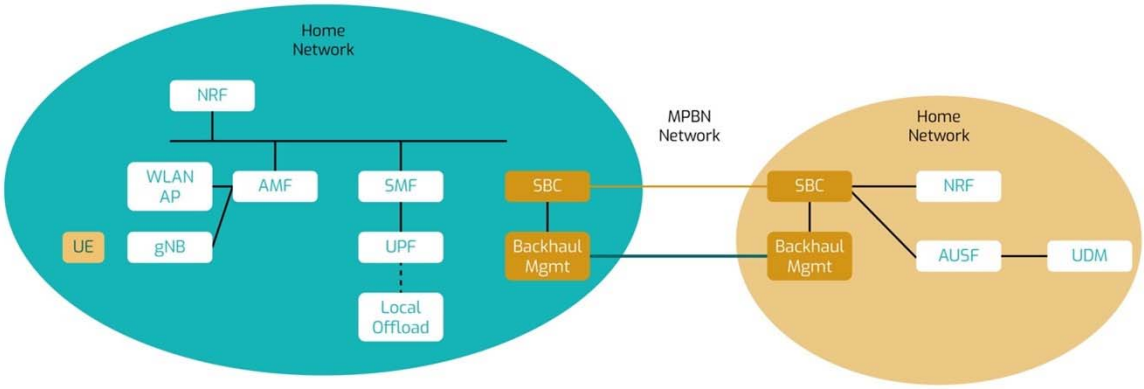
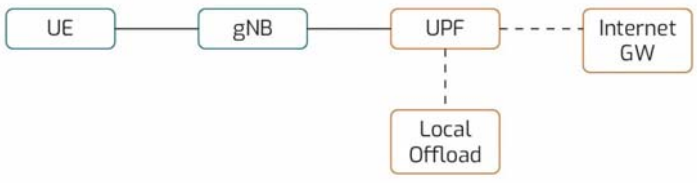


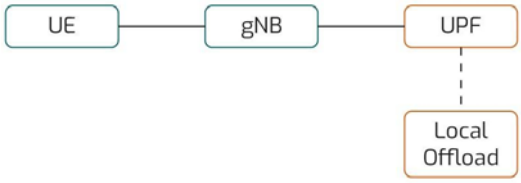
Figure 19: Interconnected NPN home subscriber scenario.

Data Path Handling:

- Home subscribers will be re-directed to a UPF serving the home network.



- Visiting subscribers might be allowed to use local breakout.



- Visiting subscribers can use local N19.

- In the later phase of the project, we may support home routed roaming for the visiting subscriber.

6.3. Key Components and High-Level Topology

6.3.1. Key Components

The key components of this use case to be integrated are as follows:

- **Devices:** Telenor will arrange the devices with SIM cards having different PLMNs.
- **RAN:** FOKUS will be using micro cell in their campus while UPV and Telenor will be using small cell at their locations.
- **5G Core Network:** Fraunhofer FOKUS Open5GCore will be used in this use case. The key 5G Core Components for this use case are AMF, AUSF, UDM, NRF, SMF and UPF.
- **SBC (Session Border Controller) components:** SCP, SEPP and backhaul API will be developed and delivered by FOKUS as part of this use case.
- Use of RADIUS for authentication.

6.3.2. High Level Topology

In this use case, Open5GCore will be deployed as 5GLANs in different locations of the campuses. The 5GC will be connected to the local RAN, which can be a small cell or microcell. Users at their home network will be able to connect to the core network through the cell. For users in the visited network, SBC will forward the request of the users to their home network and also will take care of the secured connection between the two networks.

- Open5GCore with local RAN and UE

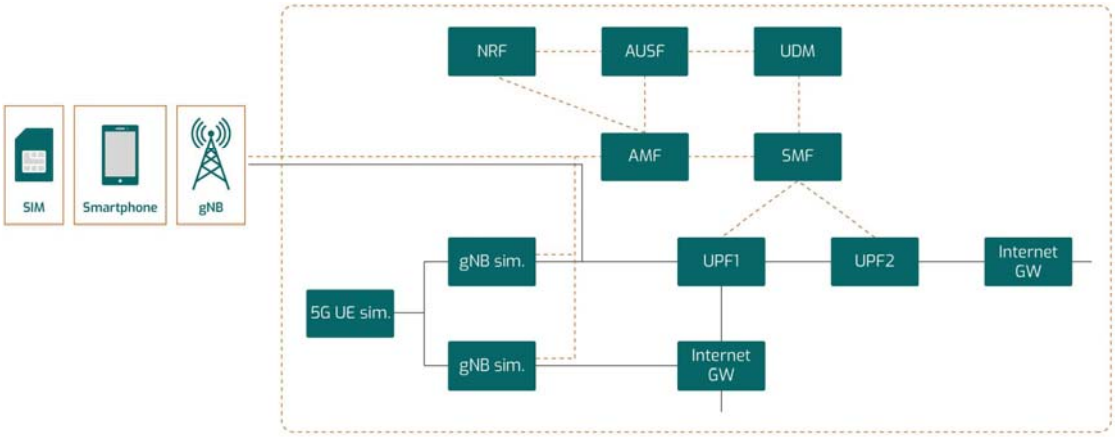


Figure 20: UC5 Open5GCore with RAN and UE.

- Integration with roaming interfaces like a Session Border Controller (SBC) which has functionalities of Service Communication Proxy (SCP) and Security Edge Protection Proxy (SEPP).

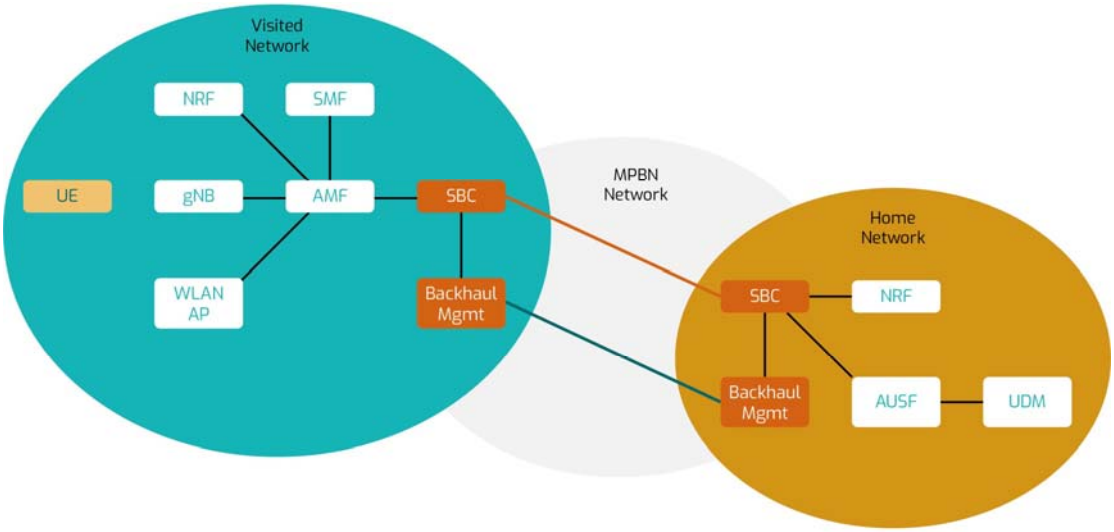


Figure 21: Interconnected NPN Session Border Controller (SBC).

6.4. Requirements

The Interconnected NPNs use case should meet the following functional and non-functional requirements.

6.4.1. Functional Requirements

The functional requirement shows the main features of the use case.

- **Discovery and selection -** The UEs should be able to receive indications on which NPNs are available close to their location and potentially provide the roaming service at the expected security and reliability levels.

- **Authentication and Authorization of subscribers:** The framework designed in the use case should be able to authenticate and authorize subscribers in home as well as in visited Eduroam networks.
- **Connectivity between NPN:** The Interconnected NPNs use case should be able to showcase the scenario of seamless connectivity among standalone Non-Public Networks.
- **Security:** The Interconnected NPNs use case should be able to demonstrate a secure network for the Eduroam subscribers. The standalone NPN networks deployed in different locations should also be connected through secure channels and the message exchange between the domains should also adhere to security.

2.1.1. Non-functional Requirements

The non-functional requirement describes the operational behaviour of the network.

- **Availability:** Availability of a network is depicted by the amount of uptime in a network system over a specific time interval. This can be measured by the percentage of uptime from the overall time of operations incurring in the network.
- **Reliability:** reliability in networks is defined as the ability to proceed with the operations within the system. If one node fails in the network other nodes in the network should keep on working.
- **Visited Network Privacy:** ensuring security of the visited network from unauthorized accesses. Users' privacy when getting authorized and secured authentication in visited network and isolating traffic from the rest of the network.
- **Accounting Information:** Visited subscribers should have the access to applications only permitted in the visited network.
- **Security of the visited network:** protection of the local services from potential attacks from the visiting subscribers through data traffic isolation.
- **Security and privacy of the inter-domain exchange:** establishment of a secure end-to-end interconnection.
- **Bi-directional secure authentication of the visited and home network:** establishment of a discovery and selection of the home domain and of a bi-directional authentication and authorization through a trust authority.
- **Accounting and lawful interception in the both visited and home domain:** a mechanism to assure the understanding and backtracking of subscriber data traffic.

6.4.2. Performance Requirements

Performance of the network can be measured by the throughput and delay of the network events.

- **End to end delay:** The latency and the delay for the end-to-end procedures triggering in the network can be used to measure end to end delay.

- **Correlation of dimensioning with the available edge node resources:** Use of networking and compute by the home network and visited network subscribers.
- **Autonomy of each NPN:** The ability for self-provisioning of resources and self-diagnosing of failure risks within the deployed networks.
- **Easy Deployment:** The deployment of a new Eduroam network should be easy including the software deployment on top of the available infrastructure, integration with base stations, configuration of devices and automatic establishment of roaming.

