5G ExPerimentation Infrastructure hosting Cloud-nativE Netapps for public proTection and disaster RElief

Innovation Action – ICT-41-2020 - 5G PPP – 5G

Innovations for verticals with third party services

D4.2: Network functions implementation

Delivery date: March 2023

Dissemination level: Public

Project Title:	**5G-EPICENTRE - 5G ExPerimentation Infrastructure hosting Cloud-nativE Netapps for public proTection and disaster RElief**
Duration:	**1 January 2021 – 31 December 2023**
Project URL	https://www.5gepicentre.eu/

This project has received funding from the European Union's Horizon 2020 Innovation Action programme under Grant Agreement No 101016521.

www.5gepicentre.eu

Document Information

Deliverable	D4.2 Network functions implementation
Work Package	WP4: Platform integration and VNF development
Task(s)	T4.2: Container Network Functions and Network Application repositories
Type	Report
Dissemination Level	Public
Due Date	M27, March 31, 2023
Submission Date	M27, March 31, 2023
Document Lead	Daniel del Teso (NEM)
Contributors	Alain Dubois (ADS) Laurent Drouglazet (ADS) Carlos Martins Marques (ALB) Jorge Carapinha (ALB) Ankur Gupta (HHI) Konstantinos Apostolakis (FORTH) Almudena Díaz (UMA) Josep Mangues-Bafalluy (CTTC) Manuel Requena (CTTC) Pedro Tomás (ONE) Luís Cordeiro (ONE) Daniel del Teso (NEM) Ivan Gonzalez (NEM) Daniel Alcaraz (RZ) Donal Morris (RZ) Rainer Wragge (OPTO) Antonio Zanesco (YBQ) Antonis Protopsaltis (ORAMA)
Internal Review	Daniel Alcaraz (RZ) Apostolos Siokis (IQU)

Document history

Version	Date	Changes	Contributor(s)
V0.1	01/11/2022	Initial deliverable structure	Daniel del Teso (NEM)
V0.2	15/11/2022	60% of the deliverable content	Alain Dubois (ADS) Laurent Drouglazet (ADS) Ankur Gupta (HHI) Pedro Tomás (ONE) Luís Cordeiro (ONE) Daniel del Teso (NEM) Pablo Garrido (NEM) Daniele Ronzani (ATH) Daniel Alcaraz (RZ) Donal Morris (RZ) Rainer Wragge (OPTO) Antonio Zanesco (YBQ) Antonis Protopsaltis (ORAMA)
V0.3	25/01/2023	90% of the deliverable content	Luigi D'Addona (IST) Anna Maria Spagnolo (IST) Daniele Ronzani (ATH) Luís Cordeiro (ONE) Alain Dubois (ADS) Laurent Drouglazet (ADS) Sozos Karageorgiou (EBOS) Daniel del Teso (NEM) Pedro Tomás (ONE) Luís Cordeiro (ONE) Konstantinos Apostolakis (FORTH)
V1.0	13/02/2022	Internal Review Version	Daniel del Teso (NEM)
V1.1	17/02/2023	1st version with suggested revisions	Apostolos Siokis (IQU)
V1.2	20/03/2023	2nd version with suggested revisions	Daniel Alcaraz (RZ)
V1.3	20/03/2023	First revisions after internal review	Daniel del Teso (NEM)
V1.5	24/03/2023	Quality review: copyediting; proofreading; formatting	Konstantinos Apostolakis (FORTH)
V1.6	30/03/2023	First revisions after final review	Alain Dubois (ADS) Daniel del Teso (NEM) Ankur Gupta (HHI) Pedro Tomás (ONE)

			Donal Morris (RZ) Rainer Wragge (OPTO) Antonio Zanesco (YBQ) Antonis Protopsaltis (ORAMA)
V2.0	31/03/2023	Final version for submission	Daniel del Teso (NEM)

Project Partners

Logo	Partner	Country	Short name
	AIRBUS DS SLC	France	**ADS**
	NOVA TELECOMMUNICATIONS SINGLE MEMBER S.A.	Greece	**NOVA**
	Altice Labs SA	Portugal	**ALB**
	Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e.V.	Germany	**HHI**
	Foundation for Research and Technology Hellas	Greece	**FORTH**
	Universidad de Malaga	Spain	**UMA**
	Centre Tecnològic de Telecomunicacions de Cata-lunya	Spain	**CTTC**
	Istella SpA	Italy	**IST**
	One Source Consultoria Informatica LDA	Portugal	**ONE**
	Iquadrat Informatica SL	Spain	**IQU**
	Nemergent Solutions S.L.	Spain	**NEM**
	EBOS Technologies Limited	Cyprus	**EBOS**
	Athonet SRL	Italy	**ATH**
	RedZinc Services Limited	Ireland	**RZ**
	OptoPrecision GmbH	Germany	**OPTO**
	Youbiquo SRL	Italy	**YBQ**
	ORamaVR SA	Switzerland	**ORAMA**

List of abbreviations

Abbreviation	Definition
5G PPP	5G Infrastructure Public Private Partnership
5GC	5G Core
aaS	as-a-service
AE	Analytics Engine
AF	Application Functions
AI	Artificial Intelligence
AICO	Analytics, Intelligence, Control and Orchestration
AMF	Audio Media Function
API	Application Programming Interface
AR	Augmented Reality
AS	Application Server
ASF	Audio Signalisation Function
AUSF	Authentication Server Function
BK	Mobitrust BodyKits
CAS	Controlling Application Server
CCC	Central Command Centre
CMS	Configuration Management Server
CNF	Containerized Network Function
CNI	Container Network Interface
COTS	Commercial-off-the-Shelf
CSCF	Call Session Control Function

CSI	Container Storage Interface
DB	Database
DHCP	Dynamic Host Configuration Protocol
DMF	Data Management Function
DNS	Domain Name System
E2E	End-to-End
ECG	Electrocardiogram/Electrocardiography
eMBB	Enhanced Mobile Broadband
FRMCS	Future Railway Mobile Communication System
GA	Grant Agreement
GMS	Group Management Server
gNB	gNodeB
HMD	Head-Mounted Display
HSPF	Holistic Security and Privacy Framework
HSS	Home Subscriber Sever
I-CSCF	Interrogating CSCF
IdMF	Identity Management Function
IdMS	Identity Management Server
IoT	Internet of Things
IMS	IP Multimedia Subsystem
IPR	Intellectual Property Rights
KMS	Key Management Server
KPI	Key Performance Indicator
KPIF	KPI Function

LMF	Location Managament Function
MCData	Data Critical Communication
MCPTT	Mission-Critical Push-to-Talk
MCVideo	Video Critical Communication
MCX	Mission Critical Services
ML	Machine Learning
mMTC	Massive Machine Type Communications
MQTT	Message Queuing Telemetry Transport
MVD	Mobile Visualisation Device
NEF	Network Exposure Function
NF	Network Functions
NIDS	Network Intrusion and Detection System
NRF	Network Repository Function
NS	Network Services
NSSAAF	Network Slice-Specific Authentication and Authorisation Function
NSSF	Network Slicing Selection Function
NWDAF	Network Data Analytics Function
P-CSCF	Proxy CSCF
PAS	Participating Application Server
PCF	Policy Control Function
PNF	Physical Network Function
PPDR	Public Protection and Disaster Relief
PVC	Persistent Volume Claim
QoE	Quality of Experience

QoS	Quality of Service
RAN	Radio Access Network
RBAC	Role-Based Access Control
RTCP	Real-Time Transport Control Protocol
RTP	Real-Time Transport Protocol
S-CSCF	Serving CSCF
SCP	Secure Copy Protocol
SCTP	Stream Control Transmission Protocol
SDS	Short Data Service
SFC	Service Function Chaining
SIP	Session Initiation Protocol
SMF	Situation Management Function
SMP	Smart Multi Platform
SpO2	Oxygen Saturation
SRTCP	Secure RTCP
SRTP	Secure RTP
TCM	Transmission Control Protocol
UAV	Unmanned Aerial Vehicle
UC	Use Case
UDM	Unified Data Management
UDP	User Datagram Protocol
UDR	Unified Data Repository
UE	User Equipment
UI	User Interface

UL	Uplink
UPF	User Plane Function
URLLC	Ultra-Reliable Low Latency Communications
VA	Vertical-agnostic
VM	Virtual Machine
VMF	Video Media Function
VNF	Virtualised Network Function
VS	Vertical-specific
VSF	Video Signalisation Function
WFS	Webfront Server
WebRTC	Web Real-Time Communication

Executive summary

This document provides an overview of the different Network Applications developed so far in the framework of 5G-EPICENTRE. The work carried out in T4.2 “Container Network Functions and Network Application repositories” is therefore presented. This provides a quick overview of the approach taken to conceptualise the term “Network Application” within 5G-EPICENTRE, classifies the developments on the basis of the definitions given, and it provides a visual and comprehensible summary of the developments made.

The work has generated a rich repository of solutions specifically designed for the Public Protection and Disaster Relief (PPDR) sector, which will be able to make use of them to accelerate their adoption of new broadband technologies. The different vertical Network Applications will demonstrate what 5G technology can achieve, thanks to the experimental processes that will be accomplished. They will also be included in the repository, allowing third parties to use them in their own experimental processes. This provides the 5G-EPICENTRE Platform with attractive tools that can be used by PPDR agencies, allowing them to focus on more specific developments.

In addition, specially designed Network Applications have been created to grant common solutions to the industry's experimental processes. New Network Applications have been created for Key Performance Indicator processing, security in containerised environments, or control over 5G network conditions. This will provide 5G-EPICENTRE with complementary tools to offer to third parties, common and wide-ranging solutions, which will accelerate the experimental processes.

An attractive repository has therefore been created for the PPDR sector, which can be considered as a living entity, as it can grow and increase the number of Network Applications it offers.

Table of Contents

List of Figures

List of Tables

1 Introduction

This deliverable shows a report of the different implementations of Network Functions (NFs) that the 5G-EPICENTRE project has submitted. It therefore provides a detailed overview of how each Network Application has chosen to bundle its NFs, and the Network Services (NSs) they may form, to achieve a value chain, interacting with the 5G-EPICENTRE platform and the 5G network. This chaining has been done on the basis of the definitions made in D1.4 “Experimentation requirements and architecture specification final version” (M25), which provides the first project's approach to NFs, physical or virtual, and how they are linked together to achieve more complete and complex solutions such as Network Applications. Aligned with other ICT-41 projects [1] [2] [3], this report also explores the differentiation of Network Applications between those that are independent of the vertical service (or in the project’s case, Public Protection and Disaster Relief) and offer generic solutions to the user, and those that are specific to the vertical.

Some of the developments made in this Task will be included in the repository of solutions that the 5G-EPICENTRE platform will offer to its users, facilitating the experimental process necessary to transition Public Protection and Disaster Relief (PPDR) solutions towards 5G broadband networks. The project will offer curated Network Applications that will allow third-party experimenters to focus on more specific aspects of their own service, accelerating the experimental process, and showing (through technology validators) how far the technology can go. For this, Network Applications stored in the repository will be eligible from the 5G-EPICENTRE platform Frontend, as described in D1.4 and will be shown in more detail in D3.2 (M30); chained and deployed in the corresponding testbed together with the PPDR vertical service to be analysed, as established in the framework of T2.2 “VNF containerization at the network edge” and T2.3 “VNF chain placement, re-routing and re-mapping”; and the experimentation will start following the premises adopted in D1.6 “Experiment evaluation strategy and experimentation plan”.

Although a Network Application may contain different components with different objectives and approaches, this document has categorised them based on their general purpose within the 5G-EPICENTRE framework. This approach is aligned with the work carried out by the latest 5G Infrastructure Public Private Partnership (5G PPP) initiatives, which have further worked in the Network Application conceptualisation in [1]-[6]. Thus, all converge in Network Applications embodying software tailored to meet specific requirements of a 5G network tenant. Within 5G-EPICENTRE, this PPDR-tailored, vertical-specific software will require custom experimental facilities to support stress testing and validation prior to solutions being moved to production. This is especially true for Public Safety Services or applications designed for PPDR, where the need to guarantee the unobtrusive exchange of not only voice, but also video, data and images [7], especially under extreme network conditions, is vital to the capacity of PPDR agents to carry out their duties.

On the other hand, the Network Application structures proposed are shown at high level due to the public nature of the document. The language used has also taken this into account, aiming to reach all 5G-EPICENTRE platform’s potential users. It should be noted that each of the Network Applications shown in the document could in turn be decomposed into chains of NFs, or sub-Network Applications. The document has also sought to be concise, avoiding long sections and summarising as much as possible each Network Application’s functionalities and features.

This D4.2 therefore initially provides an overview to the Network Application approach followed by the project. Then it summarises the different Network Applications that will be made available on the 5G-EPICENTRE platform, exploring their features and how they are going to be used by third parties. Then it categorises the Network Applications by providing the reasoning that has been employed, and the context under which they are framed. Finally, it provides more detail on the different Network Applications built on the 5G-EPICENTRE framework, differentiating between vertical-agnostic and vertical-specific.

1.1 Mapping of project's outputs

The purpose of this section is to map 5G-EPICENTRE Grant Agreement (GA) commitments within the formal Task description, against the project's respective outputs and work performed (Table 1).

