PUBLIC-PRIVATE PARTNERSHIP

DEDICAT 6G

DEDICAT 6G: Dynamic coverage Extension and Distributed Intelligence for human Centric Applications with assured security, privacy and Trust: from 5G to 6G

Deliverable D2.2
Initial System Architecture

Project Details

Call	H2020-ICT-52-2020
Type of Action	RIA
Project start date	01/01/2021
Duration	36 months
GA No	101016499

Deliverable Details

Deliverable WP:	WP2
Deliverable Task:	Task T2.2 and T2.3
Deliverable Identifier:	DEDICAT6G_D2.2
Deliverable Title:	Initial System Architecture
Editor(s):	François CARREZ (UoS)
Author(s):	Editor + WP2 partners
Reviewer(s):	Fernando Diaz Bravo & Javier Moreno (ATOS), Pablo Sanchez (TTI), Aarne Mämmelä (VTT)
Contractual Date of Delivery:	September 30th, 2021
Submission Date:	September 30th, 2021
Dissemination Level:	PU
Status:	FINAL
Version:	V1.0
File Name:	DEDICAT6G_D2.2_Initial System Architecture_v1.0.docx

Deliverable History

Version	Date	Modification	Modified by
V0.1a	*31/03/2021*	*ToC*	*François Carrez*
v0.1b -0.1g	*13/04/2021*	*Sections 2 (complete), 3, 4, 5 & 6 pre-filled*	*François Carrez*
v0.1h-v0.1p	*30/08/2021*	*Contribution*	*WP2 Partners*
v0.1q-v0.1v	*04/09/2021*	*Completion*	*François Carrez, Fernando Diaz, Javier Moreno, Srdjan Penjivrag*
v0.1w_FOR_REVIEW	*03/10/2021*	*Ready for Review*	*François Carrez*
v0.1y – v0.1_PRE-FINAL3	*29/10/2021*	*Review comments + Finalization*	*François Carrez, Fernando Diaz, Javier Moreno, Srdjan Penjivrag*
v1.0_FOR_DELIVERY	*29/10/2021*	*For delivery*	*François Carrez*

Table of Content

List of Acronyms and Abbreviations

Acronym/Abbreviation	Definition
a.k.a.	Also Known As
AAA	Authentication Authorization Accounting
ACL	Access Control List
AF	Application Function
AGV	Automated Guided Vehicle
AI	Artificial Intelligence
AMF	Access Mobility Function
AP	Access Point
API	Application Programming Interface
AR	Augmented Reality
B5G	Beyond 5G
BLE	Bluetooth Low Energy
BLEMAT	Bluetooth Low Energy Micro-location Asset Tracking
BS	Base Station
C&C	Command & Control
CEaaS	Coverage Extension as a Service
CEDM	Coverage Extension Decision Making
CU	Control Unit
CV	Context View
D6G	DEDICAT 6G (used in tables only)
DA	Distributed Agents
DC	Design Constraint
DCH	Design CHoice
DDoS	Distributed Denial of Service
DIKW	Data-Information-Knowledge-Wisdom
DNS	Domain Name Service
DoA	Description of Action
DoS	Denial of Service
DU	Distributed Unit
DVFS	Dynamic Voltage and Frequency Scaling
E2E	End-to-End
EC	Edge Computing
EN	Edge Node
eNB	e(volved) NodeB (a.k.a. E-UTRAN NodeB)
e.g.	“exempli gratia” (Latin locution)
FC	Functional Component
FCAPS	Fault/Configuration/Audit/Performance/Security
FG	Functional Group