6.5. Ecosystem

The partners involved in the use case are:

- Fraunhofer FOKUS Berlin
- UPV Valencia. Valencia NPN node also hosts a prototype of the 5G Multicast enabled Open5GCore that will be tested during the Interconnected NPNs trials.
- Telenor Research Norway
- OneSource

For Interconnected NPNs, the infrastructure will be deployed in three different locations Telenor Research Norway, UPV Valencia and Fraunhofer FOKUS Berlin.

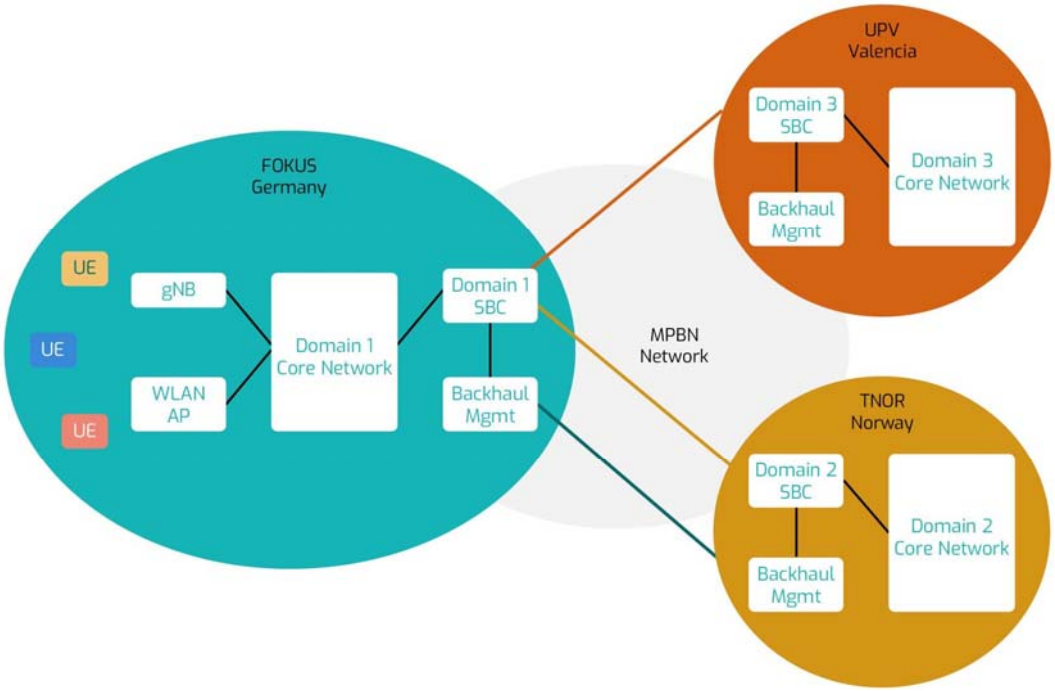


Figure 22: Interconnected NPN use case deployment locations.

In this use case, the partners mentioned above will be responsible for the following components to attain the requirements of the use case.

- **User Equipment (UE):** In this use case to target the functional requirements UEs having USIM with different PLMNs will be required. Telenor research will be responsible for arranging the corresponding devices.
- **5G Radio Infrastructure:** The radio infrastructure that will be needed for the devices to connect to 5G core network will be covered by the deploying partner. In Telenor Research, 5G VINNI RAN will be used for the communication. At FOKUS premises, microcell will be used. Small cells will be used in UPV as the Radio Access Network (RAN).
- **5G Core:** In this use case 5G Core from Fraunhofer FOKUS will be deployed in all the locations. Open5GCore acts as the 5G testbed and is the implementation of 5G core network.
- **Network discovery and selection:** as part of the core network, additional functionality for network discovery and selection should be added in order to indicate to the devices on the potential NPNs that could be discovered.
- **Authentication Server:** Both home and roaming subscribers will be authenticated and authorized by the respective local network. The connectivity between the distributed authentication servers will be handled by OneSource.

Once the prototype of the use case is ready, it will be validated by the chosen stakeholder, Oslo University. This use case can have huge impact, if it can be commercialized targeting to interconnect 5G NPNs. It will be very useful in campus networks as well as for small scale industries to provide secured private networks within organizations and providing connectivity between them.

6.6. Test Cases

The test cases for the interconnected NPN use case are as follows:

- Sanity check test: Devices in Home Network should get authenticated and authorized.
- Visited networks should be discovered and UEs should connect as visited subscribers to the RAN.
- Visited networks should discover dynamically home networks.
- Visited and home networks should bi-directionally authenticate and authorize each other.
- UEs in Roaming/Visited Network should be authenticated and authorized for visitor use.
- During roaming, the 5GCore should forward requests through SBCs (one SBC for each domain) with the target PLMN and target Network Function name.
- Service Communication Proxy (SCP) within the SBC should support control plane proxying.
- Security Edge Protection Proxy (SEPP) within the SBC should take care of the authorization of the components across domains.

- Users should have access to the network services, when they are in home network and also in visited networks.
- The visited and the home network should terminate their interconnection in case there is no visited subscriber connected.

To test the scenarios for Interconnected NPNs use case, we will be taking the steps below:

- In the first step we will be testing with the emulated UE and gNodeBs to validate the authorization framework.
- In the next step we will use Benchmarking Tool to validate the capacity of the proposal.
- In the last step, using SIMs of different PLMNs Authentication and Authorization will be tested in both the home network and visited network with access to the data network.

6.7. Expected outcome

This use case will assess the integration of the existing Wi-Fi Eduroam system with a private 5G mobile network and will extend the features of 5G Core by adding key aspects of a truly distributed network with autonomous functionality nodes. This includes the network discovery and selection mechanism as well as the authentication and authorization for roaming within private networks, which enables the deployment of private 5G LANs across multiple administrative domains and the secure inter-domain connectivity. The use case will target to assess the remote transparent usage of campus services focusing on scenarios, where a fixed network is not available. These features are designed to innovate the private network paradigm from a single network centric model to a disintegrated one, assuring that the new networks are easy to deploy and to interoperate.

6.8. Risk Assessment

Table 17: Interconnected NPN use case risk assessment.

Risk	Description	Likelihood (L/M/H)	Impact (L/M/H)	Mitigation
1	Failure to create secure connectivity between three domains	M	H	Partners will have to create the setup for three domains with different PLMN locally
2	Connection failure to the remote networks	M	H	Need to take backup of the subscriber details in a central server
3	Interoperability issue with the RAN and the 5G Core	M	M	Use of emulated gNB from the Open5GCore platform
4	Lack of Devices having SIM with different PLMNs	H	L	Use emulated UE from the Open5GCore platform

7. Validation Framework

7.1. Methodology

The validation framework to support the work of FUDGE-5G is focused on getting validation of functional and non-functional requirements of each use case, which by itself provides the means for WP4 (Vertical Trials Technology Validation) to perform gap analysis, get stakeholder satisfaction feedback and assess overall success of the project's objectives.

The methodology behind the framework is split into four inclusive components: 1) its overall description for concise definition of the architecture; 2) requirement specification and validation; 3) KPI definition, measurement, and validation tools; 4) the definition of mechanisms for stakeholder feedback, which includes questionnaires and focus groups.

Concerning the component of questionnaires and focus groups, the approach is common to all use cases. We will administer evaluation questionnaires to the participant to trials to extract meaningful responses. In general, a psychometric scale composed of a set of questions answered through a Likert scale will be used to assess each identified metric. The complete set of questions addressing all metrics will be contained in a questionnaire provided to participants, adhering to the common, unified measurement methodology presented in here. Questionnaires will be typically answered before and after the trial execution. When possible, objectively measured KPIs will serve as a complement to the questionnaire results.

The respondent will answer to each questions/statement through a 5-point Likert Scale ("Strongly Disagree -> Strongly Agree"). The use of multiple questions per construct allows for a stronger internal validity and reliability of the scale.

Exemplary questions:

- I think that I would like to use the system frequently
- I found the system unnecessary complex to use
- I thought the system was easy to use
- I think I would need the support of a technical person to be able to use the system
- I found the various functions in the system to be well integrated
- I thought there was too much inconsistency in the system
- I think many users will learn to use the system quickly
- I found the system very cumbersome to use
- I felt very confident using the system
- I needed to learn a lot of things before being able to use the system

The validation framework of FUDGE-5G also establishes a generic architecture that is followed by all use cases but leaves to each use case the specification of a more concrete and well-defined architecture that better fits their needs. In the sub-section below, the generic architecture for the framework is highlighted with greater detail.

7.2. Framework Architecture

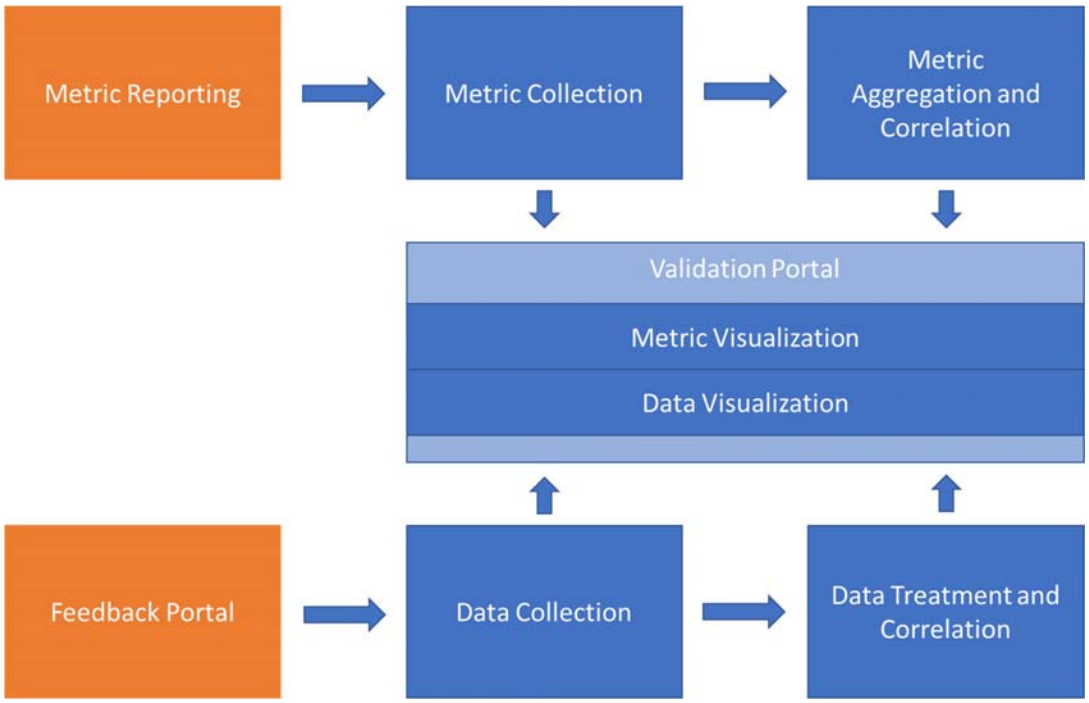


Figure 23: FUDGE-5G Validation Framework Architecture

The FUDGE-5G validation framework architecture, depicted in Figure 23, is purposely generic for flexibility of the FUDGE-5G use cases. In fact, due to the specifics of each use case, each use case defines their own validation framework with the generic architecture as a template. Despite the flexibility, a set of requirements is defined:

- It must include reporting, collection, aggregation, correlation, and visualization of all the technical and functional metrics.
- It must include reporting, collection, treatment, correlation, and visualization of all the non-technical and non-functional metrics.
- All data sources should follow a standardized interface.
- Ideally, visualization tools should be common to all use cases.

7.3. Routing

The service routing component of the FUDGE-5G platform implements Deployment Option 3 of the Service Communication Proxy of a 5G system and comes with a range of unique capabilities such as:

- **Shortest Path Routing:** Based on the network topology, the available SCP route HTTP requests to the nearest instance that serves the FQDN indicated in the HTTP request as the value in the HTTP header field “Host”. The distance is calculated based on the number of hops reported by the SDN-enabled switching fabric. Once the number of

service endpoints changes, any new HTTP request issued by any endpoint fill be treated based on the new network topology.

- **Flow and Error Control:** As the available SCP acts as a TCP proxy and implements a non-IP-based routing, the SCP comes with its own Lightweight Transport Protocol (LTP) that implements flow and error control without impacting the service routing capabilities.
- **Load Balancing:** The SCP follows a round robin approach when distributing HTTP requests to service endpoints within the same location.
- **Transparent In-Session switching of HTTP transactions:** Once a nearer service endpoint is available or a currently used service endpoint is removed by the orchestration layer, the SCP can transparently move any existing HTTP transaction (request-response) to the next suitable service endpoint, assuming at least one service endpoint still exists after a change. This feature acts entirely transparent to the endpoint which has issued the HTTP request. The same applies to the service endpoint which handles the request and provides the response.
- **TLS1.3 Support:** The SCP enables all the features listed above even when HTTPS is in use. In order to enable that, the root TLS certificate must be shared with the SCP so that the SPs are the ingress points of the SCP can act not only as a TCP proxy, but also as a TLS proxy. If certificates are not shared, the SCP still offers all features except the transparent in-session one.
- **HTTP/1.1 and HTTP/2 Support:** The SCP offers all its features for HTTP Version 1.1 and HTTP 2 assuming both endpoints implement the same HTTP version. Fallback solutions defined in IETF for HTTP/2 endpoints requesting resources from HTTP/1.1 are also supported by the SCP.

Figure 24 illustrates the network topology used to validate all features listed above. While not all trials have a multi-tier or at least multi-location deployment, some validations will be performed in the London integration testbed for Task 2.5. In the figure below, three Service Proxies (SPs) are illustrated that form the ingress and egress points of the SCP. Each SP serves a single location in the network. A single Open vSwitch (OVS) instance is illustrated that interconnects SP_1 and SP_2. SP_1 and SP_3 are connected via a single link. Furthermore, two Network Functions (NFs) are illustrated, NF_A and NF_B, which are distributed as individual instances across various locations as follows: $NF_{A,1}$ is in Location 1, $NF_{B,1}$ and $NF_{B,2}$ in Location 2, and $NF_{B,3}$ in Location 3.

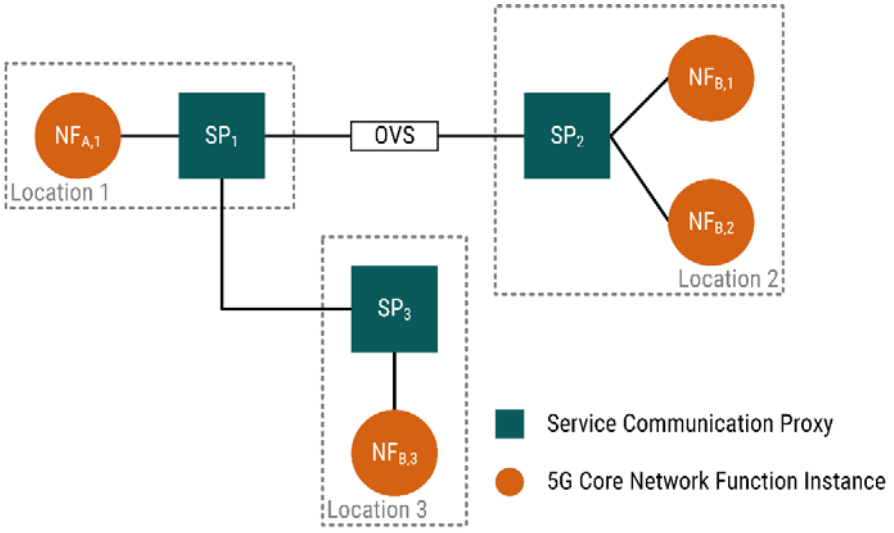


Figure 24: Network Topology for Validating Routing Capabilities of the Service Communication Proxy.

The table below provides the test cases' names, their validation methodology and quantitative measurable KPIs to indicate whether a test case has been passed.

Table 18: Test Cases, Methodologies and KPIs to Validate the Routing Capabilities of the SCP.

Test Case	Methodology	KPI
Shortest Path Routing	NF_B has been provisioned under the FQDN *foo.com* and operates a web servers capable of responding to HTTP requests for the resource *bar* of size 1MB. NF_B is provisioned as illustrated in Figure 24 with all its instances $NF_{B,1}$, $NF_{B,2}$ and $NF_{B,3}$ set to the lifecycle state CONNECTED. $NF_{A,1}$ uses the command line tools curl, wget or httpie to issue seven HTTP requests to *foo.com/bar*. To ensure independent runs of the same measurement, TCP session re-use is avoided by calling any of the three command line tools seven times from the terminal, e.g.: ~$ wget foo.com/bar	All seven HTTP requests are routed to and handled by $NF_{B,3}$. All seven bar files are stored on disk and verified to be of same length and content using a SHA2 check sum.
Flow and Error Control	NF_A has been provisioned to Location 1 under the FQDN foo.com and configured to the lifecycle state CONNECTED. All three NF_B instances have been also provisioned according to Figure 24 and configured to the lifecycle state BOOTED. NF_A is operating a web server with a file bar of size 100MB. All three NF_B instances are operating a script that utilises the command line tools wget, curl or httpie to frequently pull the resource bar from foo.com while randomly sleeping between 0 and 10 seconds between re-requesting the resource again. This procedure continues for a duration of 10min.	All HTTP requests were processed correctly without any error reported by the command line tool. All responses were stored on disk inside the NF_B instances and verified after the duration of the test against their length and content using a SHA2 check sum.

Load Balancing	$NF_{B,1}$ and $NF_{B,2}$ are provisioned in Location 2 and $NF_{A,1}$ in Location 1. NF_B is operating a web server with a resource *bar* of size 1MB and both instances are set to the lifecycle management state CONNECTED using the FQDN *foo.com*. NF_A operates a script that issues HTTP requests to foo.com/bar every 5 seconds for a duration of 30 HTTP requests.	At the end of the test, the number of HTTP requests handled by $NF_{B,1}$ and $NF_{B,2}$ is identical, i.e. 15.
Transparent In-Session Switching	NF_B implements a webserver with a resource bar if size 500MB. NF_A implements an HTTP client using a command line tool and issues a single request to foo.com/bar. NF_A and NF_B are provisioned, as illustrated in Figure 24, with $NF_{A,1}$ and $NF_{B,3}$ set to BOOTED, and $NF_{B,1}$ set to CONNECTED. In one test case, $NF_{A,1}$ issues an HTTP request and straight after $NF_{B,3}$ is set to CONNECTED. This is repeated seven times. In another test case, NF_B implements an artificial packet delay of 10s on its interface using tc resulting in any HTTP arriving at the webserver with a delay of 10s. Once the $NF_{A,1}$ instance has sent off the HTTP request to foo.com/bar, the lifecycle state of $NF_{B,3}$ is set to CONNECTED. This is repeated seven times.	In the first test case the HTTP client in $NF_{A,1}$ receives the entire resource /bar without any notice in the HTTP client. The web server of both $NF_{B,1}$ and $NF_{B,3}$ log a HTTP request to /bar with $NF_{B,3}$ seeing a request for a different content length (HTTP header field Content-Length). In the 2nd test case the HTTP client also receives the entire /bar resource which will be checked using its SHA2 check sum. Only NFB instance $NF_{B,3}$ will log the HTTP request.
HTTPS Support	The transparent in-session switching test case is repeated with the difference that the SCP has a certificate for foo.com and the communication is secured via HTTPS.	The test case outcomes are identical to the transparent in-session switching ones.

7.4. Orchestration

7.4.1. Vertical Application Orchestration

The validation procedures related with the application orchestration specifically, are structured around a number of test objectives, which reflect complete stakeholder's operational procedures (consisting of one or more application components/functionalities) or/and complete infrastructure operations, as well as user ' performance and miscellaneous requirements to be satisfied.