Table 1: Adherence to 5G-EPICENTRE's GA Deliverable & Tasks Descriptions

5G-EPICENTRE Task	Respective Document Chapters	Justification
T4.2: Container Network Functions and Network Application repositories *"This Task will deal with function developers […] carrying out development of all necessary VNFs within the 5G-EPICENTRE framework […]".*	Section 2.3 – Network Application summary	This Section provides a summary of the different Network Applications that have been collected in the framework of 5G-EPICENTRE. These in turn are further defined in Sections 3 and 4.
T4.2: Container Network Functions and Network Application repositories *"[…] this Task will deal with the development of micro-VNFs, which shall then be chained together to provide the various capabilities offered by the overall 5G-EPICENTRE framework via rich, curated repositories of Network Application".*	Section 3 – Vertical-agnostic Network Applications Section 4 – Vertical-specific Network Application	The two Sections offer an immersion into the degree of containerisation of each solution; the different NSs that compose it; its structure; and functional definitions of each NF.
T4.2.1: (micro-)VNF development *"[…] development of network functions, by identifying common middlebox functionalities (e.g. firewalls, load-balancers, etc.) […]"*	Section 3 – Vertical-agnostic Network Applications	This Section explores Network Applications that, due to their general purposes, can be consumed with other vertical Network Applications, which are more specific, and end-user driven.
T4.2.1: (micro-)VNF development *"[…]. Where possible, these traditional VNFs will be decomposed into groups of micro-VNFs, following the micro-services approach, […], thus allowing VNF placement even on low-cost edge devices and reduced VNF-to-user end to end (E2E) latency. These micro-VNFs will consist of a single container, […]"*	Section 3 – Vertical-agnostic Network Applications Section 4 – Vertical-specific Network Application	These Sections explore the different Network Application approaches to containerisation, the way the project manages different approaches, the different NS included in each solution and their definition and purpose. The level of containerisation can be checked in Section 2.3.

T4.2.2: Network Application provision *"This sub-Task will deal with service function chaining (SFC) for forming and maintaining complex, E2E services (Network Application) specifically built to satisfy the requirements of public safety, mission-critical communications and applications. [...] to deliver a curated repository of Network Application images that can be used by application service providers in their experimentation activities".*	Section 3 – Vertical Agnostic Network Application	The real potential of the project lies on one hand on the middleware created as vertical-agnostic Network Applications, and, on the other hand, on the vertical-specific repository. The definitions and decisions taken, facilitate the incorporation of new Network Applications and their integration into the platform, or the repository.
	Section 4 – Vertical Specific Network Application	

2 General overview

5G technology uncovers new options, such as Enhanced Mobile Broadband (eMBB), Massive Machine Type Communications (mMTC) and Ultra-Reliable Low Latency Communications (URLLC). The advantages offered by the 5G technology are however not just limited to improved capacities for legacy networks. The technology is designed so that vertical services can make use of it, even interact with the network, and (above all) have dynamic deployment options that streamline processes.

While the benefits that new telephony networks can bring to the PPDR sector are indisputable, the transition required to access these benefits is often complicated. The technology exists, and it can be used, but it requires a major upgrade in both vertical solutions and in the conceptualisation of deployment itself. Therefore, the 5G-EPICENTRE project has focused on generating a comprehensive catalogue of Network Applications. Aligned with the work done in the other ICT-41 projects, a solution is sought that facilitates the integration of the various solutions of the PPDR sector, in an agile and dynamic way. In this way, by making use of Network Applications, a development paradigm for vertical services proposed by the 5G PPP [8], it will be possible to accelerate the experimental processes in the PPDR sector. The agility with which these new software models can interconnect with each other to create value chains, will make it easier to interact between the services offered by the platform, and the vertical services that want to use it.

On the other hand, the microservices orientation [4]; the cloud-native architecture proposed in the project [9]; and the virtualisation of a large part of the 5G-EPICENTRE solution (see D4.4 and D1.4), offer an environment in which deploying a complete new experiment will take a short amount of time. Therefore, the orientation adopted seeks not only to be compatible with the widest variety of vertical solutions, but also to ensure that its experimentation processes are agile and do not require long assembly and development periods. Thus, the 5G-EPICENTRE platform will provide automatic deployment, orchestration and instantiation of services for the verticals' use cases, providing PPDR-tailored 5G network scenarios.

2.1 Project Network Application approach

The 5G-EPICENTRE approach follows a Network Application definition similar to [1] and [3], essentially as software packages configured to execute NFs, which can be Physical (PNFs, on dedicated hardware), or Virtual (VNFs). Through Service Function Chaining (SFC), network traffic can be directed to flow through one or more NFs, thus, forming more complex End-to-End (E2E) NSs out of NF chains. Network Applications harness these chains to provide vertical-specific or vertical-agnostic applications over the network [1].

The 5G-EPICENTRE project does not only continue with the definitions of Network Applications made so far, but also actively collaborates with the other ICT-41 projects to define common aspects of the delivery model for Network Applications. This collaboration has resulted in a joint ICT-41 projects' white paper, titled "Network Applications: Opening up 5G and beyond networks" [8].

A rather simplified way to understand the Network Application concept is to see it as a software package that understands the structure of links between NFs and NSs, and how they are chained together to form a whole with a greater purpose. These structures, in turn, may contain fully virtualised (VNF) elements (NF), or physical components (PNF), such as technical equipment. All these elements can also be part of a larger whole, *i.e.*, it is envisaged that different Network Applications can be chained together to form more complex structures in a new Network Application.

Furthermore, following a similar approach to the work carried out in other ICT-41 [1] [2] [3] projects, these Network Applications interact with the control plane by consuming the exposed Application Programming Interfaces (APIs), in a standardised and trusted manner to compose services for the vertical industries. So, Network Applications can provide services to vertical applications, either as an integrated part within the vertical application, or by exposing APIs themselves (such as those focused on PPDR solutions), with renewed control capabilities over the mobile network [6]. This means that Network Applications can be classified based on the utility for which they have been designed. So, on one hand, there will be generic solutions, which aim to be interlinked and used by other Network Applications (in a trusted manner). On the other hand, some Network Applications are so specific and so associated with the vertical itself, that they are unlikely to be reused by other services, even though there is a strong dependency of them to be operational.

5G-EPICENTRE has followed a similar approach in this regard to the one implemented in VITAL-5G [2], where these Network Applications are categorised as *vertical-specific* or *vertical-agnostic*. The services offered by the platform to facilitate the immersive process of experimentation, and that will be offered to its users (see D1.4) will be categorised as vertical agnostic.

These vertical-agnostic Network Applications offer 5G Quality of Service (QoS) management solutions, analysis and visualisation of Key Performance Indicators (KPIs), security, *etc*., all of whom are functionalities that the 5G-EPICENTRE platform manages for an adequate experimentation experience. Figure 1 shows how the vertical-specific (VS in Figure 1) Network Applications, can interact with vertical-agnostic (VA) Network Applications, consuming them. The latter will offer extra functionalities to vertical services, improving their experimental process.

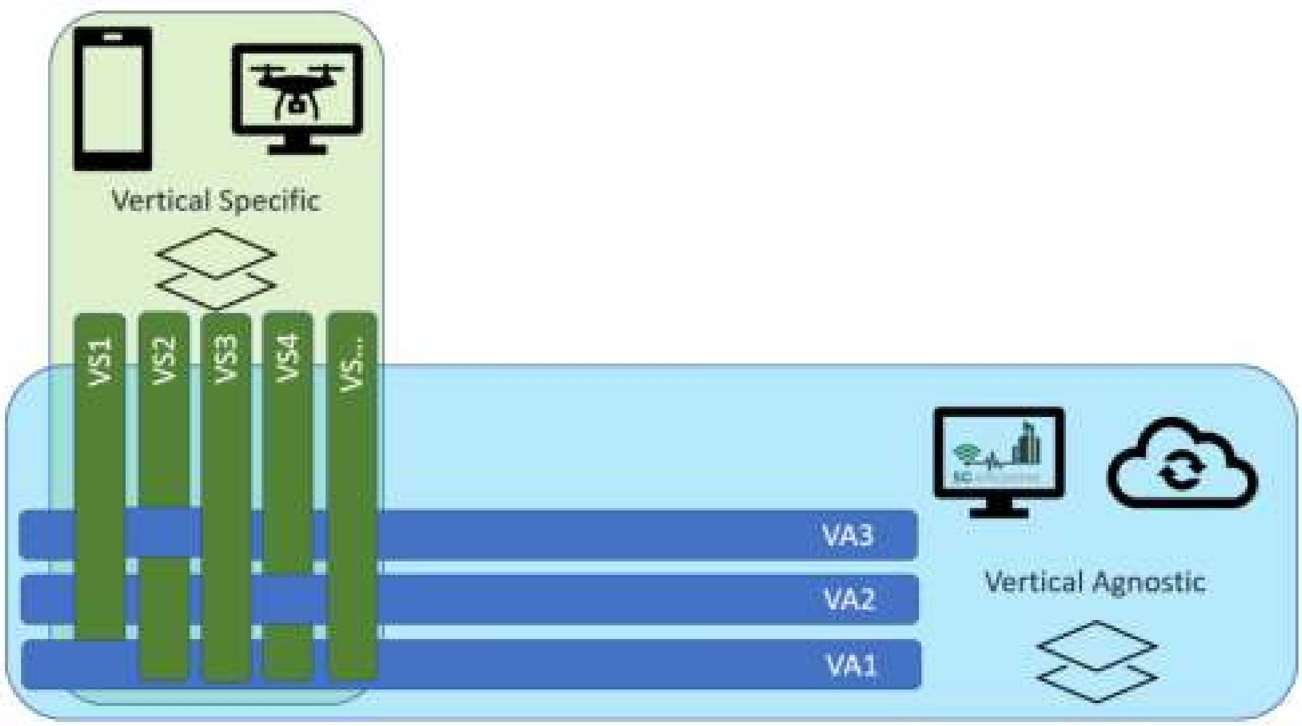


Figure 1: 5G-EPICENTRE Network Application approach

Finally, the vertical-specific Network Applications represent those solutions that, due to their PPDR sector specialisation, can hardly be used by third parties. This has to do with the specific equipment they need, the information they handle, or the level of Intellectual Property Rights (IPR) protection they need. However, their use is of vital importance to the project, as through the implementation of these solutions, the necessary knowledge to build the 5G-EPICENTRE platform has been acquired. Moreover, thanks to the experimentation carried out by these validating Network Applications, 5G scenarios adapted to the PPDR sector's needs will be drafted (see D1.2). In addition, the relationship of these verticals with 5G technology; the interaction between relevant industry players and Consortium members; and the experimentation and interconnection between solutions, have generated Network Applications of great relevance for the PPDR sector. This is the case of QoS control through the N5 interface [10] to guarantee 5G service conditions for critical communications.

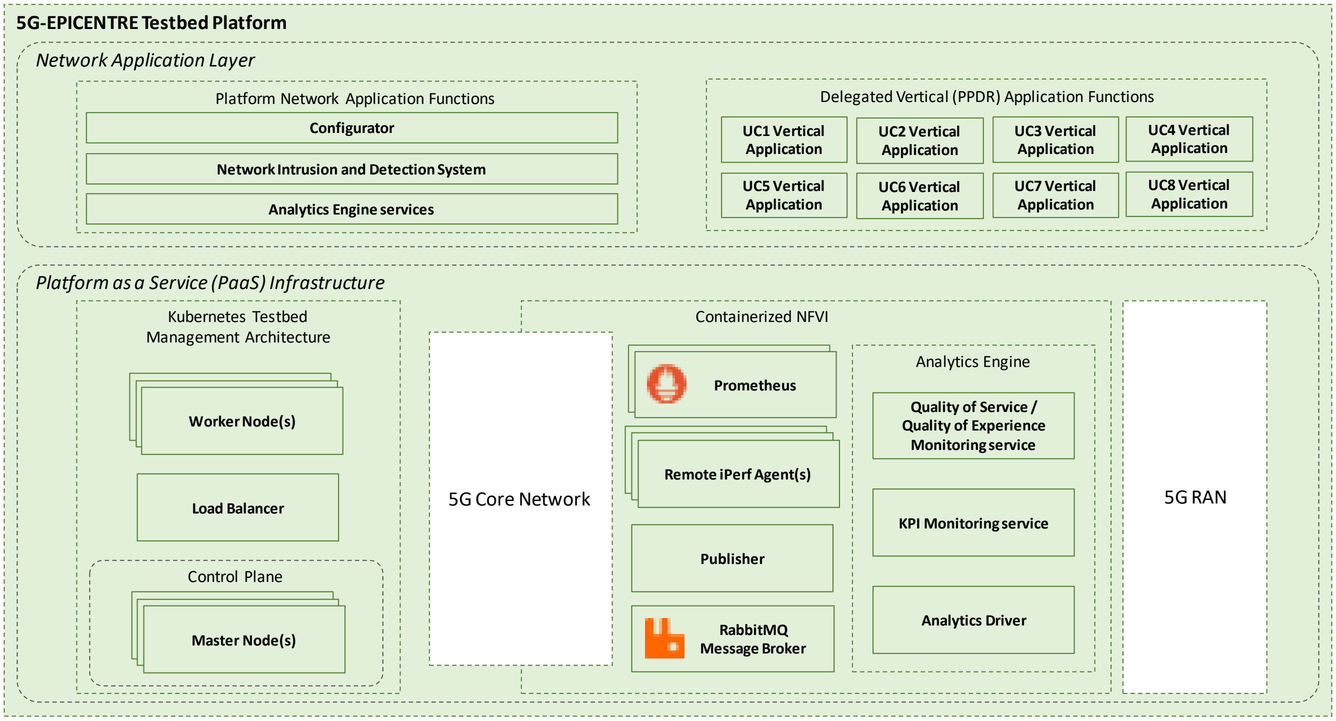


Figure 2: 5G-EPICENTRE Infrastructure Layer reference frame.

D1.4 provided a better explanation of how the Network Applications ecosystem interacts with the 5G-EPICENTRE platform. The following image shows these relationships in a schematic way, providing an overview of this issue.

2.1.1 Network Applications considerations

All Network Applications to be listed in this document follow the definitions in Section 2.1, but, in addition, they can be classified based on other criteria. This section aims to provide a brief explanation of each of the constraints associated with each solution.

2.1.1.1 Deployment models

In the framework of T1.3 "5G-EPICENTRE technical specifications and architecture" the way the different Network Applications may interact with the 5G-EPICENTRE elements has already been considered. Aligning with the common ICT-41 Network Application definition [8], D1.4 provides an overview of where each of the Network Applications is deployed (as-a-service [aaS] Model, Hybrid Deployment or Coupled/Delegated Deployment). It has been preferred to carry out this analysis from an architectural point of view. For the sake of completeness, the options of interaction between vertical application developers and 5G network system (*e.g.*, testbed) owners are re-iterated in Figure 3.