FLOPS	FLoating OPeration per Second
FM	Functional Model
FREQ	Functional REQuirement
FV	Functional View
GDPR	General Data Protection Regulation
gNB	(next)g(eneration)NodeB *(replaces 4G eNB)*
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
GUI	Graphical User Interface
H/M/L	HIGH/MEDIUM/LOW
HMI	Human Machine Interface
HTTP	Hyper-Text Transfer Protocol
H/W	HardWare
I/O	Input/Output
IAB	Integrated Access and Backhaul
ID	Identifier
IP	Internet Protocol
IDaaS	Intelligence Distribution as a Service
IDDM	Intelligence Distribution Decision Making
IEEE	Institute of Electrical and Electronics Engineers
IMS	IP Multimedia Sub-system
IoT	Internet of Things
IoV	Internet of Vehicle
i.e.	"id est" (Latin locution)
IV	Information View
JSON	Java-Script Object Notation
KPI	Key Performance Indicator
LDM	Local Dynamic Map
LiDAR	Light Detection And Ranging
µS	micro Service
MA	Mobile Assets
MAC	Medium Access Control
MANO	Management Network Orchestration
MAP	Mobile Access Point
MCS	Mission Critical Service
MCV	Manned Connected Car
MCX	Mission Critical {PTT, Video, Data Services}
MEC	Mobile Edge Computing
ML	Machine Learning
MSC	Message Sequence Chart
NAS	Non-Access Stratum

NDV	Network Deployment View
NEF	Network Exposure Function
NF	Network Function
NFREQ	Non-Functional REQuirement
NFV	Network Virtualization Function
NFV-I	NFV Infrastructure
NFV-O	NFV Orchestrator
NG-RAN	Next Generation RAN
NODM	Network Operation Decision Making
NPN	Non Public Network
NR	(5G) New Radio
NSSAI	Network Slice Selection Assistance Information
NSSF	Network Slice Selection Function
NWDAF	NetWork Data Analytics Function
OBU	On-Board Unit
OAM	Operation, Administration and Maintenance
OPS	OPeration per Second
OS	Operating System
OV	Operation View
P	Priority Level (i.e. H/M/L) used in requirement tables only
p/f	platform
PCF	Policy Control Function
PDCP	Packet Data Convergence Protocol
PDU	Protocol Data Unit
PE	Physical Entity
PEV	Physical Entity View
PF-x	Platform Functional (requirement number)-x
PFCP	Packet Forwarding Control Packet
PHY	PHYsical layer
PLMN	Public Land Mobile Network
PNF-x	Platform Non-Functional (requirement number)-x
PoP	Point of Presence
POV	Point of View
PPDR	Public Protection and Disaster Relief
PS	Physical System
PST	Privacy, Security & Trust
PTT	Push-To-Talk
QCI	QoS Class Identifier
RAM	Random Access Memory
RAN	Radio Access Network
RAT	Radio Access Technology

RDF	Resource Description Format
Resp.	Respectively
REST	Representation State Transfer
RF	Radio Frequency
RLC	Radio Link Control
RPC	Remote Procedure Call
RRC	Radio Resource Control
RSS	RDF Site Summary
RSU	Road Side Unit
RU	Radio Unit
S/W	SoftWare
SF-x	Scenario Functional (requirement number)-x
SIMD	Single Instruction Multiple Data
SLA	Service Level Agreement
SLAM	Simultaneous Location And Mapping
SMF	Session Mobility Function
SNF-x	Scenario Non-Functional (requirement number)-x
SNR	Signal Noise Ratio
SOTA	State Of The Art
SPP	Security and Privacy Protection
SSL	Secured Socket Layer
STRIDE	Spoofing (identity), Tampering (with data), Repudiation, Information (disclosure), Denial (of service), Elevation (of privileges)
T&C	Terms & Conditions
ToC	Table of Content
TSL	Transport Layer Security
UAV	Unmanned Aerial Vehicle
UC	Use-Case
UDR	Unified Data Repository
UE	User Equipment (e.g., mobile phone)
UF-x	Unified Functional (requirement number)-x
UML	Unified Modelling Language
UNF-x	Unified Non-Functional (requirement number)-x
UPF	User Plane Function
V2X	Vehicle to x
V2V	Vehicle to Vehicle
VEC	Virtual Environment Control
VIM	Virtual Infrastructure Manager
VM	Virtual Machine
VN	Vehicular Node
VNF	Virtual Network Function
VP	Viewpoint

VRU	Vulnerable Road User
vs.	versus (Latin locution)
WMS	Warehouse Management System
w.r.t.	with respect to

List of Figures

List of Tables

Executive Summary

This Initial Architecture document is the first in a series of 3 incremental versions. It aims at giving a -as precise as possible- first glance at the system architecture which consists of set of architecture views and perspective (as introduced by Rozanski and Woods architecture methodology). We tackle here many aspects of the desired DEDICAT 6G architecture, especially functional and non-functional and provide a first understanding of which functionalities the platform will provide and which qualities (in term of performance, trust, reliability to name just a few) this platform will feature.