These test objectives are stemming from the operations that the FUDGE-5G Vertical Application Orchestrator (VAO) provides. These operations regard:

The onboarding/composition of an application related operations:

- the application/component development and wrapping,

- the various applications' service graphs' definition/creation/edition,
- the runtime policies creation/edition.

The interface to end users/verticals related operations:

- the lifecycle management of applications/application components' in the repository,
- the handling of various, different profiles/operations for different users/
- stakeholders/roles.

The vertical runtime, orchestration operations:

- real-time vertical application deployment,
- enforcement of specific execution policies over the deployed vertical application following a continuous match-resolve-act approach,
- monitoring and management of applications/application components through Monitoring,
- extraction of advanced insights and events from the analytics data of the Monitoring process, for support of re-active reconfigurations (manually or automatically) of application deployment,
- the lifecycle management of the applications (application components) deployment.

The testing associated with each test objective comprises a number of different validation phases and testing procedures spanning from component to functionality validation, and further to performance evaluation.

Table 19:Application Validation Methods and Success criteria.

Test Objective	Validation Method	Success Criteria
Onboarding/ composition of an application	Tests related to the applications' composition, in particular to: • application component development and wrapping to on-board it into the VAO, including code/wrapping verification, and assessment of the VAO Wrapping Toolkit. • creation/edition of application service graphs adhering to the VAO metamodel, include also verification and assessment of the metamodels. • creation/edition of runtime policies at application component level, through the VAO Policy Editor.	Successful migration of an on-premises developed application to a cloud native 5G-ready version by using the VAO's Application Development Toolkit.
Use case Interface	Tests to be performed are related to the lifecycle management of applications/ components through the VAO GUI, including:	Successful performance of the functionalities that have been specified to be performed through

	• verification of the interface to end-users/application owners/verticals in terms of including all necessary functionality for these stakeholders • the lifecycle management of applications/application components and their metadata in the repository, including: o Insertion, o modification/update, o selection, o deletion, o users' access rights definition/alteration • the handling of the user rights for various, different profiles for different users/roles	VAO interface on a per user/role basis. Consistency maintained between the information shown through GUIs with the actual repository information, and the specified rules on a per user/role basis
Orchestration operations	Tests to be performed are related to the real-time deployment of an application through the VAO, including: • delivery of a real-time deployment of a vertical application by taking into account: the application service graph, the relevant execution policies, the programmable resources availability, • enforcement of specific execution policies over the deployed vertical application following a continuous match-resolve-act approach, based on monitoring data and analytics • termination of application instance operation upon requests	Successful performance of the functionalities related to the real-time deployment of a vertical Application, in terms of requested resources and provisioned, taking into account the infrastructure capabilities. Successful performance of the functionalities related to the reconfiguration of a vertical application deployment. Successful performance of the functionalities related to vertical application termination.
Orchestration /Monitoring	Tests to be performed are related to the real-time and historical monitoring of an application deployment, including: • real-time monitoring of multiple applications through a set of active and passive probes, • support of real-time analytics of multiple contexts, • extraction of advanced insights and events from the monitoring process, e.g. through data mining, as well as predictive and prescriptive analytics mechanisms (i.e. regression, clustering or classification algorithms),	Successful performance of real-time monitoring of multiple applications. • Extraction of real-time analytics for all the application components; • Data fusion of data coming from all application components; • Generation of real-time Predictive Analytics for metrics coming from all application components; • Representation of all the analytics on a related Analytics Dashboard to support

	• evaluation of the extracted information in terms of validity, usefulness, versatility, effectiveness and sophisticated processing.	application and infrastructure overview and development decision making.
Other Aspects (Speed ,)	Tests include measurement and evaluation of the time required for an application component and application deployment for the various UCs', at various test infrastructures.	Speed of deployment from the initial application (application components') selection from the application repository to the completion of the application initial deployment on a selected infrastructure.

7.4.2. 5G Core Orchestration

The orchestration of the 5GC NFs is realised via the newly designed and implemented Service Function Virtualisation paradigm, as described in D1.2 [1] and D2.1 [4]. The unique feature of this NFV evolution are as follows:

- **Location-aware Provisioning:** SFV offers the ability to provision instances of NFs into specific locations (aka Service Hosts). While supporting a range of virtualisation technologies such as LXC, Docker and KVM, SFV is agnostic to the environment and would even allow Service Hosts to be native Android, Windows or Apple operating systems as long as they implement the RESTful interface and methods for Service Hosts.
- **Location-aware Lifecycle Control:** SFV offers the ability to change the lifecycle state of NF instances at specific locations (Service Hosts) from an extended set of states, i.e. NON_PLACED, PLACED, BOOTED and CONNECTED. The lifecycle state changes are triggered via a dedicated RESTful SFV interface. Trigger can be ether sent by a human, the NF itself or from a telemetry component that continuously monitors the 5GC.
- **Descriptor**-based Orchestration: The provisioning and lifecycle control is programmed via a YAML or JSON-based descriptor, as described in D2.1 [4]. The descriptor is communicated via a RESTful API to the SFVO.
- **Cloud Native Packaging:** When using a virtualisation environment, SFV provide a lightweight packaging environment for LXC and Docker which installs a monitoring agent, configures the network interface and sets up system services for configuring the monitoring agent and an SFV-specific service called "whoami".

Table 20: Test Cases, Methodologies and KPIs to Validate the SFVO.

Test Case	Methodology	KPI
Packaging of all FUDGE-5G 5GCs	Using the packaging environment provided by SFV, all 5GCs are packaged as LXC or Docker containers and can be freely provisioned and lifecycle controlled in a cloud native fashion	The packaging scripts allowed all FUDGE-5G 5GC vendors to package their NFs as desired and the provisioning and lifecycle control did

	independently from the underlying hardware or operating system.	not impact their code design or execution methodologies.
Provisioning of 5GC NFs	Using the SFV resource descriptor, the 5GC is described on which Service Host which NF should be orchestrated as individual instances.	All 5GCs were able to be orchestrated based on the definition of the resource descriptor.
Lifecycle State Control	Using the SFV trigger API, the lifecycle state of NF instances is changed by hand or through threshold-based monitoring of 5GC NF instances.	Based on the logic of the underlying service routing, any addition or removal should see a change in the average number of HTTP transactions a single NF instance has to handle.

7.5. UC1 – Concurrent Media Delivery

7.5.1. Test Cases

Remote Production

Table 21: UC1 Remote Production Test Cases

Title	Description
E2E connectivity	The professional video cameras can send their captured stream and also receive data from the media production end-point using 5G. The quality of the link is maintained and stable for every case.
E2E connectivity in Multivendor	The professional video cameras can send their captured stream into the media production end-point using 5G. The 5G network consists of Network Functions provided of several manufacturers and still offer the same features
Static IP mapping	The different devices involved in the production of the content are assigned always the same IP from the 5G network.
Detection of backhaul failure	The 5G network will automatically route the data into a redundant production chain hosted locally or in the cloud in case of failure.

Media Showroom

Table 22: UC1 Media Showroom Test Cases

Title	Description
Delivery of ultra-high-quality video	The high-quality display is able to stably reproduce live content coming from the private network.
Provision of immersive content	A tactile device (smartphone or tablet) interacts with the high-quality display.

Low RTT time	The link to the tactile features a latency low enough to the sensation of immersiveness can be experienced.
Low-latency + high bandwidth service separation	Both the delivery of ultra-high-quality video and the immersiveness are able to be served concurrently while preserving the quality for both.

Concurrent Media Delivery

Table 23: UC1 Concurrent Media Delivery Test Cases

Title	Description
E2E connectivity	The professional video cameras can send their captured stream and also receive data from the media production end-point using 5G.
Static IP mapping	The different devices involved in the production of the content are assigned always the same IP from the 5G network.
Detection of backhaul failure	The 5G network will automatically route the data into a redundant production chain hosted locally or in the cloud in case of failure.
Delivery of UHD video	The high-quality display is able to stably reproduce live content coming from the private network.
Service Separation	Both the delivery of ultra-high-quality video and the immersiveness are able to be served concurrently while preserving the quality for both.

7.5.2. Validation Tools

The validation tools used in the Media Use Case are a mix of SW and HW tools. On the one hand, the SW-based validation tools are comprised by existing open source tools, bandwidth analysis websites (e.g. Speedtest, M-lab) and proprietary provided by the equipment manufacturers. On the other hand, HW-based field spectrum analysers and drive test equipment is used to evaluate the coverage signal in outdoors environments. Subjective questionnaires are also used as a validation tool and to gather feedback from the stakeholders.

7.5.3. Validation KPIs

Application KPIs

Table 24: application KPIs for Concurrent Media Delivery use case

Sub-scenario	KPI name	Description	Objective

Remote Production	Glass-to-glass latency	The time from the moment that an event is being captured by the camera until the video stream reaches the production	**< 100 ms**
	Reliability	The number of errors at the input of the video decoder. Notwithstanding faulty equipment, the transport network is assumed to be error free and capable of delivering 100% of the radio packets to the 5GC. Target KPI for reliability is Quasi Error Free (QEF)	**1 uncorrected error event per hour**
	Throughput	The output bitrate by the production cameras that the air interface and transport network should be able to absorb, multiplied by number of equipment.	**100 Mbps 1080@50** **200 Mbps 4K@25**
	Coverage Area	Area where the coverage of the 5G connection is adequate to ensure the stability of the service.	**5000 m^2**
	Number of devices	The maximum number of production devices capturing content	**5 cameras**
Media Showroom	Throughput	The bitrate of the immersive services delivered, depending on the type of display targeted	**5 Mbps Portable TV** **8 Mbps HDTV Stationary TV** **50 Mbps VR Headsets**
	Latency	This value includes the time when the client has sent off the request for a DASH segment until the HTTP response has arrived with the DASH segment.	**< 10 s**
	Coverage area	Indoor coverage where the displays can be placed and still receive enough 5G signal to receive the service properly	**100 m^2**
	Mean Opinion Score	The subjective score of the media showroom, not only based on the image quality itself but on the responsiveness and overall immersive feeling of the system	**4 or higher**

Platform KPIs

Table 25: platform KPIs for Concurrent Media Delivery use case

KPI name	Description	Objective
Management framework footprint	The HW requirements for all the management and stakeholder applications to run properly. A high amount of storage is expected to save and handle the almost error-less production streams.	**CPUs** **GB of RAM**

		TB of storage (SSD)
Number of slices	The maximum number of slices concurrently supported by the system, in order to differentiate traffic types in the network	**> 8**
Transparent Access Network Connectivity	The Platform should be able to provide a data pipe between stakeholder applications and the devices. The stakeholder applications should not be aware that the devices are under a fiber, WiFi or New Radio access.	**2 or more access network supported**

7.6. UC2 – PPDR

7.6.1. Test Cases

There are three test cases, one for each sub-scenario of the PPDR use case. We detail in the following the different steps for each test case.