2.1.1.2 Openness

This Section addresses the different ways in which the solutions offered by the project are open for third-party experimentation. Although the objective is to provide the PPDR sector with useful tools for agile access to 5G technology, the way those solutions are provided, and the solution providers' rights have also been considered. In order to accomplish it, 3 different categories have been defined, which are described in Table 2. The need to protect some of these solutions is not only due to the requirements associated with IPR, but it also considers aspects such as the security of the platform, the stability of the solution, or even simplifying the procedure for third-party testers. This is only a first approach to how the 5G-EPICENTRE solution is expected to be used by third-party experimenters. Further details considering partners' IPR will be offered in the scope of D6.8 "IPR strategy and management plan final version". These same options will also be available to third parties, who will be able to determine how open their own delegated Network Apps will be in the repository, using the Portal.

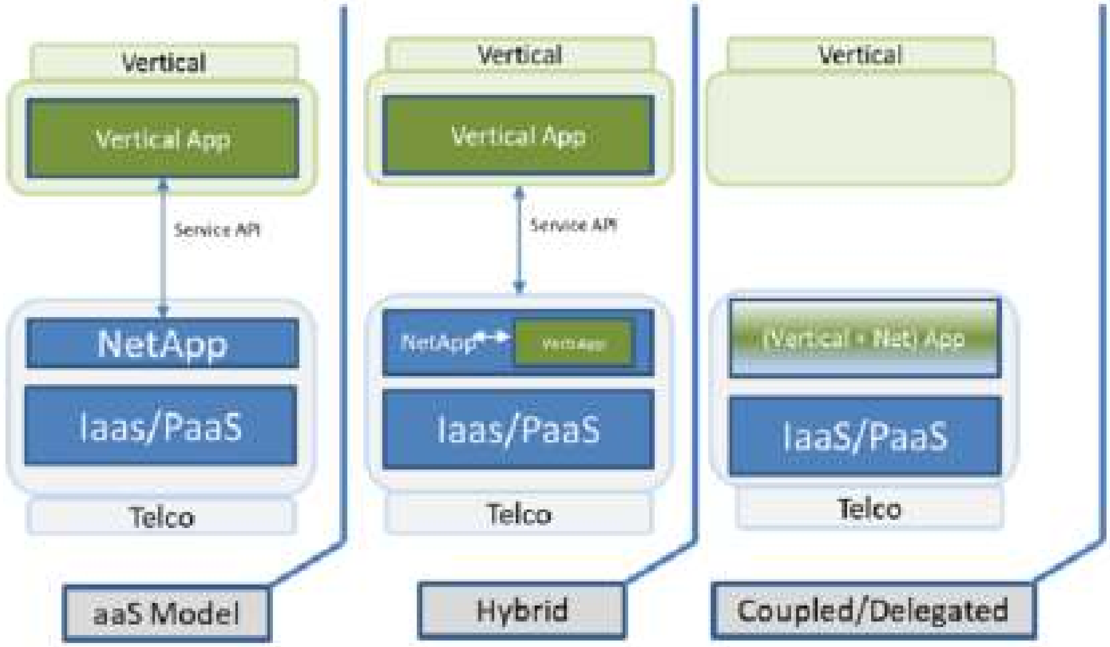


Figure 3: Options of interaction between vertical applications and Network Applications (Image retrieved from [8], licenced under CC BY 4.0).

Table 2: Network Applications' openness criteria

Criteria	Explanation
Totally open	Network Applications will be available for third-party experimentations. The Network Application will be released as open software to be used by the PPDR sector and future projects.
Open	Network Applications will be opened to third-party experimentation but with restrictions. They will be seen as a "black box", in a Helm chart packaging the service, so that they can be used without exposing the IPR of the software to third parties. This way PPDR agencies could have a vision of what PPDR solutions, based on the 5G-EPICENTRE Use Cases (UCs), can achieve over 5G, without project partners exposing their proprietary software. The way in which these Network Applications would be used will be defined in the framework of the project exploitation (in D6.8).
Totally closed	Since certain NFs may need to be excluded from exposure to third parties, this should also be considered. Whether for security reasons, own constraints, or IPR protection, it must be considered that sometimes it will not be possible to enable the use of certain components by third parties.

2.1.1.3 Containerisation level

The experimental solution proposed by 5G-EPICENTRE must consider the different possibilities of containerisation (Table 3). The UCs of this project offer a vision of the different approaches that can be taken by other innovators in the PPDR sector. D1.3 "Experimentation requirements and architecture specification preliminary version" provides more detailed definitions.

Table 3: Network Applications' containerisation level criteria

Criteria	Explanation
Fully Containerised	Solutions that are entirely containerised.
VM with KubeVirt	Solutions that, due to their specific constraints, opt for a Virtual Machine (VM) solution.
Hybrid containerisation	Solutions that, due to their specific constraints, opt for a hybrid solution merging containerised software with a VM approach in a KubeVirt environment.

2.1.1.4 Network Applications storage location

Some of the Network Applications will be stored in the Network Service Repository to be selected (or not, depending on their openness definition). Others, on the other hand, offer their service through the platform itself and need to be deployed in the different layers of the 5G-EPICENTRE solution (Table 4). An overview on how this repository works is offered in D1.4 and will be further detailed in D4.3 "Curated NetApp image repository".

Table 4: Network Applications' storage location criteria

Criteria	Explanation
Repository	Network Applications that are going to be available at the Network Service Repository.
Other	Network Applications that, due to some of their physical components or architectural considerations, are not going to be available at the Network Service Repository.

2.2 Network Application management

Although this Section will be further elaborated in D4.3, it gives an idea of how these Network Applications will be treated. The repository will store the different Network Applications and VNFs for their use when they are called. It will also store all necessary image files and descriptions. The information will be stored; and access to it will be managed by means of Role-Based Access Control (RBAC), to protect the IPR of solutions that require it. Due to the physical nature of some of the NFs that make up the Network Applications, it will not be possible to include them in the repository. These will be managed by the platform itself (by selecting a specific testbed, for example), or will be included within a larger Network Application, which will parameterise and manage them.

2.3 Network Application summary

Following the criteria and the approach explained in Section 2.1, Table 5 and Table 6 offer a brief but complete overview of the Network Applications developed in 5G-EPICENTRE's framework.

Table 5: Vertical-agnostic Network Application

Network Application ID	Network Application Name	Containerisation level	Storage location	Openness	Status
VA1	Analytics Services Network Application	Fully containerised	Shared between Testbed layer and Frontend layer	Open	Advanced status
VA2	Network Intrusion Detection Network Application	Fully containerised	Testbed layer's Docker cluster	Open	Advanced status
VA3	Configurator Network Application	Fully containerised	Frontend layer	Open	Getting started

Table 6: Vertical-specific Network Application & NS

Network Application ID	Network Application Name	Containerisation level	Storage location	Openness	Status
VS1.1	Push To Talk Critical Communication (MCPTT) Network Application	Fully containerised	Repository	Open	Ready
VS1.2	Video Critical Communication (MCVideo) Network Application	Fully containerised	Repository	Open	Ready
VS1.3	Data Critical Communication (MCData) Network Application	Fully containerised	Repository	Open	Ready
VS2.1	Full Mission Critical Services (MCX) Server Network Application	Fully containerised	Repository	Open	Ready
VS2.2	MCX Dispatcher Network Application	Full containerised	Repository	Open	Ready
VS2.3	MCX QoS management NS	Full containerised	Repository	Open	Ready

VS3.1	Network Applications and Services for ultra-reliable drone navigation and remote control	Full containerised	Repository	Closed	Getting Started
VS3.2	Video splitting NS	Full containerised	Repository	Closed	Getting Started
VS4	Network Applications and Services for internet of Things (IoT) for improving first responders' situational awareness and safety	Full containerised	Repository	Open	Ready
VS5	Network Applications and Services for wearable, mobile, point-of-view, wireless video service delivery	Full containerised	Repository	Closed	Advanced status
VS6.1	AI-Analyzer Network Application	Containerised	Repository	Open	On beta testing
VS6.2	Proxy NS	Containerised	Repository	Open	On beta testing
VS6.3	Dummy-Image-Sender NS	Containerised	Repository	Open	On beta testing
VS7	Network Applications and Services for augmented Reality (AR) and Artificial Intelligence (AI) wearable electronics for PPDR	Full containerised	Repository	Closed	On beta testing
VS8	Network Applications and Services for AR-assisted emergency surgical care	VM Based	Repository	Closed	On beta testing

3 Vertical-agnostic Network Applications

Following the definitions made in [1] [3], and the overall approach to Network Applications followed in other ICT 41 projects [2] [8], those Network Applications that (due to their level of abstraction) can be used by any vertical, have been identified as **vertical-agnostic (VA)**. This means that they are Network Applications that, due to their general purposes, can be consumed with other vertical Network Applications, which are more specific, and end-user driven. Therefore, the Network Applications that have been considered as agnostic, are those that offer solutions to the general needs of the 5G-EPICENTRE experimental platform, following a similar approach to [1].

On the other hand, the cloud native architecture on which the 5G-EPICENTRE project is based, means that some elements are containerised, or can interact in a containerised environment [9]. Although they should continue to be considered as a fundamental part of the 5G-EPICENTRE platform architecture (see D1.4), in some cases, it is true that, because of the way they interact with vertical services, they could also be considered as an extra Network Application that is consumed to add value to the entire E2E chain.

The following subsections show some of the VA Network Applications identified.

3.1 VA1: Analytic Services Network Application

The 5G-EPICENTRE platform includes an Analytics Engine (AE), able to analyse experimental data coming from the 5G network and the vertical services; providing KPI statistical post-processing when needed; statistical analysis; and more advanced functionalities, based on Artificial Intelligence (AI), such as anomaly detection and KPI prediction, in near real time. Those data will be then used by the 5G-EPICENTRE Portal's Visualisation Tools, to present experimentation results in a visually attractive way. Further architectural analysis of this component is offered in D1.4, whereas its full description will be delivered with D2.6.

The operation of this module is largely based on the experimental definitions made in D1.6, in the message structure defined in D4.1. However, during the project, occasions have been identified where verticals require a certain degree of measurement customisation. The Analytic Services Network Application should offer a way for verticals to interact, where they can provide details of their experimental data structure, for example.

For this reason, a simple API has been envisioned, which gives access to the verticals to interact directly with some of the elements of the AE, thus creating a Network Application. This Analytic Services Network Application chains some of AE's NSs, so to be consumed by the vertical.

As can be seen in Figure 4, the QoS/Quality of Experience (QoE) Monitor would be left out of the selected NS, since this component requires a high amount of data to be trained, and given the exceptional nature for which the Network Application has been conceived, will not be useful for the vertical. In order to provide AI functionalities (such as Anomaly Detection and KPI prediction), the AE needs to collect a significant amount of data to be analysed for the selection of the most suitable Machine Learning (ML) technology; and used for the training of ML models. This type of implementation has been left out of the conceptualisation of this Network Application.

The Analytic Services Network Application is composed of different NSs. The KPI Monitor and the Analytics Driver would be set at the Testbed Level (Infrastructure Layer), and would work together to perform data-intensive operations. The Analytics Aggregator NS would be deployed at the platform level (Backend Layer). The Analytic Services Network Application uses containerised solutions compatible with Kubernetes-based deployments. Currently, the module has the following dependencies:

- **Data gathering.** Access to the RabbitMQ instance provided by the Testbeds where measurements from the UCs and the infrastructure are published (by the Publisher module).

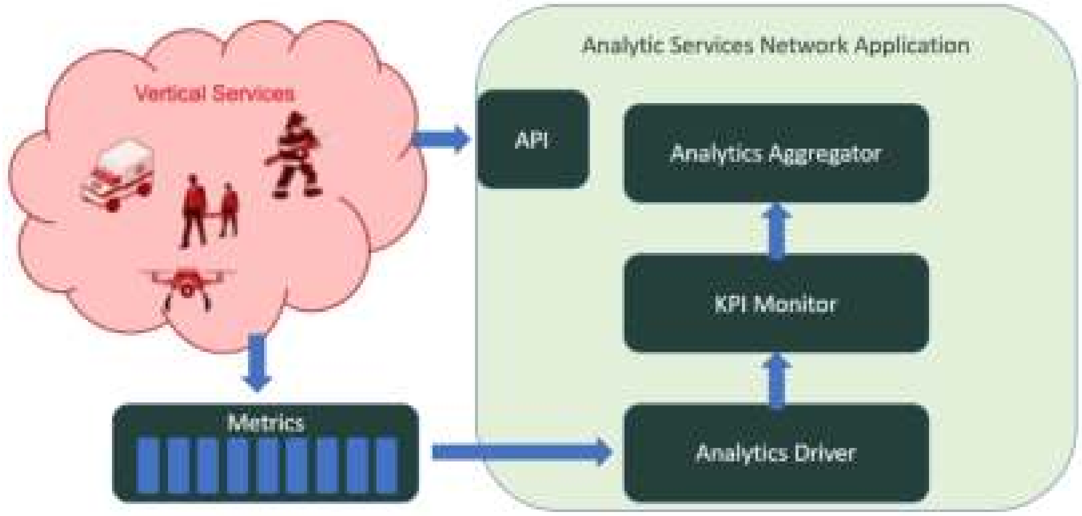


Figure 4: Analytic Services Network Application

- **Storage.** The AE needs an external InfluxDB instance (provided by the Testbed) to guarantee persistence of critical data (the measurements gathered from infrastructure/UC) and retrieve them for data analytics tasks.

A list of the different services composing the Analytic Services Network Application is provided below:

- **Analytics Driver:** the NS responsible for collecting information in the form of input data from the Testbed Layer (*e.g.*, metrics related to 5G networks and vertical services); and for pre-processing the data, in order to forward them to the other AE NSs for KPIs calculation.
- **KPI Monitor:** responsible for computing experiment KPIs (when needed), using data provided by the Analytics Driver; and forwarding output KPI values to the Analytics Aggregator NS.
- **Analytics Aggregator:** will receive input data from the internal Analytics Engine NS at each individual testbed; aggregate the information; and propagate it to the visualisation components residing in the Frontend layer.
- **Analytic Services Network Application API:** The vertical would subscribe through the API to avoid any undesired interaction with the data stored (to make sure that only trusted verticals will access their own experimental data); and request for specific data management, such as statistical analysis over pre-determined intervals.