Before introducing the architecture, it is worth reminding the main technical objectives of DEDICAT 6G, that are the three following pillars: 1) Dynamic Coverage Extension of existing legacy 5G Network, 2) Dynamic Intelligence Distribution towards (mobile) Edge Nodes and 3) novel solutions for Trust management based on federated learning.

The architecture work follows a precise and logical methodology that encompasses various steps, starting from an extensive requirement engineering process, followed by a first functional decomposition that gives a first glimpse at the functionalities which must be specified and implemented in order to fulfill those project technical objectives and a first description of the non-functional properties it must implement.

Other steps involve defining the technical perimeter of platform (what is in and what is out), elucidating the role of the external entities (human or not) and their interactions with the DEDICAT 6G system and most importantly, defining an initial description of how the platform and 5G legacy network will interact and cooperate with each other in selected operational scenarios, called system use-cases.

As for the main results obtained with this document we can include the definition of the project perimeter, which identifies what entities stand in the "cloud" and which other entities (e.g., Edge Nodes like Drones and Robots) stand at the Edge as a support to both dynamic Intelligence Distribution and 5G Coverage Extension e.g., Another important result consists of a preliminary functional decomposition and a set of system use-cases that demonstrate how those identified functional components work together in some selected scenarios like for instance, when providing Intelligence Distribution as a Service and Coverage Extension as a Service to a vertical business application. Finally, we also show (in the Network deployment View) how the DEDICAT 6G deploys alongside the 5G legacy network typical deployment (`access -> far edge -> Edge -> Cloud`) and interacts with the legacy 5G components.

This initial document will be complemented by 2 other iterations, leveraging, and aligning with the technical work achieved by the other technical work packages WP3, 4 and 5. With those new iterations, we will gain in overall preciseness and touch other aspects of the DEDICAT 6G system which, could not be dealt with in this initial version (especially additional views, perspectives and extended system use-case).

1 Introduction

This document provides a first version of DEDICAT 6G architecture as a set of architecture views and perspectives. A logical pathways leads us from the requirement collection and analysis to the targeted system functional decomposition, which consists of a large set of components interacting with each other and with the existing 5G network in order to implement the main concepts introduced in DEDICAT 6G "Description of Action" document [1], namely 1) dynamic radio coverage extension using a variety of mobile access points and edge nodes, 2) dynamic intelligence distribution relying on those edge nodes and 3) federated learning-based trust management.

Because we expect a lot of interactions to take place between DEDICAT 6G and the legacy 5G network we provide a first set of text-based system use-case the goal of which is to illustrate such interaction in the context of a particular system behaviour (e.g., reacting to a performance drop, equipment failure, etc.) Of course, those system use-cases are focusing on how Coverage Extension and Intelligence Distribution can be pragmatically implemented using DEDICAT 6G functional components and 5G legacy network component as well (Core and RAN).

This first document is intended to drive the work of the other technical work packages, and its further versions will align with the future results of those work packages.

An outline of the purpose and outcomes of the other sections of this document follows:

- Section 2 introduces the overall methodology (after Rozanski & Woods [2]) and concepts, which are used along this document. It provides a very clear, thorough and formal framework for elucidating the views and perspectives that ultimately define the DEDICAT 6G architecture.

  This process is initiated with a thorough requirement engineering process that starts with collecting requirements following two different standpoints (scenario holder and platform designer). The result of this step is embodied into a set of unified functional and non-functional requirements reflecting both standpoints at once. Two different pathways can then be followed:

  - The functional pathway: from understanding a functional requirement some needed functionalities can be identified, it could also be some information-related design choices or even some deployment constraints and strategies. Those different inputs are used to build up the views (e.g., in that case, the Functional, Information and Network Deployment views respectively);
  - The non-functional pathway: since we are in presence of the characterization of a system quality (non-functional requirement), we can't straightaway impact the views. On the contrary we need to elucidate first the corresponding perspective (like Privacy, Trust, Performance, Ethics, reliability, scalability etc.) Doing so, we delve into elaborating strategies and tactics to be followed in order to implement the desired system properties. The result of that process is a list of Design Choices that in turn will impact one, if not all, views (e.g., one or several new functional Components for the Functional View that are mandatory for implementing the property, or a particular component deployment strategy impacting then the Network Deployment view).
- With Section 3 we start digging into the DEDICAT 6G architecture. This first section is all about implementing the Requirement Engineering process as defined in Section 2. Because requirement collection was initiated already in D2.1 [3] (with the scenario standpoint), the main outcomes of this section is 1) a list of platform requirements (the platform designer's stand point) 2) a unified list of requirements that embodies both scenario and platform standpoints and finally a requirement mapping that maps all requirements to Views (Functional Group/Components) and Perspective. The result of this mapping is embodied within a VOLERE [4] Excel™ document, which can be accessed online. The list of