Standalone Network on Wheels

Table 26: PPDR standalone Network on Wheels test cases

Title	Description
Basic 5G connectivity available	A 5G device in the proximity of the NoW can associate with the 5G network provided by the NoW. From the device it is possible ping a local edge server deployed on the NoW, then to realize a speed test to evaluate the available bandwidth.
Push-to-talk (PTT) between a group of devices	A group of 5G devices connected to the NoW can exchange voice PTT communications over the 5G network provided by the NoW. The PTT server is deployed locally on the NoW
Group video conference between deployed forces and a C2 operator	A 5G device associated to the NoW can stream a video from the field to the other members of the group and back to an operator sitting inside the NoW via a C2 application. The C2 application is deployed locally on the NoW.
Group chat with BFT and situational awareness update	A group of 5G devices connected to the NoW can exchange textual messages and situation awareness data (photo, video, audio files and GPS positioning) in order to help reconstruct the hostile environment. The situation awareness server is deployed locally on the NoW.
Live tracking of health data	5G sensors are connected with the NoW. An operator sitting inside the NoW is able to subscribe to alerts from sensor readings and to evaluate the status of each sensor. The situation awareness server is deployed locally on the NoW.
Broadcast warning messages to all end-devices in coverage	An operator sitting inside the NoW can broadcast a warning message (textual) to all devices in the radio coverage of the NoW. The message is received also by devices not associated with the network provided by the NoW. The broadcast server is deployed locally on the NoW.

Crowd-sourced gun-detection system	5G devices serves as gunshot detection probes to discover the orientation and position of a gunshot. The devices continuously overhear and use a gunshot detection server to discover the position and the type of weapon. The gunshot detection server is deployed locally on the NoW.

Interconnectivity with remote cloud

Table 27: PPDR interconnectivity with remote cloud test cases

Title	Description
Basic 5G connectivity available	A 5G device in the proximity of the NoW can associate with the 5G network provided by the NoW. From the device, it is possible to ping both the local NoW and the remote cloud. It is possible realize a speed test to evaluate the available bandwidth with both endpoints.
Push-to-talk (PTT) between a group of devices	A group of devices connected to the NoW can exchange voice PTT communications over the 5G network provided by the NoW. The PTT server is deployed on the remote cloud.
Group video conference between deployed forces and a C2 operator	A 5G device associated to the NoW can stream a video from the field to the other members of the group and back to an operator sitting inside the NoW via a C2 application. The C2 application is deployed on the remote cloud.
Group chat with BFT and situational awareness update	A group of 5G devices connected to the NoW can exchange textual messages and situation awareness data (photo, video, audio files and GPS positioning) in order to help reconstructing the hostile environment. The situation awareness server is deployed on the remote cloud.
Live tracking of health data	5G sensors are connected with the NoW. An operator sitting inside the NoW is able to subscribe to alerts from sensor readings and to evaluate the status of each sensor. The situation awareness server is deployed on the remote cloud
Broadcast warning messages to all end-devices in coverage	An operator sitting inside the NoW can broadcast a warning message (textual) to all devices in the radio coverage of the NoW. The message is received also by devices not associated with the network provided by the NoW. The broadcast server is deployed on the remote Cloud.
Crowd-sourced gun-detection system	5G devices serves as gunshot detection probes to discover the orientation and position of a gunshot. The devices continuously overhear and use a gunshot detection server to discover the position and the type of weapon. The gunshot detection server is on the remote Cloud.
Intermittent connectivity with remote cloud	Any of the vertical applications (e.g., gunshot detection or messaging server) from the previous test cases is instantiated locally at the NoW. Once backhaul connectivity with a remote cloud is activated, an instance of the vertical application is launched on the remote cloud and application traffic is rerouted there. In case of disconnection, local traffic is brought back to the autonomous edge instance.

Coexistence of public and non-public networks

Table 28: PPDR Coexistence of public and non-public networks test cases

Title	Description
Simultaneous use of NPN and PLMN	A 5G device is capable of exchanging data with a mission-critical service provided via the NoW (e.g., MC-PTT communications), but also a non-critical service provided over a PLMN (e.g., web browsing, map application).

7.6.2. Validation Tools

The test tools will provide both quantitative and qualitative analysis regarding the execution of the use case, and how its objectives are fulfilled. In addition to the traditional network testing tools such as iPerf3, Nmap, OpenSpeedTest and CiscoTrex, this use case will leverage an IMSI catcher to test and validate the security measures put in place to avoid mobile phone traffic eavesdropping and location tracking. For multimedia streams, Mean Opinion Score (MOS) via subjective quality evaluation tests will be considered.

7.6.3. Validation KPIs

The targets listed below are the minimum required to ensure that the functionalities proposed on the use case are successfully delivered.

Application KPIs

Table 29: application KPIs for PPDR use case

Application	KPI name	Description	Objective
Voice	Mouth-to-ear latency	The time between an utterance by the transmitting user, and the playback of the utterance at the receiving user's speaker (both for PTT and group calls)	**< 350 ms**
	Late call entry time	The time to enter an ongoing group call measured from the time that a user decides to monitor such a group call, to the time when the UE's speaker starts to play the audio	**< 350 ms**
	Access time	The time between when a PTT user request to speak and when this user gets a signal to start speaking.	**< 300 ms**
	Concurrent calls	The maximum number of concurrent person-to-person and PTT calls that the system can handle	**>10 concurrent calls**
	Users in a group call	The maximum number of users in a PTT group call	**> 25 users**
Video	Throughput	The measured average data rate to support H265 (4K)	**DL: >25 Mbps** **UL: >25 Mbps**
	Latency	The time between when a video stream is captured and when the user receive the stream	**500 ms**

	Late stream entry time	The time to enter an ongoing MC-Video stream measured from the time that a user decides to monitor such a MC-Video stream, to the time when the UE's scree, starts to play the video	**350 ms**
	Concurrent streams	The maximum number of concurrent H265 streams that the system can handle	**> 10 concurrent video stream**
Messaging / Facsimile	Latency of distribution	The time required to distribute a message to all members of a distribution group	**< 1000 ms**
	Delivery failure	The percentage of messages that were not delivered after the delivery deadline	**< 0.1%**
Location	Localization latency	The time between the localization reading by a user device and the visualization over a remote C2 screen	**< 2000 ms**
Public warning broadcast	Coverage	The maximum distance where a device can receive the public warning message	**> 1500 m @ 43 dBm**
	Initialization time	The time to setup the public warning message network service before it being operational	**< 5min**
	Public warning latency	The time required to distribute a public warning message to the last device receiving it	**< 1000 ms**
Vital signs monitoring / telemetry	Monitoring latency	The time between the vital signs readings by a user device and the visualization over a remote C2 screen	**< 1000 ms**
Data	Data Rate	The maximum speed at which data is transferred between the source and its destination device	**> 100 Mbps**

Platform KPIs

Table 30: platform KPIs for PPDR use case

KPI name	Description	Objective
Autonomous edge installation time	The time to provision and setup autonomous edge software, including, configuration (all of day 0 operations)	**< 0.5 days**
Management framework footprint	The minimum (recommended) HW requirements for all the management (VIM, orchestrators) to run properly	**CPUs GB of RAM GB of storage**
Service establishment time	The elapsed time to setup a specific network service before it being operational (from the deploy command)	**< 5 min**

Orchestrator discovery time	The time required to discovery a new orchestrator entity once connectivity appears	**< 5 sec**
Single touch orchestration	Minimum number of workflow interventions to setup the autonomous edge software stack	**< 10**
Number of slices	The maximum number of slices concurrently supported by the system	**> 8**

7.7. UC3 – 5G Virtual Office

7.7.1. Test Cases

There are three test cases, one for each sub-scenario of the 5G Virtual Office use case. The multiple steps of each test case are detailed in the subsections below.

Ward Remote Monitoring

Table 31: 5G Virtual Office Ward Remote Monitoring test cases.

Title	Description
The doctor connects a UE to the video camera, microphone and sensors	The doctor in the office has direct access to the hardware located at the patient's room at the ward, so it is able to monitor the patient's condition remotely.
Doctor subscribes to alerts from sensors attached to a patient	All the sensors on the patient's room at the ward are connected to the hospital network, so it is possible to subscribe to alerts from sensor readings. A doctor that is responsible for a patient receives these alerts on his/her UE, regardless of his/her location.
Sensor levels move outside typical ranges, or an abnormal pattern is detected, so the doctor receives an alert	Examples: if the SpO2 level drops under the threshold, the system raises an alarm and places an alert to the responsible doctor's UE; if an abnormal ECG pattern is detected by machine learning, an alarm is raised, and an alert is sent to the responsible doctor's UE for further analysis.
Remote medical procedure support	A patient at the ward requires a medical procedure that needs supervision of a specialized doctor. The doctor, connects his/her UE to the patient sensors, camera and microphone and guides the staff, located in the ward, on the steps to perform the necessary procedure.