The project effort is currently focused on creating an interface, a RESTful API that will enable this functionality. Different UCs will be able to make use of this functionality, which allows a certain degree of adjustment by the vertical on the display of the experimental data. Because of its relationship with 5G-EPICENTRE's Network Application approach, this particular effort will be followed up in the framework of T4.2, whereas the component itself is done in T2.5 "ML-driven experimentation analytics".

3.2 VA2: Network Intrusion Detection Network Application

When experimenting on the platform, it is necessary to be able to guarantee security, both for the vertical users and for the testbeds and the platform itself. To this end, a new Network Application has been developed, that identifies possible threats; evaluates them; and acts accordingly, by blocking them to prevent any type of malicious software in the E2E chain.

The reference architecture of the Holistic Security and Privacy Framework (HSPF) is depicted in Figure 5. This framework was, initially presented in D2.1 "Cloud-native security", where the detailed 5G-EPICENTRE approach

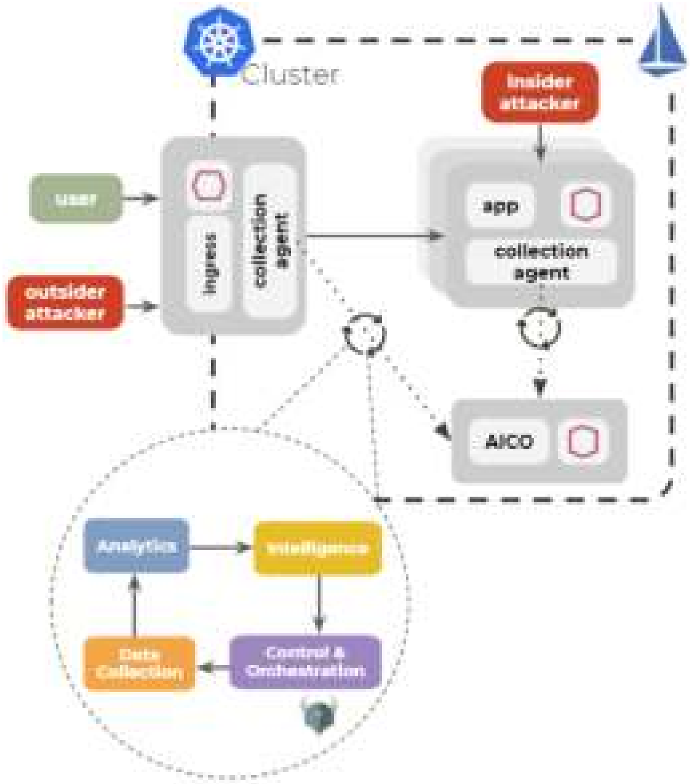


Figure 5: Holistic Security and Privacy Framework (HSPF) (retrieved from D2.1)

to the platform security is shown as part of the work in T2.6 “Attack surface decrease and network edge access control”.

The HSPF is currently evolving into a Network Intrusion and Detection System (NIDS), which can be exposed to vertical experimenters to detect traffic anomalies related to security incidents. It can also trigger security policies. The solution currently integrates with the project UC4 only, but it is planned to secure against any vertical Network Application (even third parties).

To this end, the next steps of the project will focus on exposing an API to the vertical application component in the vertical service domain, allowing it to consume this Network Application, gathering security intelligence from the network so the vertical can react to any event detected (*e.g.*, if anomalous traffic is detected, the vertical might want to terminate a stream).

The deployment of this Network Application assumes a Kubernetes environment with Istio's implementation of the Service Mesh. The injection of collection-agents during run-time is allowed by Kubernetes, thus enabling the possibility of deploying this framework next to an already executing Network Application, without disrupting its normal behaviour.

The NIDS is composed of two major NSs: the *collection agents* and the *Analytics, Intelligence, Control and Orchestration (AICO)* component, both of which arecompletely containerised.

Each collection agent corresponds to a sidecar proxy that is automatically deployed next to each application micro-service, with the objective of collecting the incoming and outgoing traffic. Afterwards, it forwards that traffic to the AICO component, that is responsible for pre-processing the incoming data, classifying it and applying security policies every time a threat is detected.

3.3 VA3: Configurator Network Application

5G has been conceived to allow verticals to interact more naturally with the network's control plane. According to 3GPP standards [11] [12], Network Applications can act on the control plane of the 5G Core (5GC) as (or via) Application Functions (AFs). As such, via the corresponding 3GPP interfaces, and through the Network Exposure Function (NEF), Network Applications can i) influence traffic policies and routing decisions; ii) remotely trigger specific user equipment (UE) actions; iii) request the execution of services provided by the Location Management Function (LMF); or iv) gather from, and share with the network, any kind of data and analytics via the Network Data Analytics Function (NWDAF).

In the framework of 5G-EPICENTRE and with ADS, ONE and NEM as technology validators, a demonstration of QoS management leveraging 5G functionalities has been achieved. This has been possible thanks to the interaction with ATH's 5GC, and UMA's Radio Access Network (RAN) [13]. This project achievement provides a value chain to secure network conditions for the most demanding vertical services, such as those associated with the PPDR sector. It offers a way to allocate specific resources to those verticals identified as PPDR.

Figure 6 shows the state of the work so far. The vertical AF identifies itself as a PPDR service provider, and requests a specific QoS for media flows. The 5GC manages the request, checks its origin and legitimacy, allocates the new QoS to the vertical service, and propagates it to the rest of the 5G network elements. It takes advantage of the verticality with which 5G networks were conceptualised, to address the controlled interaction of PPDR-related Network Applications. Through the protocols established for the Policy Control Function (PCF), the Network Applications are identified as a PPDR solution, and its QoS assurance request is accepted. This resource allocation is propagated to the rest of the 5G network elements, to guarantee the assigned service throughout the E2E chain. It prioritises and guarantees service to 5G network's PPDR users, enabling the use of specific slices, or specific configuration within the same slice. This effort demonstrates that it is possible to deliver all the benefits that the 5G network can bring to the PPDR sector in a secure and stable manner.

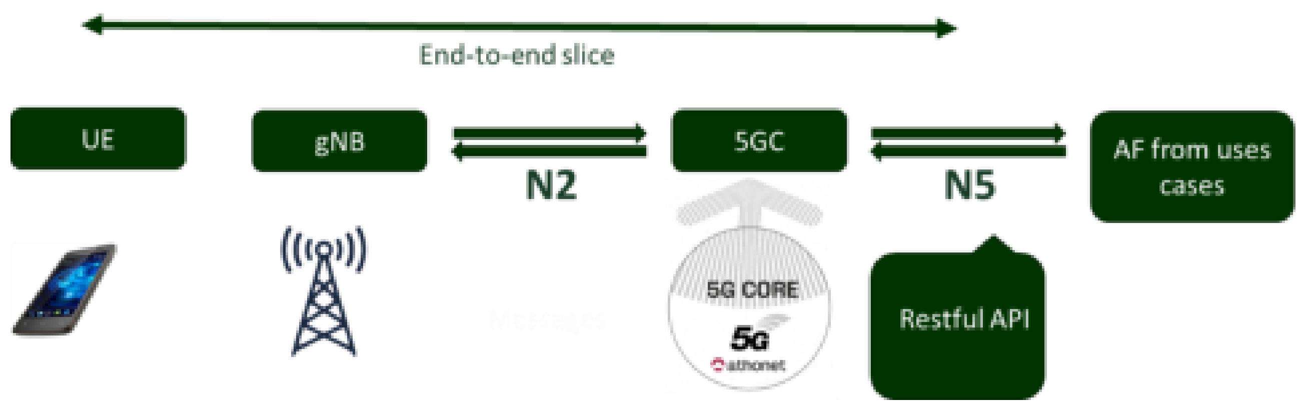


Figure 6: QoS Management Network Application

The project effort is currently focused on creating an interface, a RESTful API that will enable this functionality to less experienced verticals with 5G standards, facilitating their access to this functionality. UMA is exploring with ATH the exposure of the 5GC, through RESTful APIs, to set up a specific slice that will ensure the resources of PPDR applications in high-traffic load conditions. This API will be exposed at the N5 interface and the UC's AFs would be able to request the usage of a specific slice that will be configured in the network for its usage by PPDR applications. The network function that will expose this API is the PCF component of the 5GC. This initiative is aligned with the work carried out in D1.2, where the creation of a specific 5G experimentation scenario is framed in UMA's facilities, enabling the research on slicing and QoS management.

On the other hand, EBOS will be the partner in charge of re-purposing the previous Northbound API into this general-purpose Network Application, considering on one hand the experimental conclusions obtained from this trial (in which the synergies between ADS, UMA, ONE, NEM and ATH had a successful outcome [13]), and on the other hand the definitions related to the N5 and QoS management set in [10] and [14]. Although this work is framed in T3.1 “Northbound API information models and implementations”, which is responsible for exposing a User Interface (UI) to vertical third parties, given its relation to the 5G-EPICENTRE approach to Network Applications, has been considered in D4.2. This API would simplify access to QoS management for third parties, obviating the need for standard knowledge.

4 Vertical-specific Network Applications

In order to validate the 5G-EPICENTRE experimentation platform, 8 different vertical systems, developed by project partners (first-party experimenters) have been considered, all of which are linked to the PPDR sector. Thanks to this, it has been possible to identify the needs of the sector, as the 8 UCs offer a heterogeneous vision of the different possible approaches to PPDR over 5G integration. In general, each UC is considered as a vertical system, which showcases an end-to-end solution over 5G, to help demonstrate to the PPDR end users what 5G can do for them. The vertical system has a vertical application component, *e.g.*, a front-end on a smartphone, that is deployed in the vertical domain (see Figure 2: 5G-EPICENTRE Infrastructure Layer reference frame.), and one or more network application components, that provide the services needed, and abstract the 5G network below in simple API calls.

In this Section we define the integration model of these **vertical-specific (VS)** Network Applications in the 5G-EPICENTRE platform, provide a basic overview of their decomposition into NFs, and show the adopted solution for linking these NFs with the 5G layers. These Network Applications will be chained with the VA layers defined in Section 3, creating E2E chains of Network Applications for the experimentation of PPDR services in 5G conditions. This Section aims to offer an overview of the VS Network Applications from an integration and decomposition point of view. In some cases, and depending on the vertical, the depth with which each NS is detailed is limited. Furthermore, it is also desirable to avoid the disclosure of sensitive information related to UC owners' architecture and IPR, given the public nature of this deliverable.

The project focuses on cloud-native architecture, and the effort made by the verticals in adopting solutions based on microservices, easy and quick to implement, has been valued. However, in order to offer a useful platform for all types of PPDR solutions, UCs where the solution is not fully (or not at all) containerised have also been considered. The 8 UCs below provide the necessary heterogeneous view to create an attractive platform for all types of PPDR solutions, including fully containerised solutions; VM-based solutions (to be deployed via KubeVirt, as detailed in D1.3); and hybrid solutions.

4.1 VS1: Network Applications and Services for UC1

UC1 deploys all its MCX solution specifically configured for MCPTT (VS1.1), MCVideo (VS1.2) and MCData (VS1.3). This section provides an overview of this MCX solution.

The critical communications platform follows cloud-native design principles, allowing exploitation and experimentation of 5G modern features (NFV, slicing, Multi-Access Edge Computing). It is composed of several loosely coupled and stateless micro services, that can work together or independently, and that constitute light Containerized Network Function (CNF) workloads. This backend is completed by a client vertical application (considering the deployment options, this is the part of the UC that goes to the vertical domain, whereas the rest is delegated – Hybrid model), that can run on android smartphones. There is no restriction or dependency. The system can be deployed on any container runtime engine, or leverage modern orchestration frameworks, like Kubernetes. The Network Application is lightweight. Below are the recommendations relative to the system:

- 1vCPU and 1GB RAM.
- Bandwidth Rx: Around 500kpbs per video stream and per user for SD stream 15fps / Around 5Mpbs per video stream and per user for FHD stream 30fps.
- Bandwidth Tx: Around 500kpbs per video stream for SD stream 15fps / Around 5Mpbs per video stream for FHD stream 30fps.
- The application includes a KPI server recording real time media performance audio/video, that shall be addressed by REST API.

The Network Application does not include a cartography server, and needs to be connected to the Internet to load background maps (nonetheless, a cache can be exploited). It is fully interoperable with diverse protocols allowing to enrol diverse devices in the system (including those of third parties). In that case, the servers must be reachable from outside the private network. The Network Application presents external interfaces, thus allowing third party vertical applications to be built on top of it. In that case, for example in the framework of the third-party experimentation.

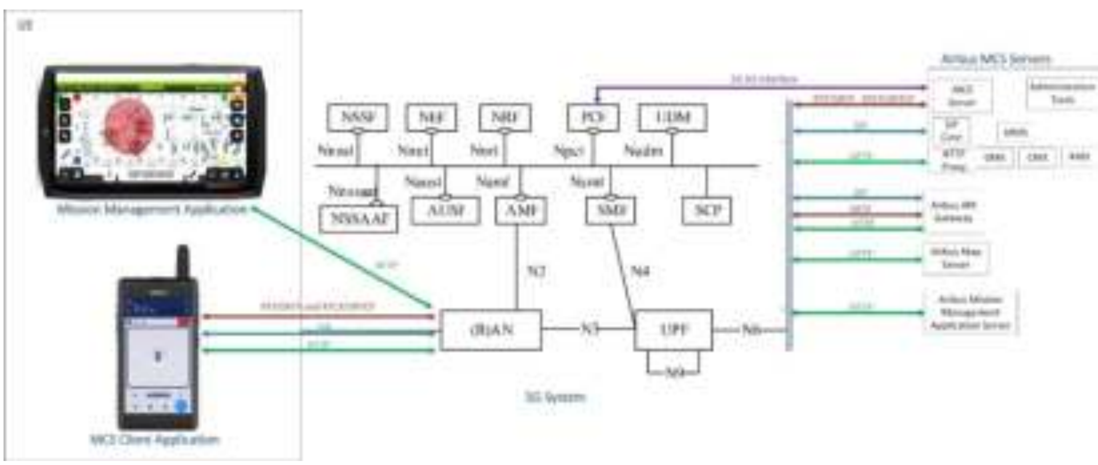
Finally, ADS media microservices can work with mixed protocols, Transmission Control Protocol (TCP) and User Datagram Protocol (UDP), potentially increasing performance and QoE (not mandatory). In order to exploit this on Kubernetes infrastructure, the feature gate MixedProtocolLBService must be enabled.