unified requirements -without its mapping part- can be accessed in this document in Section 3.3.

- Section 4 is fully dedicated to the architecture views, namely (and in order) the Physical-Entity, Context, Functional and Network Deployment views. It is worth noting here that the Information and instantiation views will be dealt with in respectively iterations 2 and 3 of this document. In a nutshell:
  - The Physical-Entity view (Section 4.1) is about defining the actors involved in DEDICAT 6G (human or not), their roles and their expected interactions with the system. We also emphasis here the pieces of information that are exchanged with DEDICAT 6G or captured by DEDICAT 6G (using sensors for instance) pinpointing potential privacy issues. This view is really focused on that data aspect;
  - The Context View (section 4.2) is about defining the perimeter of DEDICAT 6G elucidating which Devices -at large- (a.k.a. Physical Systems) are considered as part of DEDICAT 6G or outside its perimeter. This allows us in particular to identifying those Physical Systems that can be used to support the Dynamic Distribution of Intelligence towards the (mobile) edge nodes;
  - The Functional View (Section 4.3) proposes a functional model which is a layered group of clusters hosting functional components sharing similar purposes and concerns. Then follows the functional decomposition that gives a comprehensive list of functional components that are meant to implement the functional requirements. Finally, the system use-case sections provide an illustration of how those functional components interact with each other or with the legacy 5G system, for example to support the *Intelligence Distribution as a Service* and *Coverage Extension as a Service* scenarios;
  - Finally, the Network Deployment View (Section 4.4) focuses on the base-line generic deployment of the DEDICAT 6G (including the core part and edge part) alongside the 5G legacy system. It also shows how we intend to deploy some of the candidate functional components for migration. This first version of the network deployment view does not give insight upon the scenario deployment. This will be taken care of in the second iteration of this document;
- Section 5 completes the DEDICAT 6G architecture with the Perspectives. For each perspective (which represents a particular targeted quality of the system) we propose a set of activities and tactics that will lead to a set of design choices, while each design choices impacts one particular view. As a result, each perspective potentially impacts all views or just a few depending on the nature of the property and implemented tactics. In this first iteration we only deal with the Privacy, Security and Trust perspectives. Additional perspectives will be considered in the next iterations;
- The final Section 6 provides a conclusion and presents shortly the planned updates for the next iteration. It is followed by the bibliography.
- An additional Annex A gives the list of unified (scenario) requirements, as this document main purpose is on platform requirement and unification only.

1.1 Quick access to the main D2.2 outcomes

In this section (Table 1) the reader can quickly access the main outcomes of the current architecture iteration which are summarized into a table with access links to the relevant sections.

Table 1: Summary of project outcomes and quick access links

Category	Outcome	Link
Requirements engineering	DEDICAT 6G Threat Analysis	Section 3.1
	Platform Functional Requirements	Table 9
	Platform Non-Functional and Non-technical Requirements	Table 10

	UNIfied Functional Requirements	Table 11
	UNIfied Non-Functional & Non-Technical Requirements	Table 12
Views	**Physical-Entity View**	Section 4.1
	Inventory of Physical-Entities (Actors and role definition / nature of inter-actions)	Table 13
	Inventory of information of interest	Table 14
	Context View	Section 4.2
	Perimeter of DEDICAT 6G (inventory of Physical Systems)	Table 15
	Inventory of FCs at the edge of DEDICAT 6G or outside (includes scenario-specific FCs)	Table 16
	Scenario UML Use cases	Section 4.2.2
	Functional View	Section 4.3
	Functional model	Figure 21, Section 4.3.1
	Functional Decomposition (list of FCs per FG)	Section 4.3.2 & 4.3.3
	System Use-cases	Section 4.3.4
	Network Deployment View	Section 4.4
Perspectives	Privacy Perspective	Section 5.1
	Security Perspective	Section 5.2
	Trust Perspective	Section 5.3
Annex	List of Unified scenario requirements	Table 23 & Table 24