Intra-Hospital Patient Transport Monitoring

Table 32: 5G Virtual Office Intra-Hospital Patient Transport Monitoring test cases.

Title	Description
A patient needs to be transported from the ward to the radiology department	A doctor, in office, connects the UE to the sensors, camera and microphone on the patient to be transported.

The doctor monitors remotely the patient state during the transport	A doctor, at his office, connects his UE to the sensors, camera and microphone on the patient to be transported.
Patient transport starts	The staff starts moving the patient towards the Radiology department. The sensors remain connected and roam from microcell to microcell without any disruption in connectivity.
Supervised medical procedure required	The doctor, monitoring remotely, receives an alert that the patient blood pressure is dropping. Immediately, the doctor request that the appropriated medication is applied and supervises the procedure.
The patient undergoes radiology exam and then is returned to his room at the ward	During the exam and when returning to the room, the doctor can monitor the patient from office, without any connectivity loss. Also, machine learning algorithms always keep processing sensor's data in real time.

Ambulance Emergency Response

Table 33: 5G Virtual Office Ambulance Emergency Response test cases.

Title	Description
An ambulance is notified of the new call (patient's address, possible status)	An ambulance on its way back to the headquarters receives a notification from the central that an emergency is happening. The crew gets the patient's address and the status report.
Paramedics retrieve patient's electronic health records from the hospital (simulated)	The ambulance, on its way to the emergency location, connects to the hospital database and retrieves the patient's electronic health records.
The ambulance arrives at the patient´s address, the doctor is notified	The notification is generated automatically when the Vertical Applications detects that the ambulance arrived at the patient's location. It is based on Geofencing to select the group of doctors to receive the notification and to understand the location of the paramedics.
The doctor connects his UE to the ambulance's video camera, microphone and sensors	The doctor connects to the ambulance's video camera, microphone, and sensors. As the paramedic enters the patient's house, the doctor gets a live FPV video feed.
The doctor assesses the patient situation and countermeasures are performed by the paramedics	The doctor and the paramedic assess the patient's state and the paramedic deploys the countermeasures requested by the doctor. The paramedic can perform some simple procedures with the supervision of the doctor at the hospital.
Paramedics update electronic health records	As soon as the patient is stable, the paramedic updates the patient's electronic health records from the ambulance. The updated file is instantly accessible at the hospital.
The on-site staff gets notified of the imminent arrival of the ambulance (patient id)	The staff on the hospital are notified and can monitor time left before the arrival of the ambulance. At the same time, they prepare the room with the required equipment according to the information received from the scene.

7.7.2. Validation Tools

As defined in Section 7.2, the 5G Virtual Office use case adopts the generic validation framework architecture of FUDGE-5G, further specifying it for its needs. In Figure 25, this architecture is depicted in detail. It includes three sources for metrics: the 5G infrastructure and platform and the Kubernetes Cluster (functional metrics), as well as the stakeholders (non-functional metrics). For functional metrics, the process can follow different paths depending on how they are collected, aggregated, and correlated: they can come already as metrics, or they may require pre-processing if obtained through logging systems. Once these metrics and processed, they are visualised in the portal provided by Grafana. In the same portal, a different interface is used for non-functional metrics through the capabilities of Google Forms, aiming at collecting, processing and visualize feedback from stakeholders in the form of questionnaires.

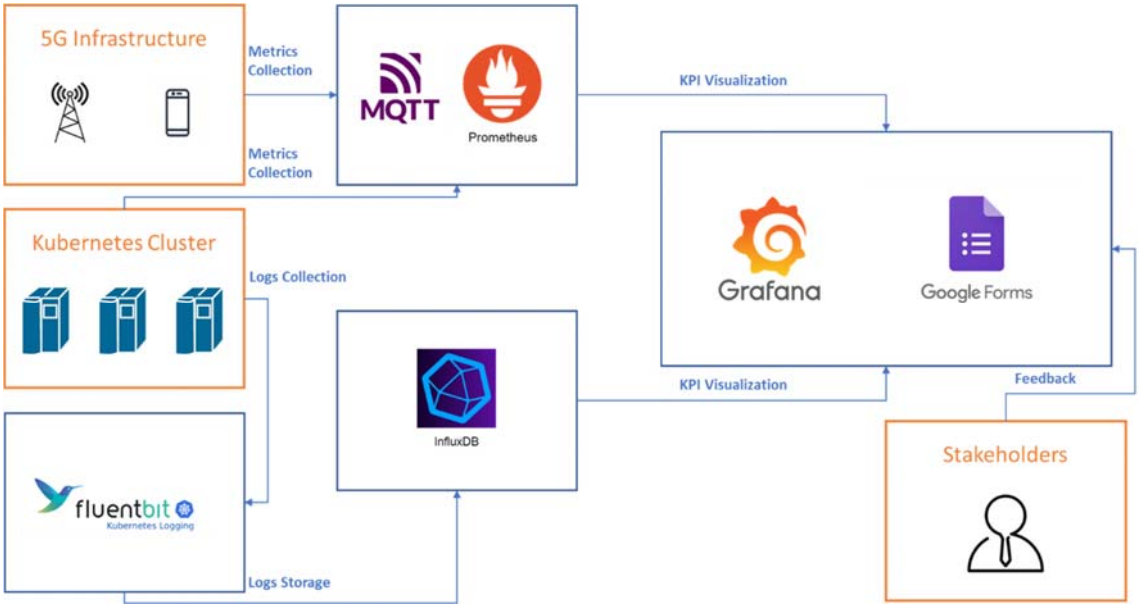


Figure 25: Validation Framework Architecture for 5G Virtual Office

Finally, a set of tools with be used to test the performance and user experience of the use case's platform in combination with the data sources that were previously mentioned. These will provide both quantitative and qualitative analysis regarding the execution of the use case and how its objectives are achieved and can be split into two different categories. IPerf3 will be used as traffic generator to validate the traffic values targeted in the KPIs. Also, Mean Opinion Score (MOS) will be calculated from ratings attributed by the stakeholders of the use case. This metric is especially relevant for the live video feeds from the ambulance and from the patient's room.

7.7.3. Validation KPIs

Platform KPIs

Table 34 lists the KPIs for the platform on the 5G Virtual Office UC, as well as its target values. The targets listed are the minimum required to ensure that the functionalities proposed on the use case are successfully delivered.

Table 34: Platform KPIs for 5G Virtual Office

Profile	Distance	Resolution	Frame Rate	E2E Latency	Packet error Rate	Date Rate UL	Date Rate DL
Live Video from patient´s room	up to 500m	3840 x 2160 4K	60 fps	400 ms	10^{-10} UL 10^{-7} DL	50 Mbps	20 Mbps
Live Video from ambulance	< 1 km	3840 x 2160 4K	60 fps	450 ms	10^{-10} UL 10^{-7} DL	50 Mbps	20 Mbps
	< 10 km		60 fps	600 ms	10^{-10} UL 10^{-7} DL		
	< 50 km		60 fps	1.5 s	10^{-10} UL 10^{-7} DL		
Remote Monitoring of Vital Signs from ambulance	< 1 km	n.d.	n.d.	10 ms	10^{-10} UL 10^{-7} DL	250 kbps	500 kbps
	< 10 km	n.d.	n.d.	20 ms	10^{-10} UL 10^{-7} DL	250 kbps	500 kbps
	< 50 km	n.d.	n.d.	50 ms	10^{-10} UL 10^{-7} DL	250 kbps	500 kbps
Remote Monitoring of Vital Signs within Hospital	up to 1 km	n.d.	n.d.	10 ms	10^{-10} UL 10^{-7} DL	250 kbps	500 kbps

Application KPIs

Table 35: Application KPIs for 5G Virtual Office

KPI ID	Description	Measurement procedure
UC3-K1	Incident Notification Time (INT) is the elapsed time from the moment the incident is identified (TS1) until the moment the users receive the notification (TS2). INT should not exceed 1000 ms.	The identification, the content of the message and TS1 and TS2 timestamps will be logged into a KPI pool.
UC3-K2	End-to-End HD Multimedia Latency (HML) is the elapsed time from the moment HD Multimedia is requested (TS1) by the operator until the multimedia is displayed at the operator screen (TS2). HML should not exceed 600ms.	The identification, the content of the message and TS1 and TS2 timestamps will be logged into a KPI pool.

UC3-K3	HD Multimedia Quality of Experience (QoE) represents the user satisfaction feedback by evaluating the responses to the question “How satisfied are you with multimedia experience” on a 0 a 5 scale (Very dissatisfied, Dissatisfied, Neutral, Satisfied, Very satisfied). 80% of users are expected to provide a “Very satisfied” feedback.	The identification, HD Multimedia QoE type, and response to the satisfaction inquiry will be logged into a KPI pool.
UC3-K4	Incident Response Action Time (IRT) is the elapsed time from the moment the incident was identified (TS1) until the moment the response action is initiated (TS2). IRT should not exceed 1000 ms.	The identification, the content of the message and TS1 and TS2 timestamps will be logged into a KPI pool.
UC3-K5	End-to-End SD Multimedia Latency (SML) is the elapsed time from the moment the device starts sending SD Multimedia (TS1) until it is displayed at the operator screen (TS2). SML should not exceed 400 ms.	The identification, the content of the message and TS1 and TS2 timestamps will be logged into a KPI pool.
UC3-K6	Mobitrust Platform QoE represents the user satisfaction feedback by evaluating the responses to the question “How satisfied are you with MOBITRUST platform” in a 0 a 5 scale (Very dissatisfied, Dissatisfied, Neutral, Satisfied, Very satisfied). It is expected that, at least, 80% of the users providing a “Very satisfied” feedback.	The identification, platform QoE type, and response to the satisfaction inquiry will be logged into a KPI pool.
UC3-K7	Sensor Data Latency (SDL) is the elapsed time between the timestamps of the messages since they are delivered from the device (TS1) until the moment they are received by the operator (TS2). SDL should not exceed 10 ms.	The identification, the content of the message and TS1 and TS2 timestamps will be logged into a KPI pool.
UC3-K8	Device Authentication Time (DAT) is the elapsed time from the moment the device is turned on (TS1) until the moment it receives the acknowledgement (TS2). DAT should not exceed 1000 ms.	The identification, the content of the message and TS1 and TS2 timestamps will be logged into a KPI pool.
UC3-K9	Device battery life should last 4 hours while delivering sensor data to the CCC, since they are turned on (TS1) until the moment they are shut down (TS2).	TS1 and TS2 for BK Devices are logged into a KPI pool.
UC3-K10	Device should run without restarts.	Connection log messages will help to identify the number of device restarts since they are turned on.
UC4-K11	Device communication should be available 99% of the time.	Device communication downtime (DT) will be retrieved from device logs. This KPI will consider the total running time (RT) to compute the formula (DT/RT)*100.