Here is the description of the various microservices of the UC1 critical communication platform:

- ***Identity Management Function (IdMF):*** is responsible for authenticating an MCPTT client in the system. For testing purposes, the server can accept any new registration.
- ***Situation Management Function (SMF):*** is responsible for managing the situation information: status, locations, *etc.*
- ***Audio Signalisation Function (ASF):*** handles floor control for audio communications.
- ***Audio Media Function (AMF):*** handles real-time packets for audio communications.
- ***Video Signalisation Function (VSF):*** handles control for video communications.
- ***Video Media Function (VMF):*** handles real-time packets for video communications.
- ***Data Management Function (DMF):*** handles non real-time data streams.
- ***KPI Function (KPIF):*** Records KPI related to communications.

The vertical application used to demonstrate the Network Application composed of the above services is a Web-front Server (WFS), *e.g.,* Web User Interface (UI) for client.

Figure 7[1] presents the UC1 vertical system's specific architecture. Table 7 shows the vertical solutions decomposed in NSs, identifying the interfaces between them, and providing a brief description for each one.



[1] The abbreviations shown in Figure 7 are explained below and are also included in the list of abbreviations.

- AMF: Access and Mobility Management Function
- AUSF: Authentication Server Function
- CMS: Configuration Management Server
- GMS: Group Management Server
- KMS: Key Management Server
- NEF: Network Exposure Function
- NRF: Network Repository Function
- NSSAAF: Network Slice-Specific Authentication and Authorization Function
- NSSF: Network Slicing Selection Function
- PCF: Point Control Function
- RAN: Radio Access Network
- SCP: Secure Copy Protocol
- SIP: Session Initiation Protocol
- SMF: Situation Management Function
- UPF: User Plane Function

Figure 7: UC1 vertical system under test - specific architecture

Table 7: UC1 NSs and interfaces

Source Network Service	Interface	Destination Network Service	Comments
MCX Server	3GPP N5	5G Core	5G QoS Management
Mission Management Application	HTTPS	Mission Management Application Server (AS)	Application protocol and data
MCX Client Application	HTTPS	HTTP Proxy	Common Services
Airbus API Gateway	HTTPS	HTTP Proxy	Common Services
MCX Client Application	Real-Time Transport Protocol (RTP)/Secure RTP (SRTP) - Real-Time Transport Control Protocol (RTCP)/Secure RTCP (SRTCP)	MCX Server	Floor control and media transport
MCX Client Application	HTTPS	Airbus Map Server	Map data
Airbus API Gateway	SRTP	MCX Server	Media transport
MCX Client Application	SIP	SIP Core	Registration, Subscription, Affiliation and Session Management
Airbus API Gateway	SIP	SIP Core	Session Management

4.2 VS2: Network Applications and Services for UC2

The solution proposed by NEM consists of 2 Network Applications, *Full MCX Server Network Application* (VS2.1) and *MCX Dispatcher Network Application* (VS2.2). Additionally, a new MCX QoS management NS (VS2.3) has been developed, which will be chained together with MCX Server Network Application to enable QoS management (it would be usable for third-party experimenters, but only through the MCX Server Network Application, hence the need for a more generic solution in VA3). While the MCX Server Network Application encompasses the main elements for MCX (MCPTT, MCVideo and MCData [15] [16] [17]), such as Key Management Server

(KMS), Configuration Management Server (CMS), *etc.*, the MCX Dispatcher Network Application offers a way to create and provision campaigns, workgroups, *etc*.

NEM's MCX solution is entirely based on Kubernetes. The service can be deployed using Helm, a package manager for Kubernetes. It helps to deploy applications reading the templates, deploying the services accordingly. If the cluster environment does not support Helm, it can be used from an external machine pointing out to the cluster.

Currently, the MCX deployment has the following dependencies:

- Network: Container Network Interface (CNI) (any should work).
- Storage: Container Storage Interface (CSI) (any should work).
- Seamless monitoring: Kubernetes Prometheus operator is required. External access to services, which can be configured to use LoadBalancer or NodePort. The system is by default configured to use LoadBalancer:
    - If LoadBalancer is to be used, the cluster where the services are deployed must have a LoadBalancer instance. So far, metalLB has been chosen.
    - If NodePort is to be used, it does not have any requirement.
- RTPengine requires to be able to deploy it in hostnetwork mode.
- Deploying tool: Helm is required. It is not necessary to use Helm on the host machine. Helm can be used in a remote machine pointing out to the host machine.

A summary of the different microservices (NFs) and NSs is given below:

- **MCX AS:** It is responsible for providing control and management of communications (MCPTT-voice-, MCVideo-video- and MCData-data-). The MCX AS could be divided in two main roles in the system:
    - The ***MCX Controlling Application Server (CAS):*** It handles the floor control for both private and group calls, and it forwards media flow as well. Besides the MCX Participating Application Server, the MCX CAS could also communicate with other CAS or non-Controlling AS(s).
    - The ***MCX Participating Application Server (PAS):*** It handles the communication with the MCX clients, and plays the role of a relay point for floor control between the MCX clients and the MCX CAS. It also manages access and priority control of users to the communication in place; and access control to MCX clients triggering communications (checking the capabilities of each).
- **Identity Management Server (IdMS):** It is responsible for authenticating an MCPTT client in the system. The server is provisioned with the client ID, MCPTT ID and password.
- **Configuration Management Server (CMS):** It is responsible for managing the MCPTT/MCX configurations, such as user profile, UE configuration, functional aliases and service configurations.
- **Group Management Server (GMS):** It is responsible for managing the groups' information. The groups could be either formed by clients/users, or other groups (group regroup).
- **Key Management Server (KMS):** It is responsible for the distribution and storage of security keys and information like encryption keys for the communication of MCPTT calls (private and group); Short Data Service (SDS) data protection; management server safe; and integrity-based communication (both signalling and media).
- **Session Initiation Protocol (SIP)/IP Multimedia Subsystem (IMS) Core:** provides the SIP core required as a SIP register and message forwarding framework. This SIP core comprises different elements: Proxy Call Session Control Function (P-CSCF); Interrogating CSCF (I-CSCF); Serving CSCF (S-CSCF); and Home Subscriber Sever (HSS).
- **Backend + Enabler:** It manages sessions between server and end users, and implements different interfaces and translation for non-MCPTT systems with MCPTT devices.
- **Non-relational database (DB):** It is used to store dynamic information, like registered users.
- **DB:** SQL DB used to store micro-service configuration information.

- **Enabler-WS:** Backend used by Dispatcher.
- **HTTP-Proxy:** middleware of external HTTP traffic, that inspects HTTP traffics redirecting it to the corresponding micro-service.
- **MCPTT-Exporter:** module that exports monitoring information according the monitoring process instantiated (RabbitMQ or Prometheus).

Figure 8[2] presents the UC2 vertical system's specific architecture. Table 8 shows the vertical solutions decomposed in NSs, identifying the interfaces between them, and providing a brief description of each one.

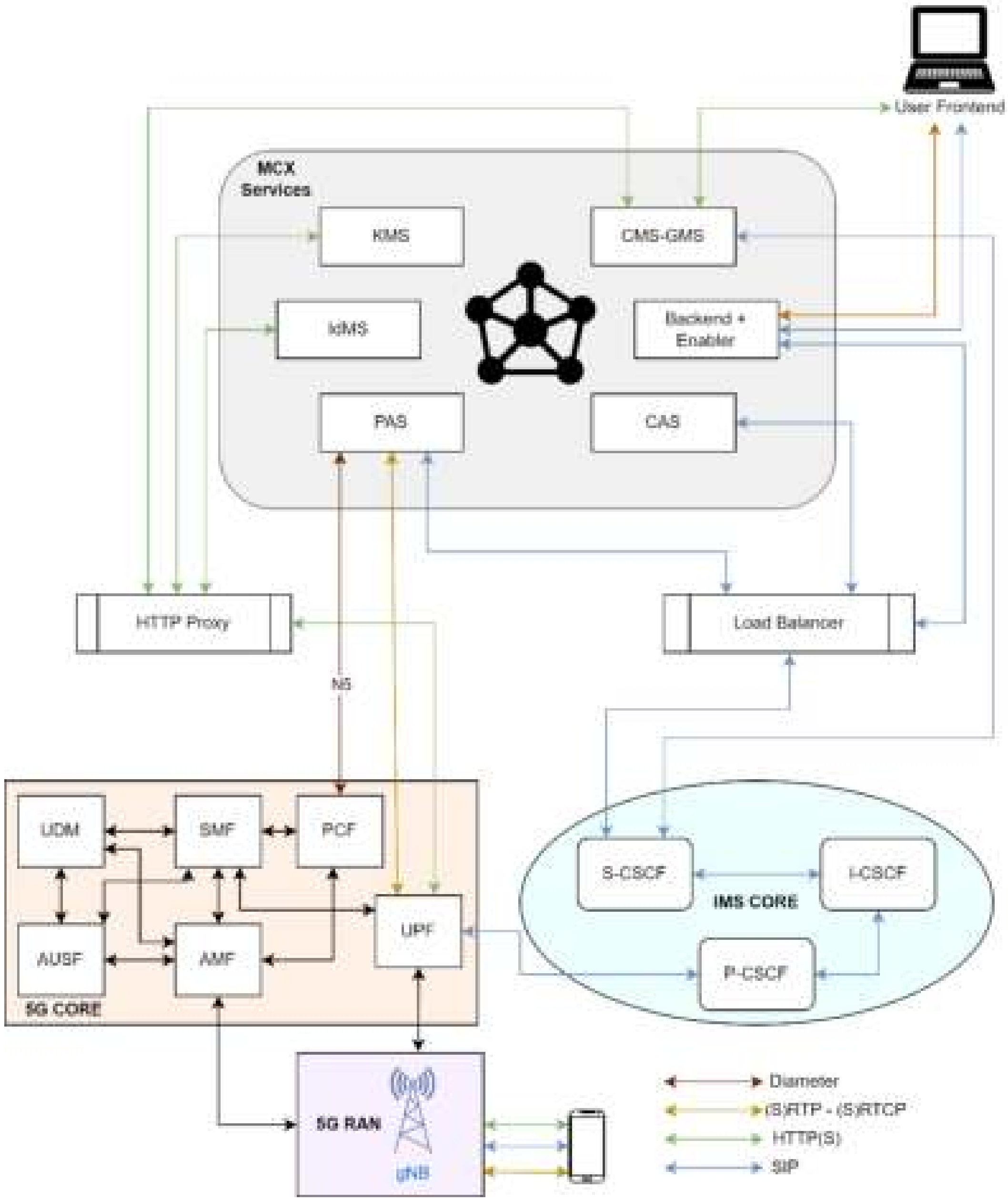


Figure 8: UC2 vertical system under test - specific architecture

[2] The abbreviations that are included in Figure 8 and have not been defined earlier in the document are the following:

- UDM: Unified Data Management

Table 8: UC2 NSs and interfaces

Source Network Service	Interface	Destination Network Service	Comments
PAS	Diameter (N5, MB2C/U)	5GC PCF	Diameter traffic used to signal QoS reservations and multicast sessions
PAS	RTP	5G CORE UPF	Ongoing calls from UE
PAS	SIP	SIP Load Balancer	SIP Traffic from IMS or Enabler arrives via SIP Load Balancer
CAS	SIP	SIP Load Balancer	Initial SIP traffic to PAS or Enabler
Backend + Enabler	SIP, RTP	User Frontend	
CMS - GMS	SIP	IMS CORE	External SIP Traffic
CMS - GMS	HTTP	HTTP Proxy	External HTTP traffic
IdMS	HTTP	HTTP Proxy	External traffic UE
KMS	HTTP	HTTP Proxy	External traffic
SIP Load Balancer	SIP	IMS CORE	
SIP Load Balancer	SIP	CAS, PAS, Backend + Enabler	
HTTP Proxy	HTTP	5GC UPF	
HTTP Proxy	HTTP	KMS, IdMS, CMS-GMS, Backend + Enabler	
5GC	Diameter (N5, MB2C/U)	PAS	
5GC	RTP	PAS	
5GC	HTTP	HTTP Proxy	
5GC	SIP	SIP Load Balancer	
5GC	HTTP, SIP, RTP	5G RAN	
5GC	-	5G RAN (AMF)	Control plane

5G RAN	HTTP, RTP, SIP	5G CORE	
5G RAN	HTTP, RTP, SIP	UE	
5G RAN	-	5G CORE	Control plane
IMS CORE	SIP	Load Balancer	
IMS CORE	SIP	5G CORE UPF	

4.3 VS3: Network Applications and Services for UC3

UC3 follows hybrid model where following NS are utilized:

- MAVLink Proxy (Micro Air Vehicle communication protocol).
- CC Link for the Command/Mission Control Centre.
- Live Video Server for the management of the video streams of the drone.

QGroundControl consumes the above mentioned network services and henceforth act as a network application for the use case and is utilized as a mission control operator. Additional clients of QGroundControl in the vertical domain can be installed which will receive the drone feeding from live video server deployed as NS. It is planned to containerise the Network Application along with its NSs under Kubernetes. To use the Vertical Applications, the following configuration is required:

- 1 VM with 1 CPU, 8GB RAM and 30GB hard disk.
- Bandwidth Uplink (UL) (drone to live video server): Approximately 20Mpbs per video stream.

In addition, a dedicated NS will be created, to measure latency and data rate in the context of the UC. This requires a Kubernetes environment that includes:

- Kubernetes Master + 2 Worker Nodes.
- VPN access.
- CNI (Flannel).
- Message Queuing Telemetry Transport (MQTT) message broker.
- LoadBalancer (metalLB).

A VM will be deployed, in which all the NSs with QGroundControl will be installed. Through this, one cannot only control the drone, but can also stream the live video either in telco domain or in client domain from drone. As a prerequisite, the VM must be connected to the 5GC in order to communicate with the drone over 5G.