2 Methodology

2.1 Some elements of Rozanski & Woods terminology

2.1.1 Views

The Views are used to described non-overlapping aspects of a concrete system and defined as:

> *"A view is a representation of one or more structural aspects of an architecture that illustrates how the architecture addresses one or more concerns held by one or more of its stakeholders." [2]*

In DEDICAT 6G we will define the following views. Some of them are generic while others are application dependent (therefore bound to our four Scenarios/Use- Cases). Those later ones are marked with an asterisk.

- Physical-Entity View* (Section 2.6.1)
- Context View* (Section 2.6.2)
- Functional View (Section 2.6.3)
- Information View (Section 2.6.4 but not covered in D2.2)
- Network Deployment View * (Section 2.6.5)
- Instantiation View (Section 2.6.6 but not covered in D2.2)

2.1.2 Viewpoints

In order to describe a view, architects use viewpoints which aggregates different architectural concepts like for instance data flows, sequence diagrams, data modelling… in order to describe that particular aspect of the system. The definition by the IEEE 1471 standard *[6]* is:

> *"A viewpoint is a collection of patterns, templates, and conventions for constructing one type of view. It defines the stakeholders whose concerns are reflected in the viewpoint and the guidelines, principles, and template models for constructing its views. "[7]* In DEDICAT 6G we will be using various UML-based viewpoints to describe various aspects of the views, e.g.:

- **Data modelling:** Specification of data models using UML Object-oriented modelling;
- **System Use-case:** specification of inter-Functional Component interactions when achieving a specific task;
- **Scenario Use-Cases:** to specify the interactions taking place between the scenario Actors (including pieces of equipment outside the perimeter of the DEDICAT 6G platform) and the DEDICAT 6G system it-self;
- **Sequence diagrams (a.k.a. Message Sequence Charts or MSC):** to provide a dynamic look at the interactions between various Functional Components during a specific task;
- **Data flows:** identifying the flows of data between the different Functional Components during a specific task;
- **Textual descriptions.**

This list is not exhaustive and additional viewpoints could be used if needed.

2.1.3 Perspectives

> *An **architectural perspective** is a collection of activities, tactics, and guidelines that are used to ensure that a system exhibits a particular set of related quality properties that require consideration across a number of the system's architectural views. [7]*

where a quality property is defined as:

> *A **quality property** is an externally visible, non-functional property of a system such as performance, security, or scalability [7]*

Perspectives provide a more abstract description of a system, focusing on how the system behaves in opposition to what the system must do. Focusing on the qualities of the system, versus its functionalities, we can derive a number of categorized high-level objectives that need then to be analysed (resulting into the so-called strategies and tactics) before being translated into concrete *Design Choices* (DCH). Those categories are the architecture perspectives. The following preliminary set of perspectives is relatively common among IT systems and is by no mean to be considered as exhaustive; additional perspectives could be needed depending on the nature of the targeted IT system:

1. Trust, Security and Privacy (usually split into 3 perspectives)
2. Availability and Resilience
3. Evolution and Interoperability
4. Performance and Scalability

Perspectives are further explained in Section 2.7.

2.2 Introduction to architecting process

Having discussed a few points of terminology we can elucidate now the whole methodology (see Figure 1 below) that logically relates the different architecting tasks with each other.

In this figure, plain arrows refer to control flow while dashed arrows refer to dependency.