7.8. UC4 – Industry 4.0

7.8.1. Test Cases

Use case 4 has been divided into four different test applications, with an additional and optional test application to be performed. We detail in the following tables the different test cases or steps for each application. Information about the target KPIs, requirements and assumptions are also highlighted.

Table 36: Test cases for application 1: Remote monitoring as a service.

Test case	Description	Target KPIs	Assumption
1	Video streaming of remote assets and processes – no image processing.	UL throughput, DL throughput, E2E latency	8 streams of 4K-quality. *UL throughput ideal requirement*: 200 Mbps
2	Video streaming of remote assets and processes – image processing at the edge node.	UL throughput, DL throughput, E2E latency	8 streams of 4K-quality. *UL throughput ideal requirement*: 200 Mbps
3	Network orchestration – dynamic resources allocation	QoS	-
4	Data traffic handling – seamless handling of traffic with varying priority levels. Traffic with high priority is prioritized	Throughput, Reliability	-
5	Network throughput handling with distance and mobility	Throughput vs static distance, Throughput vs. moving object	Moving object speed of up to 20-80 cm/s
6	Coverage of NPN with multiple gNB and smooth handling of client handover from one gNB to another.	Availability, Latency	-

Table 37: Test cases for application 2: Remote control as a service with real-time feedback.

Test case	Description	Target KPIs	Assumption
1	Video streaming of remote assets and processes with equipment control running in parallel over the same network	UL throughput, DL throughput, E2E latency	8 streams of 4K-quality. *UL throughput requirement*: 200 Mbps *Control requirement*: max. 10ms latency.
2	TSN support with 5G NPN	TSN for IP traffic, TSN for non-IP traffic	-
3	Time sync functionality evaluation	Timing accuracy	-
4	Data traffic handling – seamless handling of traffic with varying	Throughput, Reliability	8 types of traffic will be simulated

	priority levels. Traffic with high priority is prioritized		
5	Network throughput handling with distance and mobility	Throughput vs static distance, Throughput vs. moving object.	Moving object speed of up to 20-80 cm/s
6	Coverage of NPN with multiple gNB and smooth handling of client handover from one gNB to other	Availability, Latency	-
7	Localization service over 5G	Position accuracy	-

Table 38: Test cases for application 3: 5G adaptability in industrial environments.

Test case	Description	Target KPIs
1	Transmission power level control for safe operations in hazardous areas	UL throughput, DL throughput, E2E latency, Reliability
2	Coverage in dense environments with heavy metal and concrete construction – onshore/offshore. Small cell coverage and options to connect repeaters.	QoS
3	Interoperability and hardware independency of 5G core &f RAN from different vendors.	Reliability
4	Impact of 5G spectrum on NPN.	Frequency bands to be tested in Norway
5	5G devices and network provisioning	Software as a service test, Whitelisting

Table 39: Test cases for application 4: Process control over 5G.

Test case	Description	Target KPIs
1	PID over 5G – simulated process.	Quality of Control (QoC)
2	PID over 5G – optional (test bed).	QoC
3	Control functionality with physical controller.	QoC
4	Control functionality with soft/virtual controller.	QoC

Table 40: Test cases for application 5 (optional): VR + AR control over 5G.

Test case	Description	Target KPIs
1	IoT over 5G	QoS
2	VR over 5G	QoS

3	AR over 5G	QoS
4	Positioning over 5G outdoor	Accuracy
5	Positioning over 5G indoor	Accuracy
6	Test cases 1-3 orchestrated together	QoS

7.8.2. Validation tools

A set of tools with be used to test the performance and user experience of the use case's platform. These will provide both quantitative and qualitative analysis regarding the execution of the use case and how its objectives are fulfilled.

Test equipment will be industrial devices and host systems will be actual process control software. Use case partners shall meet the application requirements transparently without having host system intervention. In addition, ABB expects to be provided with adequate software and tools to design, provision, commission and operate 5G NPN with connected devices. The tools being referred here are the software packages needed to configure/control the 5G NPN. The test applications in end devices and host systems will be designed assuming that the network provides the services within the acceptable level of target KPIs.

7.8.3. Validation KPIs

The table below lists the ideal minimum required application and network KPIs to ensure that the functionalities proposed on the use case are successfully delivered, as well as the expected achievable values for these KPIs with the hardware available in the project.

In the factory, a controller will interact with many sensor and actuator devices located within a small area (up to 100 m^2). These applications have high performance requirements such as low latency, high reliability, and deterministic delivery of messages. The following validation KPIs and performance requirements are expected to be met.

Application KPIs

Table 41: application KPIs for Industry 4.0 use case

KPI name	Description	Achievable requirements	Ideal requirements
End-to-end latency	Latency is measured as the time delay from message generated at source until its arrival at the end node.	Depends on the application	10 ms
NPN 5G latency	Considered as part of the end-to-end latency. Delay introduced by the 5G NPN network	10 ms	1-2 ms
DL throughput	Average data rate in the DL. In typical 5G consumer use cases, DL throughput is of utmost importance. Condition monitoring,	900 Mbps	4 Gbps

	optimization, VR, AR, and CCTV applications require significant throughputs		
UL throughput	Average data rate in the UL. Note that in in industrial use cases UL throughput is also important	80 Mbps	200 Mbps
Power consumption	Controlling energy levels is key in this use case, because of the need to reduce production costs.	-	-
Transmission power	Transmission power levels in the gNB must be kept to a lower value to ensure that it is safe to operate the equipment when deployed in a hazardous area in the considered frequency range.	EIRP ~ 2-10 W	EIRP ~ 2-10 W
5G coverage	The maximum distance where a device can receive the public warning message. gNB transmission power levels should be enough to provide coverage and support the required communication in the industrial environment. This will be supported for the considered frequencies.	Related to consumption	Related to consumption
Reliability	Quality of a system of being trustworthy or of performing consistently well.	99.9%	99.9%
Availability	This value will vary depending on the outage time permitted in a year, that is, the period of time when the system is unavailable.	TBD	99.8% for 17h 31m 53s 99.9% for 8h 45m 56s 99.999% for 5m 15s 99.999999% for 0.3s
Mobility	Maximum speed tolerated for guaranteeing a minimum reliability specified.	80-100 cm/s	20-80 cm/s
QoS	Overall performance of a service experienced by the users of the network.	-	-
Position accuracy	The difference in location between a measured value to a standard or known value.	< 1 m	< 1 m
QoC	Process that ensures that product quality is maintained or improved.	-	-

7.9. UC5 – Interconnected NPNs

7.9.1. Test Cases

There are four test cases, depending on the scenarios covered by this Interconnected NPNs. The multiple steps of each test case are detailed in the subsections below. These tests are used as both functional tests – checking if the system is properly functioning – as well as to measure some specific performance characteristics.

Interconnection of the NPNs

Table 42: Interconnected NPNs connectivity between NPNs test case

Title	Description
Establishment of connectivity between Visited and Home Network	Visited network initiates connection to the home network, if there is visited subscriber which needs to be authenticated by the home network.
Termination of connectivity between Visited and Home Network	The visited and the home network should terminate their interconnection in case there is no visited subscriber connected.

Home Subscriber Authentication

Table 43: Interconnected NPNs home subscriber authentication test case

Title	Description
Home subscriber connects to the home network	Home subscriber is within the coverage of home network, it initiates registration procedure by sending the registration request to the local AMF through the local RAN.
Home subscriber authenticated by the home network	After receiving the registration request, the home subscriber gets authorized by the home network.

Visited Subscriber Authentication

Table 44: Interconnected NPNs visited subscriber authentication test case

Title	Description
Visited subscriber connects to the visited network	Visited subscriber is within the coverage range of a potential visited NPN, it initiates registration procedure by sending the registration request to the local AMF through the local RAN.

Identity check for the visited subscriber	The local AMF in the visited network will determine the identity provided by the visited subscriber belongs to the local domain or an external one. In case of external domain AMF will forward the request to local SBC.
Discovering home network and establishing connectivity	Visited networks should discover dynamically home networks for the visited subscribers and initiate a secure connection towards the home network.
Forwarding message to the home network for the visited subscriber	Once the connection is established the SBC in visited network will forward the authentication request for the visited subscriber to the home network SBC.
Visited subscriber authenticated by the home network	After receiving the authentication request, the visited subscriber gets authorized by the home network and the response is sent to the visited network to complete the registration procedure.

Access to network services

Table 45: Interconnected NPNs access to local and remote network services test case

Title	Description
Access to local network services	Both Home and Visited subscriber will have access to the local network services and local offload.
Access to home network services	Subscribers connected to the home network will have access to home network services. Subscribers connected to the visited network will have access to home network services in case of home routed roaming, not for local breakout.

7.9.2. Validation tools

The following set of tools is planned to be used to test the scenarios and validate the performance of the platform. These will provide both quantitative and qualitative analysis regarding the execution of the use case and how its objectives are fulfilled.

- Emulated UEs and gNodeBs within the Open5GCore testbed will be used to validate the authorization framework.
- Devices with different PLMNs will be connected to the 5G cores through a 5G RAN. The interoperability testing will be performed and devices for which the PLMNs belong to another domain will be authenticated by the remote domain.
- The Open5GCore integrated Benchmarking Tool (BT) will be used to validate the capacity and performance of the system. The variation of procedure duration will be validated for both home and visited subscribers.