In the VS3.1 Network Application, a new VS3.2 NS has been considered, which provides the provision of splitting the video from the drone, not only to the different clients (such as 5G phones), which are connected to the testbed, but also to other UCs, which are being deployed in the same AS. This additional functionality motivates the synergies between different UCs which are being deployed in the HHI testbed. As an example, the video stream can be directed to UC7, which utilises smart glasses.

Figure 9[3] shows UC3 vertical system's specific architecture. Table 9 shows the vertical solutions decomposed in NSs, identifying the interfaces between them, and providing a brief description of each one.

[3] The abbreviations that are included in Figure 9 and do not appear earlier in the document are the following ones:

- DHCP: Dynamic Host Configuration Protocol

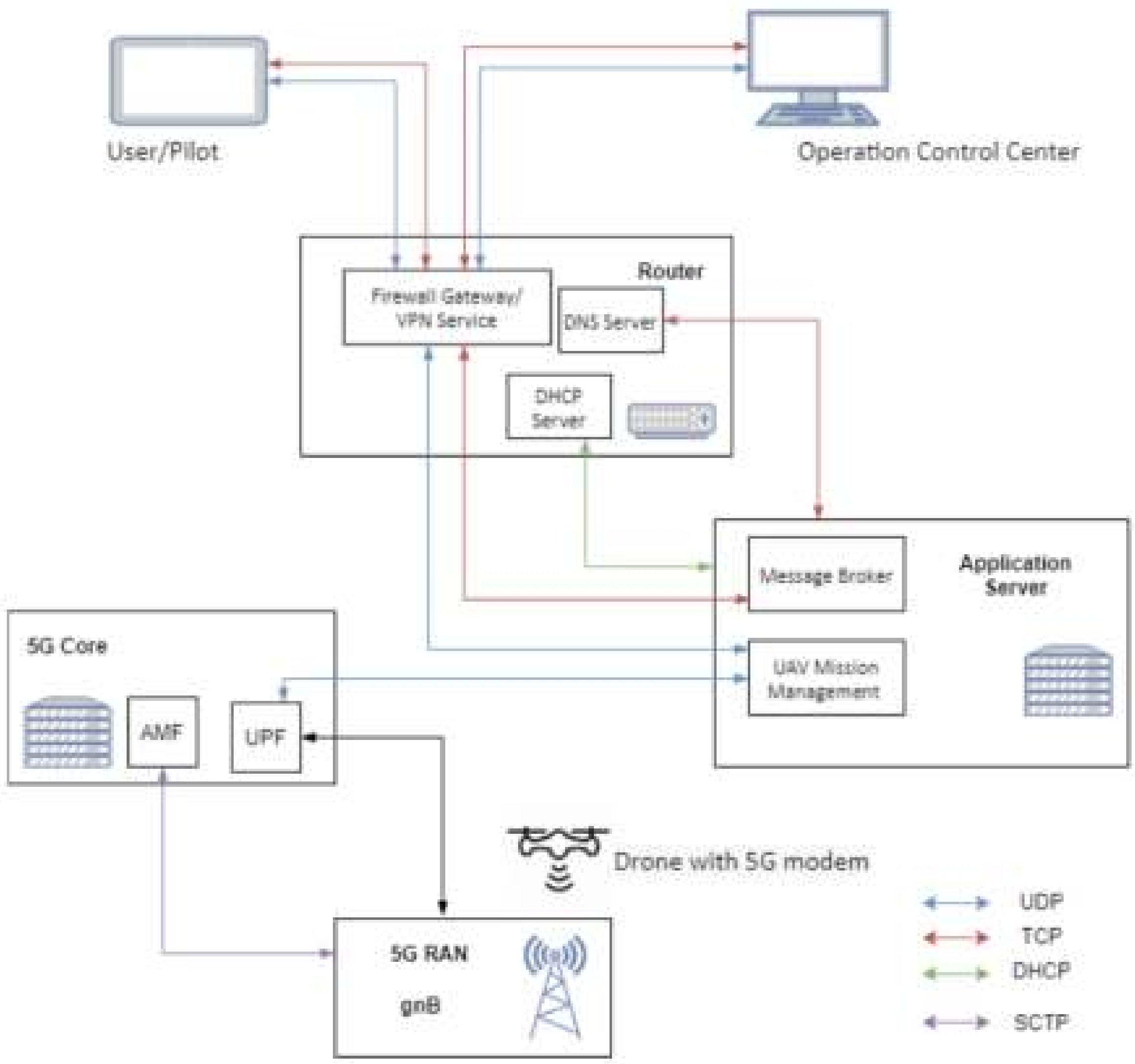


Figure 9: UC3 vertical system under test - specific architecture

Table 9: UC3 NSs and interfaces

Source Network Service	Interface	Destination Network Service	Comments
5GC	UDP	5G RAN	User plane
5GC	Stream Control Transmission Protocol (SCTP)	5G RAN (AMF)	Control plane
5G RAN	UDP	Drone	
DNS Server	TCP/UDP	AS/Internet	

- DNS: Domain Name System
- SCTP: Stream Control Transmission Protocol

AS/ UAV Mission Management Server	UDP	5GC (UPF)	
Dynamic Host Configuration Protocol (DHCP) Server	DHCP	AS	
Monitor AS/ UAV Mission Management Server	UDP	Internet Gateway	
Message Broker	TCP	User/Pilot	
Internet Gateway	UDP	Control Application Server (Operation Control Centre)	
Internet Gateway	UDP	User/Pilot	
Identity Management Server		Control Application Server (Operation Control Centre)	Access Management
Identity Management Server		User/Pilot	Access Management
VPN access			

4.4 VS4: Network Applications and Services for UC4

This UC supports the implementation of a situational awareness platform in support of Central Command Centre (CCC) operations, so as to obtain full awareness from the field during a disaster response. It utilises the Mobitrust Platform [18], which allows CCC to monitor PPDR agents in the field equipped with Body-Kit Devices, by automatically collecting, retrieving and monitoring data from different types of sources: agent bio-sensors (*e.g.*, Electrocardiography [ECG], Oxygen Saturation [SpO2], respiration rate); geographical/indoor positioning; internal communication systems; vehicles; devices (*e.g.*, drones); shared services (*e.g.*, private websites or shared folders); and real-time text, audio and video transmissions. The UC4 vertical application is fully compatible with Kubernetes-based deployments. Following the paradigm of cloud-native solutions, all the internal components exist as CNFs. This contributes to the few hardware dependencies that the lightweight version of this vertical application presents:

- 8GB RAM.
- 16GB storage.
- i5 1.80GHz processor.

In terms of deployment, the internal components of the application may be deployed using a script that invokes sequentially a specific set of YAML files (one per component). This process uses readiness probes, to make sure that the dependencies among the different components are fulfilled, and the application is successfully deployed. In the future, the application will also be deployable through Helm package manager. In terms of cluster constraints, there are a few that need to be met:

- Kubernetes cluster has a Load Balancer installed, as well as a Nginx-controller.
- Storage is available through Persistent Volume Claims (PVCs).
- A DNS core change needs to be conducted by the cluster admin in order to redirect traffic aiming to reach the application for the correct deployment.

It is also advised to create a dedicated namespace for the application, aiming to prevent any co-existence problems (arising from the convenience of different applications in the same namespace). Internet access must be granted, mainly to deal with the loading of maps for geo-location.

The following list describes the main components of the Network Application (which are all CNFs):

- **End-user Device Simulator:** This component is used for integration tests and debug purposes. It pretends to simulate the data streams usually established between a real end-user device and the Mobitrust several components.
- **InfluxDB:** This represents the DB used to store the information collected from the multiple sensors present in the Mobitrust BodyKits (BK) [18].
- **Orchestrator:** The orchestrator is responsible for the management of the control data. It deals with the authentication and authorisation of users. Moreover, it is responsible for the setup of the end-user device components, including its drivers, and the establishment of the data channels for sensors and communication devices (cameras and microphones).
- **Web Real-Time Communication (WebRTC) Server:** The WebRTC Server is the component that deals with audio and video transmission in real time from the field to the CCC.
- **Message Broker:** This component represents the communication backhaul of the system. It follows a publish/subscribe model. The Message Broker is responsible for all the communication among components.
- **Telegraf:** A plugin-driven server agent for collecting and reporting metrics. Through connecting to the Message Broker, it collects data from the system, mainly sensor data from the end-user devices.
- **Monitor:** This micro-service is responsible for watching and reporting on the state of the end-user devices.
- **PostgreSQL:** The relational DB stores the information regarding users, end-user devices, WebRTC mount points, and their associations, as well as the access control policies.
- **Kapacitor:** This is a native data processing engine. It can process both stream and batch data from InfluxDB. With Kapacitor, it is possible to plug in custom logic, or user-defined functions, to process alerts with dynamic thresholds and perform specific actions based on these alerts.
- **Gateway:** The operational controller is responsible for the services provided by the CCC. It has all the backend operations that enable the visualisation of the data collected by the platform, as well as the processing of requests of the human operators.

The vertical application used to demonstrate the Network Application composed of the above services is a Portal which is the frontend of the platform developed by ONE. It corresponds to the actual CCC application to be used by human operators and it provides a way to obtain situational awareness by visualising all the data collected by the platform.

Figure 10[4] presents the UC4 vertical system's specific architecture. Table 10 shows the vertical solutions decomposed in NSs, identifying the interfaces between them, and providing a brief description of each one.

[4] In Figure 10, the abbreviation that has not been mentioned earlier in the document is the following one:
UDR: Unified Data Repository

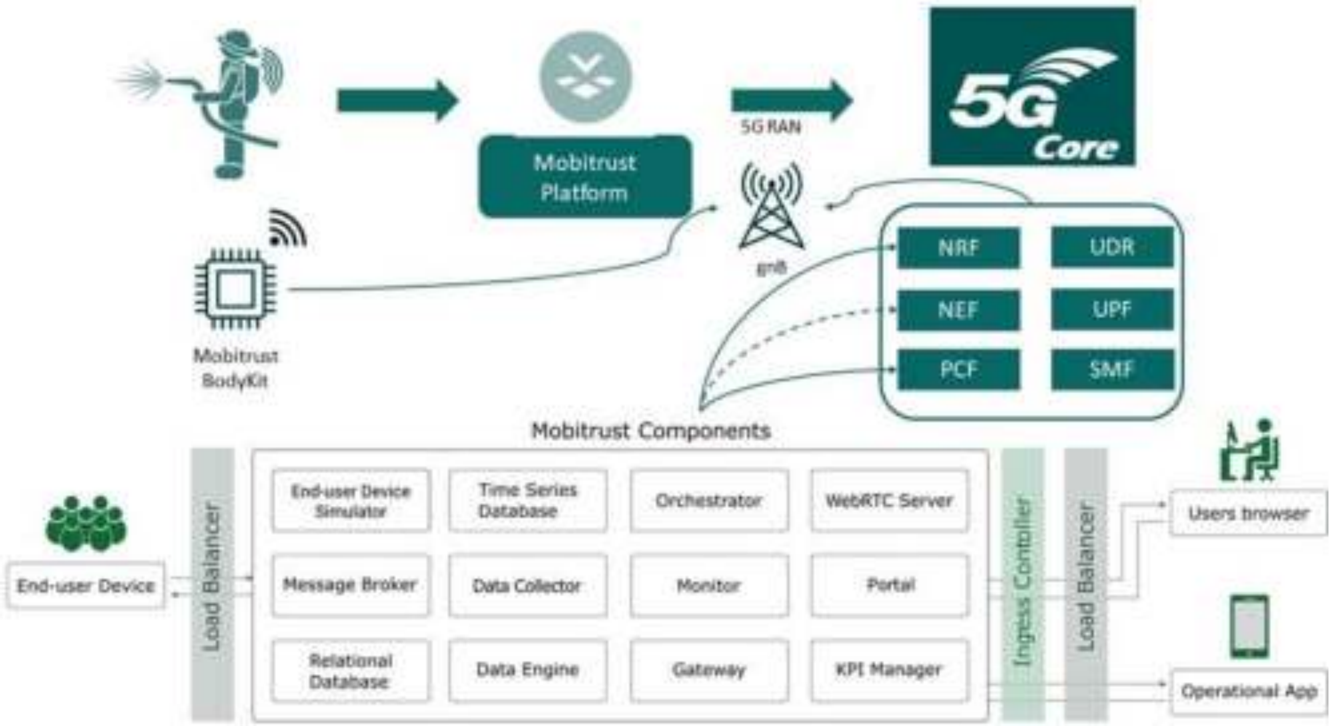


Figure 10: UC4 vertical system under test - specific architecture

Table 10: UC4 NSs and interfaces

Source Network Service	Interface	Destination Network Service	Comments
5GC		5G RAN (NRF)	
5GC		5G RAN (NEF)	
5GC		5G RAN (PCF)	
5GC		5G RAN	
End-user Device	TCP / UDP	Commercial-off-the-Shelf (COTS) device	
User browser	TCP / UDP	Mobitrust CCC	
Operational App	TCP / UDP	Mobitrust Operational App	
Internal Mobitrust Compo-nents	HTTPS, SCTP, TCP	Mobitrust Compo-nents	

4.5 VS5: Network Applications and Services for UC5

The UC5 vertical system will interact with 5G-EPICENTRE's cloud-native environment and the underlying 5G infrastructure as shown in Figure 11.

The solution is based on managing a small fully containerized cloud with video routing elements, in yellow in the picture which we call the video region cloud. While the main management of the Network Application is on a global cloud (in blue in the picture), the actual video elements are meant to be placed closer to users to both improve performance and security. This deployment is meant to scale horizontally based on load.

This video region cloud is composed of 1 to N WebRTC Servers that distribute video as required and 1 to N load balanced Turn Server that coordinate video transmission handshakes and can act as relay over firewalls.

The deployment of this video region cloud can be coordinated from an orchestration service in the main cloud, this orchestration service also provides any configurations required to run the containerized NSs.

The Green boxes are meant to show how the services are in relation to a 5G Core, in case the video region is deployed in an edge cloud or in a regular cloud.