7.9.3. Validation KPIs

Performance KPIs

As this use case interconnects two distinct networks using a third party backhaul. The backhaul is a “best-effort” network which is not under the control of the experiments. Because of this all the specific KPIs are dependent on the backhaul characteristics (e.g. the delay of the best effort network should be added to the procedures delay, etc.).

The KPI performance values presented into the next table are done without including the impact of the backhaul. This will be computed during the actual execution of the measurements.

Table 46: performance KPIs for the Interconnected NPNs use case

KPI ID	Type of UE	Description	Measurement procedure	Measurement
UC5-K0	N/A	Control KPI to determine the “best-effort”	Parallel control during the other measurements of backhaul RTT and capacity with ICMP measurements and iPerf capacity and jitter measurement.	Depending on the best-effort network.
UC5-K1	Home Network UE	Time taken by the UE for completing the registration procedure with the core network as defined by 3GPP in the specifications.	To measure this parameter, a UE from Benchmarking tool will be registered to calculate the time for completing the procedure.	60 ms
UC5-K2		Time taken by the UE for completing the PDU session establishment procedure with the given data network.	To measure this parameter, PDU session establishment procedure will be triggered for a UE from Benchmarking tool to calculate the time for completing the procedure.	40 ms
UC5-K3		Time taken by the UE for completing the de-registration procedure with the core network as defined by 3GPP in the specifications.	To measure this parameter, a UE from Benchmarking tool will be de-registered to calculate the time for completing the procedure.	20 ms
UC5-K4		RTT for data path to home network.	To measure this parameter, ping will be executed to home network DNN.	15 ms

UC5-K5	Visited Network UE	Time taken by the UE for completing the registration procedure with the core network as defined by 3GPP in the specifications.	To measure this parameter, a UE from Benchmarking tool will be registered to calculate the time for completing the procedure.	60 ms + 8 * Backahul RTT.
UC5-K6		Time taken by the UE for completing the PDU session establishment procedure with the given data network.	To measure this parameter, PDU session establishment procedure will be triggered for a UE from Benchmarking tool to calculate the time for completing the procedure.	40 ms + 4 * Backhaul RTT
UC5-K7		Time taken by the UE for completing the de-registration procedure with the core network as defined by 3GPP in the specifications.	To measure this parameter, a UE from Benchmarking tool will be de-registered to calculate the time for completing the procedure.	20 ms + 2 * Backhaul RTT
UC5-K8		RTT for data path to home network.	To measure this parameter, ping will be executed to home network DNN.	15 ms + 2 * Backhaul RTT
UC5-K9		RTT for data path to visited network.	To measure this parameter, ping will be executed to visited network DNN.	15 ms

For the network capacity, there is a direct dependency on the backhaul capacity to the home network. The following KPIs will be measured:

Table 47: performance KPIs for the Interconnected NPNs use case

KPI ID	Type of UE	Description	Measurement procedure	Measurement
UC5-K10	Visited Network UE	Data path capacity in the local network	Fill up the local RAN connection	Mbps
UC5-K11		Effective data path capacity in the local network	Fill up the local RAN connection	Effective capacity (Mbps) / Momentary Outbound Capacity (Mbps)
UC5-K12		Data path capacity over the best effort backhaul	Fill up the local RAN connection	Effective capacity (Mbps) / Momentary

				Backhaul (Mbps)	Capacity

8. Conclusions

This document provided the technical blueprint and the validation framework for the five FUDGE-5G use cases taking into account the input from the vertical stakeholders. A short overview of the DevOps environment and the FUDGE-5G innovations was also presented. This document will be the guideline for the overall project in terms of realising the five use cases.

References

[1] FUDGE-5G, “D1.2 FUDGE-5G Platform Architecture: Components and Interfaces”.

[2] Detecon Consulting, “5G Campus Networks: An Industry Survey,” 2019.

[3] “Key 5G Use Cases and Requirements,” 5G-ACIA, 2020.

[4] FUDGE-5G, “D2.1 FUDGE-5G Technology Components and Platform – Interim Release”.

[5] D. Trossen and S. Robitzsch, “MWC18: 5G Networks Demo,” InterDigital, 2018. [Online]. Available: https://www.interdigital.com/videos/mwc18-5g-networks-demo.

[6] European Broadcaster Union, “TR 056: 5G for Professional Media Production and Contribution,” 2020. [Online].

[7] 5GCity, “5GCity: A distributed cloud & radio application for 5G Neutral Hosts,” [Online]. Available: https://www.5gcity.eu/.

[8] 5G-XCAST, “ 5G-Xcast: Broadcast and Multicast Communication Enablers for the Fifth Generation of Wireless Systems,” [Online]. Available: 5g-xcast.eu.

[9] 5G-SOLUTIONS, “5G Solutions for European Citizens,” [Online]. Available: https://www.5gsolutionsproject.eu .

[10] 5G-TOURS, “5G-TOURS: SmarT mObility, media and e-health for toURists and citizenS,” [Online]. Available: http://5gtours.eu .

[11] B. Altman, “5G for media and entertainment: from theory to practical use cases,” *IABM Journal,* no. 114, 2020.

[12] 5G-MAG, “5G-MAG Explainer: Non-Public 5G Networks for Content Production,” 2021. [Online].

[13] Everything RF, “5G Frequency Bands,” 2018. [Online]. Available: https://www.everythingrf.com/community/5g-frequency-bands.

[14] 3GPP, “TR 22.263. Service requirements for Video, Imaging and Audio for Professional Applications (VIAPA),” 2020. [Online].

[15] 3GPP, “TR 22.827. Technical Specification Group Services and System Aspects, Study on Audio-Visual Service Production; Stage 1,” [Online].

[16] European Broadcaster Union, “TR 054: 5G for the Distribution of Audiovisual Media Content and Services,” 2020. [Online].

[17] European Broadcaster Union, “Assessment of Available Options for the Distribution of Broadcast Services,” 2014. [Online].

[18] JPEG, “JPEG XS, a new standard for visually lossless low-latency lightweight image coding system,” 2019. [Online]. Available: http://ds.jpeg.org/whitepapers/jpeg-xs-whitepaper.pdf.

[19] E. Reuss, “VC-5 Video Compression for Mezzanine Compression Workflows,” in *SMPTE 2013 Annual Technical Conference & Exhibition*, Hollywood, 2013.

[20] PA consulting, “5G for Smart Manufacturing: Insights on how 5G and IoT can transform Industry,” 2020.

[21] Andreas Müller, Bosch, “5 reasons for 5G: What does the new communications standard mean for Bosch and Industry 4.0?,” 2020.

[22] B. V. G. M. J. S. János Farkas, “5G-TSN integration meets networking requirements for industrial automation,” *Ericsson,* 2017.

[23] GSMA, “5G LAN Support for IoT in Cloud Office,” Future Networks, 2020.

[24] GSMA, “5G IoT Private & Dedicated Networks for Industry 4.0,” 2020.

[25] Qualcomm Technologies, Inc., “Private LTE networks create new opportunities for industrial IoT,” 2017.

[26] K. Auman, “Overcoming Key Pain Points When Adopting Industry 4.0 Strategies,” in *LogicBay press release*, March 2020.

[27] D. Geiger, “5 Challenges to Overcome to Increase Manufacturing Productivity,” in *Aegis Software press release*, May 2019.

[28] CAST, Inc, “TSN-EP: TSN Ethernet Endpoint Controller”.

[29] 5G-ACIA , “5G Non-Public Networks for Industrial Scenarios,” White Paper, July 2019.

[30] C. Mannweiler, B. Gajic, P. Rost, R. S. Ganesan, C. Markwart, R. Halfmann, J. Gebert and A. Wich, “Reliable and Deterministic Mobile Communications for Industry 4.0: Key Challenges and Solutions for the Integration of the 3GPP 5G System with IEEE,” in *24. ITG-Symposium*, Osnabrueck, Germany, 2019.

[31] P. Herd and J. H. Adamowicz, “GREEN 5G FOR A GREENER, SMARTER EUROPE,” [Online]. Available: https://huawei.eu/press-release/green-5g-greener-smarter-europe.

[32] Huawei Technologies,, “Green 5G: Building a sustainable world,” Analysis Mason, 2020.

[33] Ericsson, “5G spectrum for local industrial networks,” June 2020.

[34] J. Farkas, B. Varga, G. Miklós and J. Sachs, “5G-TSN integration meets networking requirements for industrial automation,” *ERICSSON TECHNOLOGY REVIEW,* August 2019.

[35] Deutsche Telekom, “5G technology in industrial campus networks,” [Online]. Available: https://www.telekom.com/en/company/details/5g-technology-in-campus-networks-556692.

[36] Telekom, “5G technology in industrial campus networks,” [Online]. Available: https://www.telekom.com/en/company/details/5g-technology-in-campus-networks-556692.

[37] European 5G observatory, “5G private licences spectrum in Europe,” April 2020.

[38] Ericsson, “You need a robust signaling solution in 5G too!,” [Online]. Available: https://www.ericsson.com/en/blog/2019/10/you-need-a-robust-signaling-solution-in-5g-too.

[39] M. Keltsch, S. Prokesch, O. P. Gordo, J. Serrano, T. Phan and I. Fritzsch, “Remote Production and Mobile Contribution Over 5G Networks: Scenarios, Requirements and Approaches for Broadcast Quality Media Streaming,” in *BMSB*, Valencia, 2018.

[40] VideoXlink, [Online]. Available: https://www.videoxlink.com.

[41] Nevion, [Online]. Available: https://nevion.com/products/nevion-virtuoso-jpeg-xs-uhd-hd/.

[42] NR LTE Blog, “Supplementary Uplink,” [Online]. Available: https://info-nrlte.com/category/5g-nr/supplementary-uplink/.