The main cloud in BlueEye is also responsible for Network Application-level management and control, such as assigned and directing users to connect to the proper video region for the video transmission they want to see or broadcast.

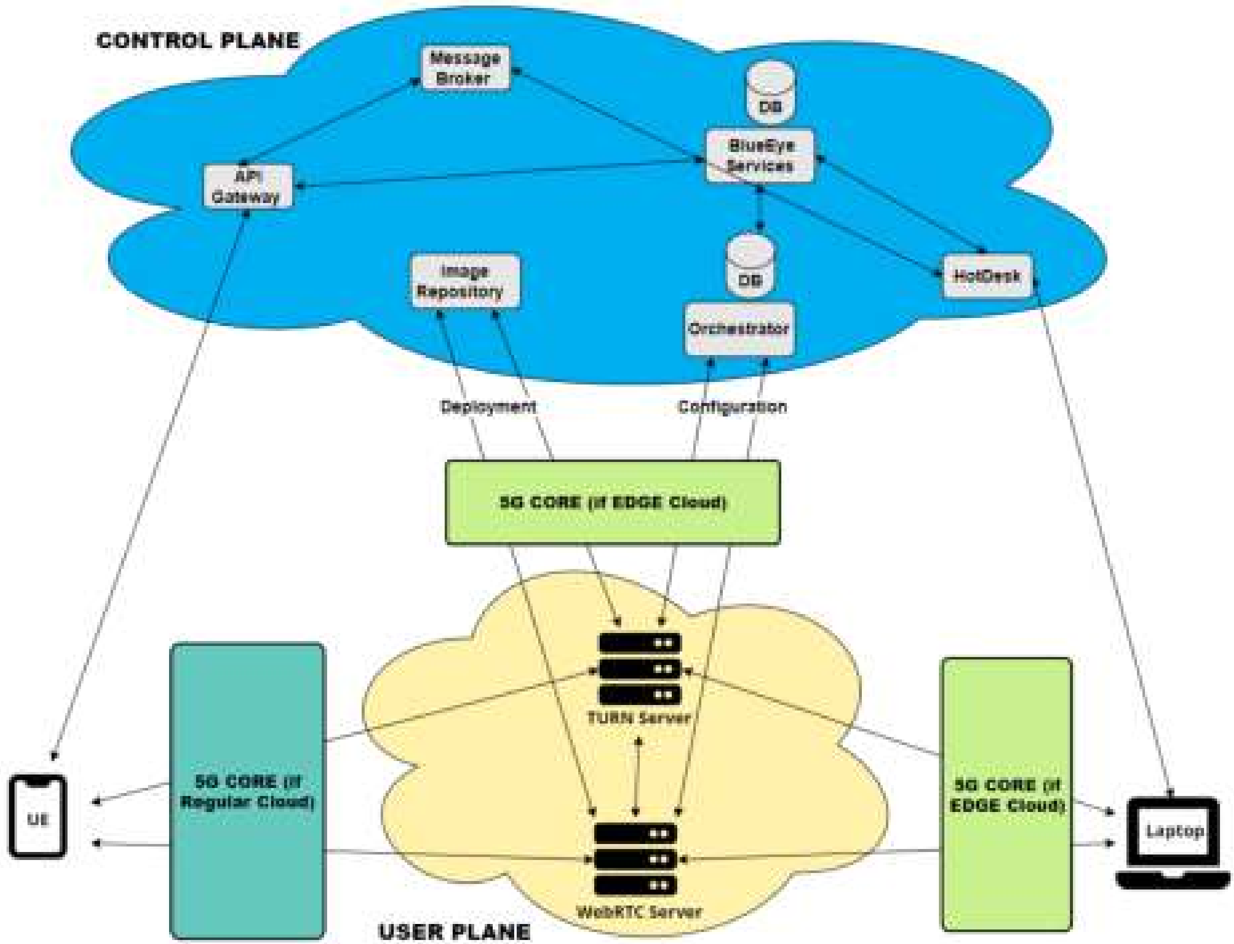


Figure 11: UC5 vertical system under test - specific architecture

Table 11 shows the vertical solutions decomposed in NSs, identifying the interfaces between them, and providing a brief description of each one.

Table 11: UC5 NSs and interfaces

Source Network Service	Interface	Destination Network Service	Comments
UE	TCP	TURN Server	
UE	TCP/UDP	WebRTC Server	
UE	TCP	API Gateway	
TURN Server	TCP/UDP	WebRTC Server	
TURN Server	TCP	Laptop	
TURN Server		Container Image Repository	Deployment Purpose
TURN Server	TCP	Orchestrator	
WebRTC Server	TCP/UDP	Laptop	
WebRTC Server		Container Image Repository	Deployment Purpose
WebRTC Server	TCP	Orchestrator	
Laptop	TCP	Hotdesk	
Hotdesk	TCP	BlueEye Services	
Hotdesk	TCP	Message Broker	
BlueEye Services	TCP	Orchestrator	
BlueEye Services	TCP	API Gateway	
API Gateway	TCP	Message Broker	

4.6 VS6: Network Applications and Services for UC6

UC6 is planning to transfer images from a camera (SMP) to a containerized AI Analyzer (AI-AS) Network Application, running on the 5G Core Network. An also running containerized Proxy-NS will relay the images to the Display-Devices (as part of the AS). The AI-Analyzer Network Application will recognize objects and send the found objects meta data to the Display device (MVD).

Vertical Application domain:

- Image Sender

- Display Device

Network Application Domain:

- Containerized AI-Analyzer Network Application
- Containerized Proxy NS
- Containerized Dummy-Image-Sender NS

The Mobile Display Device receives the relayed images and the detected objects meta data and displays the information's with *e.g.* boxes around objects and prediction tag.

The AI-Network Application and the Proxy-NS expect to receive images with timestamps in a pre-defined format. The format depends on the classic Unix timestamp format.

To measure processing times and latency's the AI- Network Application and Proxy-NS will generate timestamps on receiving, on processing start on processing end and on finished after sending the metadata or images. They will send these timestamps for further calculations via MQTT to the HHI 5G MQTT instance.

For further testing UC6 provide a Dummy-Image-Sender NS, which sends images in the right format periodically to the proxy and AI-Analyzer. The Dummy-Image-Sender NS is fully containerized too.

The UC6 vertical system will interact with the 5G-EPICENTRE cloud-native environment and the underlying 5G infrastructure as shown in Figure 12.

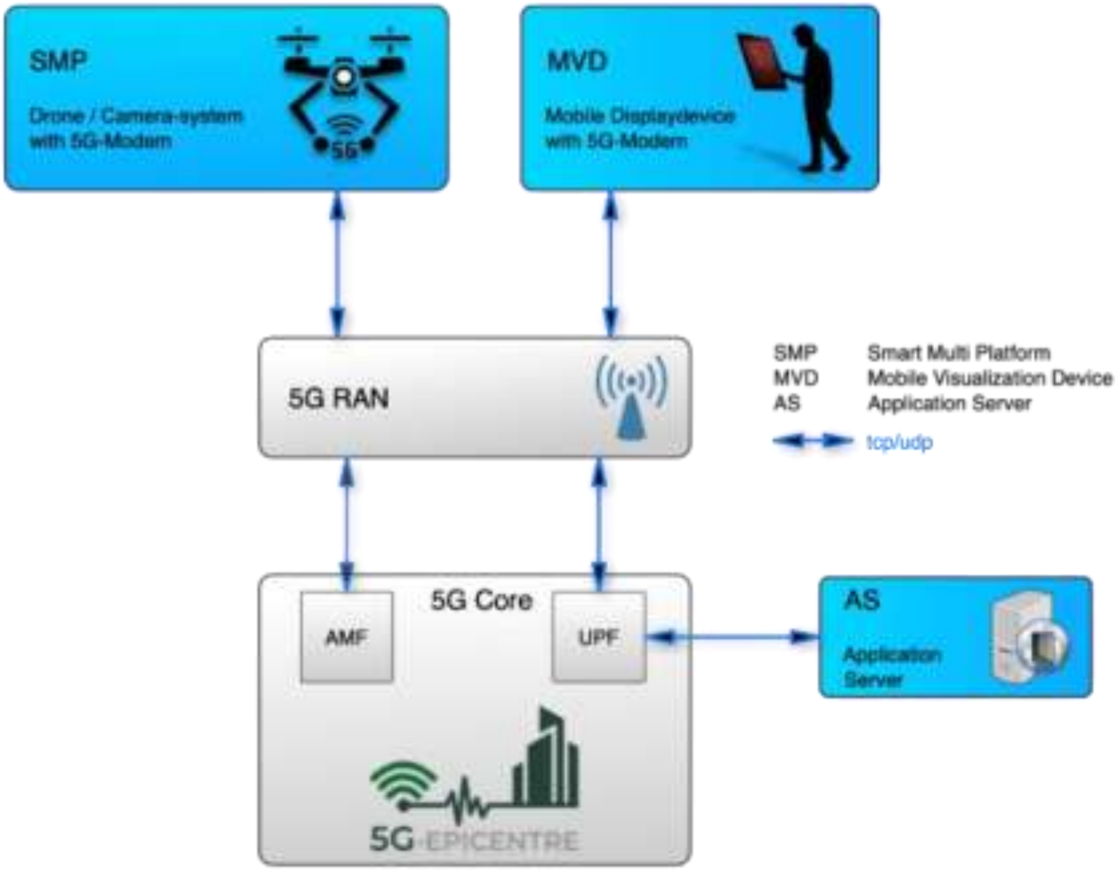


Figure 12: UC6 vertical system under test - specific architecture

Table 12 shows the vertical solutions decomposed in NS, identifying the interfaces between them, and providing a brief description of each one.

Table 12: UC6 NSs and interfaces

Source Network Service	Interface	Destination Network Service	Comments
SMP 5G	TCP / UDP	5G RAN	Bidirectional
MVD 5G	TCP / UDP	5G RAN	Bidirectional
5GC (AMF)	TCP / UDP	5G RAN	Bidirectional
5GC (UPF)	TCP / UDP	5G RAN	Bidirectional
5GC (UPF)	TCP / UDP	AS Application Server	Bidirectional
AS	TCP / TCP	Internet	Bidirectional

4.7 VS7: Network Applications and Services for UC7

The UC7 vertical system relies on Q-Application component, which provides the collection of geolocated data and makes it available through a fast communication channel. Systems can use the Q-Application to deposit geolocated information that is later consumed by interconnecting, or data presentation systems.

The system is based on the Qube framework, allowing for high customisation in both NFs and data presentation and storage.

The application requires these hardware features:

- 24 virtual CPUs.
- At least 24Gb of RAM.
- At least 10Gb of persistent storage (this depends on the multimedia materials to be stored).
- Open ports: 80 for web interface and 5672 for the broker.

A summary of the different micro-services involved in the UC7 vertical system trial is provided below:

- **Q-Application:** Vertical application component responsible for data management and organisation of information by providing support to departments for submission of collected data:
    - ***ProcessToStoreData:*** It is responsible for processing the data taken from the broker, and saving it in the system.
    - ***LiveData:*** It is responsible for collecting data to produce a live data stream.
- **DB:** SQL DB used to store data and configuration information.
- **Message Broker:** It implements the intercommunication channel between systems and NFs.
- **HTTP-Proxy:** It is middleware of external HTTP traffic, redirecting HTTP traffic to the corresponding microservice.

The architecture of the UC7 vertical system is shown in Figure 13. Table 13 shows the vertical solutions decomposed in NSs, identifying the interfaces between them, and providing a brief description of each one.

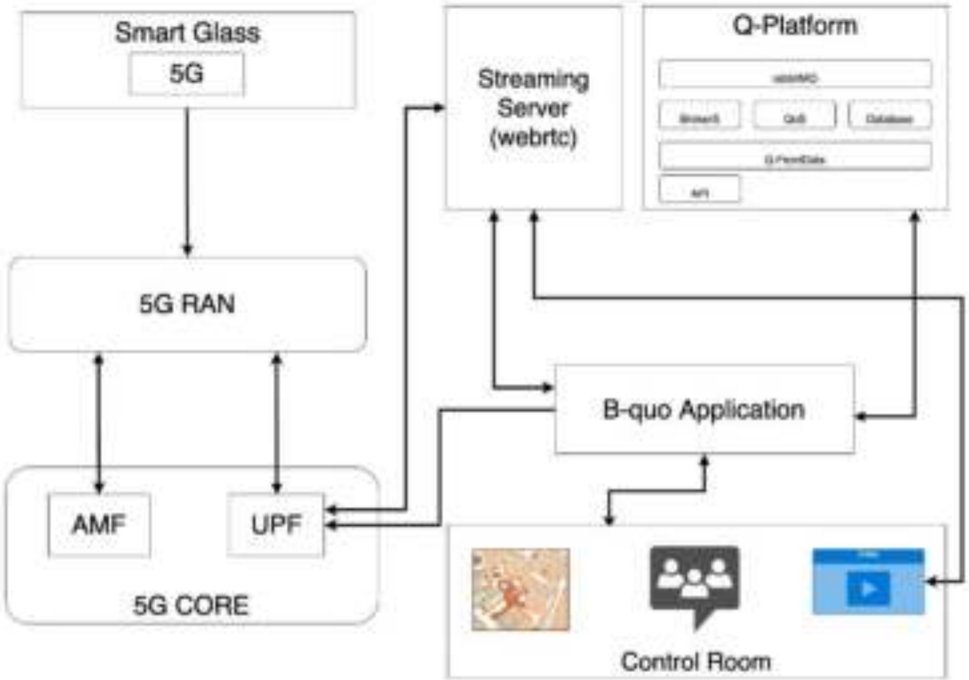


Figure 13: UC7 vertical system under test - specific architecture

Table 13: UC7 NSs and interfaces

Source Network Service	Interface	Destination Network Service	Comments
SGs	TCP / UDP	5G RAN	
5G RAN	TCP / UDP	5G Core AMF	
5G RAN	TCP / UDP	5G Core UPF	
5G Core UPF	UDP	Streaming Server	
Streaming Server	UPD	Control Room / Live Monitoring Video	

4.8 VS8: Network Applications and Services for UC8

Mobile AR vertical applications are among the technologies expected to benefit the most from the wide deployment of 5G networks [19]. This UC involves real-time, remote AR 3D rendering and streaming in the context of

PPDR. More specifically, the UC8 vertical system to be experimented with entails the use of light, portable, and battery-efficient AR Head-Mounted Displays (HMDs), allowing first responders to view deformable 3D objects (bones, vessels, organs, *etc.*) overlayed on top of a victim at a disaster site.

A single VM will be deployed within a kubevirt sandbox. For the time being, the testbed will be deployed on the CTTC testbed only. Below is some relevant information.

- Ensure that Kubernetes cluster with kubevirt is installed.
- For each cluster, depending on hardware capabilities, the corresponding number of VMs can be spawned. In our case, this is usually 1 per machine (with an NVIDIA GPU, performance-wise greater than GTX 1060).
- Ensure that storage (persistent volumes) is available through PVCs.
- Wait for an instantiation message from an external vertical application connected with the message handler of the framework.
- Upon receiving the aforementioned message, instantiate exactly one instance of the VM.
- For the VM, ports 9090 and [20000-24999] (subject to change) as well as 3478 need to be forwarded to ensure that WebRTC will find a connection or use the proper STUN or TURN servers:
    - Expose the IP address of the VM externally.
    - Send the IP address as an answer back to the externally connected application that initially made it.
    - Another vertical application component (ORAMA_HMD application) will be deployed on a Magic Leap 1 AR-HMD. Both the HMD and the vertical application are provided by ORAMA.

Table 14 shows the vertical system decomposed in NSs, identifying the interfaces between them, and providing a brief description of each one. Figure 14 presents the architecture of the UC8 solution.

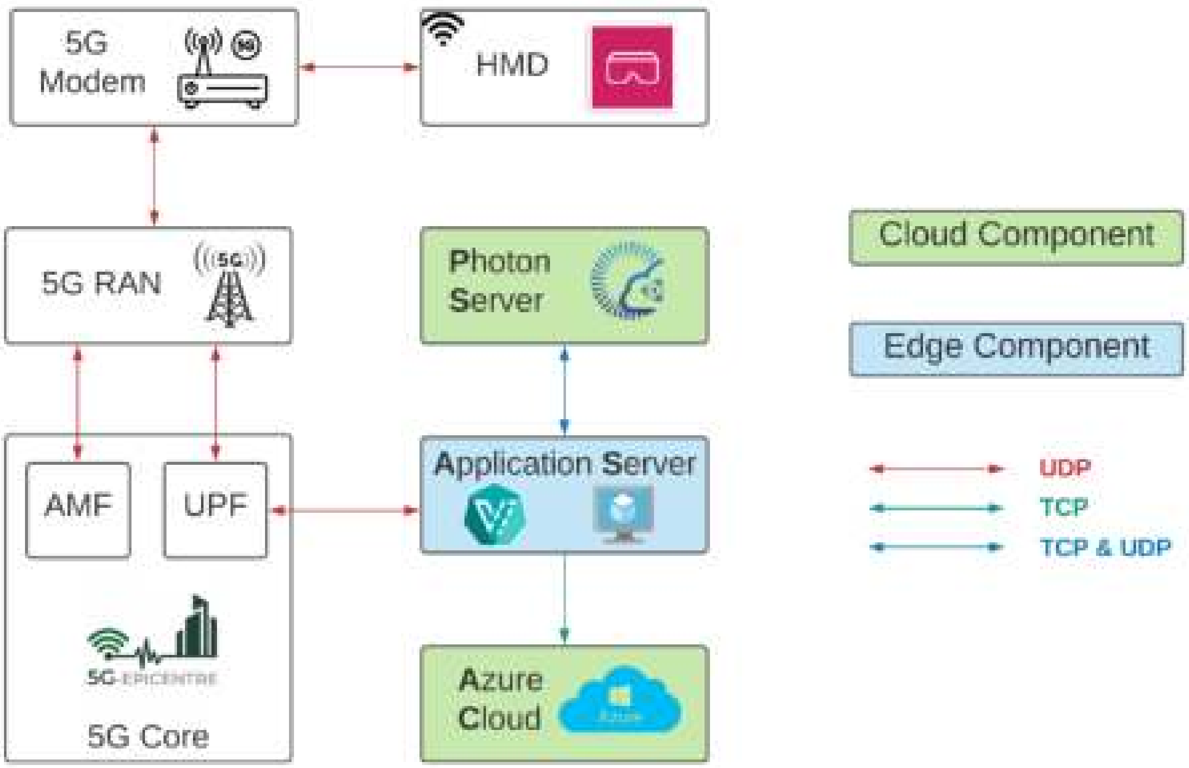


Figure 14: UC8 vertical system under test - specific architecture

Table 14: UC8 NSs and interfaces

Source Network Service	Interface	Destination Network Service	Comments
5GC (AMF)	UDP	5G RAN	Bidirectional
5GC (UPF)	UDP	5G RAN	Bidirectional
5GC (UPF)	UDP	AS	Bidirectional
5G RAN	UDP	5G Modem	Bidirectional
5G Modem	UDP	AR HMD Application	Bidirectional, over Wi-Fi
AS	TCP	Azure Cloud	
AS	TCP, UDP	Photon Server	Bidirectional

A short summary of the UC8 Network Application microservices is provided below:

- **AR AS:** This component is responsible for performing the physics calculations and final scene rendering based on the user inputs it receives over the 5G network. It is also responsible for compressing the video stream and transmitting it via WebRTC (or an equivalent protocol) to the HMD. A message broker is incorporated within this component too.
- **Photon Server (optional):** This component is responsible for exchanging the required information among users, in multi-user scenarios, keeping them in sync. This component will be deployed only if a multi-user AR scenario is designed.
- **Azure Cloud Service (optional):** This component is responsible for storing necessary data. The data may be digested (analytics) after being anonymised. This component will be deployed only if user's actions analytics are incorporated in an AR-scenario.

The vertical application used to demonstrate the Network Application composed of the above services is an AR HMD Application, which is responsible for the broadcast of the initiate sequence to the 5G-platform and receiving the IP of the VM as a response from the respective edge node. It is also responsible for the broadcast of user input (displacement & triggers) via the 5G network to the AS, as well as for decoding and projecting the video stream, received from the AS.

5 Conclusions

This deliverable provides an overview of the developments that have been made in the framework of 5G-EPICENTRE and its approach to Network Applications. It provides a concise overview of the functionalities for which the Network Applications have been created, the main NSs that compose them, the specific approach followed by each one, and classifies them according to their openness or containerisation level.

Common Network Applications have been created, which will be useful to any 5G-EPICENTRE experimenter. This middleware is especially oriented towards PPDR experimenters, facilitating the manipulation of experimental data in a personalised manner, offering security guarantees in a sector in which these aspects are of vital importance, or enabling new 5G functionalities that represent a differentiating factor for the choice of this type of networks, thus boosting the adoption of the technology. The three vertical-agnostic Network Applications developed so far are: i) Analytic Services Network Application; ii) Network Intrusion Detection Network Application; and iii) QoS Management Network Application.

On the other hand, the verticals that have validated the platform have been contributing to the creation of a repository (or library) of Network Applications, specially designed for the PPDR sector. More specifically, these are disruptive Network Applications that can be offered to future experimenters both to show what is possible to achieve on 5G networks, and to facilitate their internal processes in the adoption of the technology.

In addition, thanks to the collaboration between partners, and the interactions between architecture elements and Network Applications considered in this document, common definitions have been created. Processes have been standardised, providing concrete models through which future Network Applications can be incorporated into the 5G-EPICENTRE solution. This means a coherent context, in which the PPDR sector can explore the possibilities that 5G technology offers them, a habitat which the sector is able to use (and at the same time, nurture) to make it bigger.

In short, a useful platform has been created for the PPDR sector, with tools that will simplify their access to 5G technology. It creates a repository of different solutions that can be used by third parties, creating a library of sector-specific tools. The 5G-EPICENTRE platform can grow and incorporate new Network Applications as it is opened to third parties, thus aiming to become a library of services specialised in PPDR solutions and with access to facilities for experimentation.

The next steps will seek to consolidate the work done so far, and refining the APIs that will be exposed to verticals to maximise their usefulness in the framework of 5G-EPICENTRE.

References

[1] Patachia-Sultanoiu, C., Bogdan, I., Suciu, G., Vulpe, A., Badita, O., & Rusti, B. (2021,). Advanced 5g architectures for future netapps and verticals. In *2021 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom)* (pp. 1-6). IEEE. https://doi.org/10.1109/BlackSeaCom52164.2021.9527889

[2] Trichias, K., Landi, G., Seder, E., Marquez-Barja, J., Frizzell, R., Iordache, M., & Demestichas, P. (2021,). Vital-5g: innovative network applications (netapps) support over 5g connectivity for the transport & logistics vertical. In *2021 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit)* (pp. 437-442). IEEE. https://doi.org/10.1109/EuCNC/6GSummit51104.2021.9482437

[3] Slamnik-Kriještorac, N., Landi, G., Brenes, J., Vulpe, A., Suciu, G., Carlan, V., et al. (2022). Network applications (netapps) as a 5g booster for transport & logistics (t&l) services: The vital-5g approach. In *2022 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit)* (pp. 279-284). IEEE. https://doi.org/10.1109/EuCNC/6GSummit54941.2022.9815830

[4] Apostolakis, K. C., Margetis, G., Stephanidis, C., Duquerrois, J. M., Drouglazet, L., Lallet, A., et al. (2021). Cloud-native 5g infrastructure and network applications (netapps) for public protection and disaster relief: The 5g-epicentre project. In *2021 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit)* (pp. 235-240). IEEE. https://doi.org/10.1109/EuCNC/6GSummit51104.2021.9482425

[5] Trantzas, K., Tranoris, C., Denazis, S., Direito, R., Gomes, D., Gallego-Madrid, J., et al. (2021). An automated ci/cd process for testing and deployment of network applications over 5g infrastructure. In *2021 IEEE International Mediterranean Conference on Communications and Networking (MeditCom)* (pp. 156-161). IEEE. https://doi.org/10.1109/MeditCom49071.2021.9647628

[6] Koumaras, H., Tsolkas, D., Garcia, J., Artunedo, D., Garcia, B., Marco, R., et al. (2022). A network programmability framework for vertical applications in the beyond 5G era. In *2022 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit)* (pp. 375-380). IEEE. https://doi.org/10.1109/EuCNC/6GSummit54941.2022.9815790

[7] Chochliouros, I. P., Spiliopoulou, A. S., Lazaridis, P. I., Zaharis, Z. D., Spada, M. R., Pérez-Romero, J., et al. (2021). 5G for the support of public safety services. *Wireless Personal Communications*, *120*(3), 2321-2348. https://doi.org/10.1007/s11277-021-08473-5

[8] Sayadi, B., Chang, C.-Y., Tranoris, C., Iordache, M., Katsaros, K., Vilalta, R., et al. (2022). *Network Applications: Opening up 5G and beyond networks* [White paper]. Zenodo. https://doi.org/10.5281/zenodo.7123919

[9] Arampatzis, D., Apostolakis, K. C., Margetis, G., Stephanidis, C., Atxutegi, E., Amor, M., et al. (2021). Unification architecture of cross-site 5g testbed resources for ppdr verticals. In *2021 IEEE International Mediterranean Conference on Communications and Networking (MeditCom)* (pp. 13-19). IEEE. https://doi.org/10.1109/MeditCom49071.2021.9647591

[10] 3GPP Organizational Partners. (2022). 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; 5G System; Policy and Charging Control signalling flows and QoS parameter mapping; Stage 3 (Release 17). *3GPP TS 29.513 V17.8.0 (2022-09) Technical Specification*. Retrieved from https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3354

[11] 3GPP Organizational Partners. (2021). 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; System architecture for the 5G System (5GS); Stage 2 (Release 16). *3GPP TS 23.501 V16.11.0 (2021-12) Technical Specification*. Retrieved from https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3144

[12] 3GPP Organizational Partners. (2021). 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Procedures for the 5G System (5GS); Stage 2 (Release 17). *3GPP TS 23.502 V17.3.0 (2021-12) Technical Specification*. Retrieved from https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3145

[13] Race, N. (2022, November). *Airbus and partners successfully integrated Mission Critical Services on University of Malaga 5G mobile network as part of the 5G-EPICENTRE project* [Airbus press release]. Retrieved from

https://www.securelandcommunications.com/en-press-releases/airbus-and-partners-successfully-integrated-mission-critical-services-on-university-of-malaga-5g-mobile-network-as-part-of-the-5g-epicentre-project

[14] 3GPP Organizational Partners . (2022). 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; 5G System; Policy Authorization Service; Stage 3 (Release 17). *3GPP TS 29.514 V17.6.0 (2022-09) Technical Specification*. Retrieved from https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3353

[15] 3GPP Organizational Partners. (2021). 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Functional architecture and information flows to support Mission Critical Push To Talk (MCPTT); Stage 2 (Release 17). *3GPP TS 23.379 V17.8.0 (2021-09) Technical Specification*. Retrieved from https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3089

[16] 3GPP Organizational Partners. (2021). 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Functional architecture and information flows to support Mission Critical Video (MCVideo); Stage 2 (Release 17). *3GPP TS 23.281 V17.6.0 (2021-06) Technical Specification*. Retrieved from https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3087

[17] 3GPP Organizational Partners. (2021). 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Functional architecture and information flows to support Mission Critical Data (MCData); Stage 2 (Release 17). *3GPP TS 23.282 V17.8.0 (2021-09) Technical Specification*. Retrieved from https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3088

[18]Henriques, J., Gomes, A., & Cordeiro, L. (2022). Iot for improving first responders' situational awareness and safety on federated 5g testbeds. *Zenodo*. https://doi.org/10.5281/zenodo.6783271

[19]Qiao, X., Ren, P., Dustdar, S., Liu, L., Ma, H., & Chen, J. (2019). Web ar: A promising future for mobile augmented reality—State of the art, challenges, and insights. *Proceedings of the IEEE*, *107*(4), 651-666. https://doi.org/10.1109/JPROC.2019.2895105