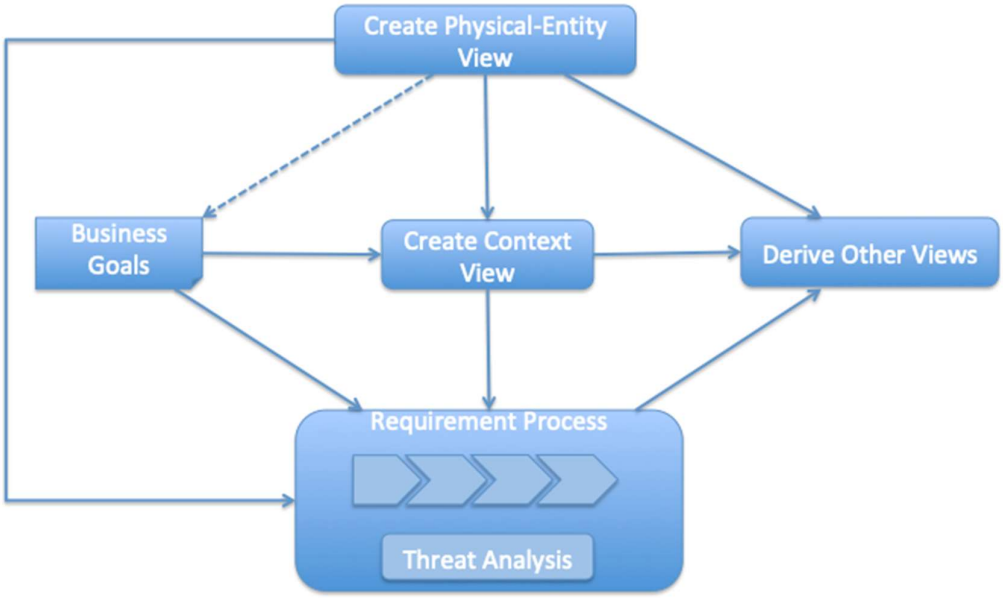


Figure 1: Simplified view of the architecting process

It is important to build first the *Physical-Entity View*[1] *(PEV)* because the exact nature of those entities (whether they are human or physical object) and what sort of information is tracked (e.g., location, pace/gait for humans and various sorts of quantities for physical objects) have an incidence on various aspects of the system and are fed to context View and the requirement process for further analysis.

[1] The PEV is described in more detail in Section 2.6.1

Second, the *Context View*[2] *(CV)* focuses on relationships between the system and its environment (consisting of people a.k.a. actors in D2.1 [3]), side (legacy) systems) which also impacts the requirement process.

Third Business Goals also impact the requirements process (via NFREQ) and the CV as the relationships between people/actors and the system may depend on those goals.

Finally, the remaining arrows are straightforward, based on the CV, PEV and requirement process outputs the other views are elucidated.

It is worth noting that part of "Derive other Views" box is the activity of dealing with perspectives, i.e. to describe tactics and sub-sequent concrete DCHs that –as we explain in detail in Section 2.6.6 below- do impact the design of the other views (i.e. FV, IV and NDV).

2.3 Introduction to the Threat analysis

This section describes the process, which will be used in the context of DEDICAT 6G for conducting a Threat Analysis.

The threat analysis can be considered as a part of the overall requirement engineering process, but was kept outside the Figure 2 below because it is conducted in parallel and more than once: 1st time to help identifying Security/Trust/Privacy requirements and a 2nd time to identify additional threats to the architecture itself (including the Security pane), after a first version has been built.

A threat analysis needs to be performed in order to come up with a list of potential threats to the system under design (some being identified during requirement collection), which are worth taking into account. In this process, we mitigate between known vulnerabilities, risks and potential impacts. This step will result in a set of security/privacy/trust-focused requirements.

In that process, one traditionally begins with a definition of the elements that have to be protected. Then, a thorough analysis of possible threats is conducted. How identified threats may actually affect elements to be protected, leads to the definition of risks. These risks have to be categorized, considering parameters such as criticality or probability of occurrence. In DEDICAT 6G the STRIDE [4] methodology is used for performing the threat analysis. Some more detail about STRIDE is available in Section 3.1, as an introduction to the actual DEDICAT 6G threat analysis that follows.

2.4 Introduction to the Requirement engineering process

The following Figure 2 is taken from D2.1 [3] (where it was first introduced) and is a reminder of the tasks involved during the requirement engineering process, namely:

- **Requirement collection:** to collect requirements from both the scenarios and platform points of view;
- **Requirement analysis:** This activity can be split into the two following steps:
  - **Requirements consistency check:** to check and deal with potential requirement inconsistencies, especially when multiple sources are involved;
  - **Requirement rewriting, factorization and alignment:** to discard duplicates and factorize as much as possible, to align with common vocabulary;
- **Requirement mapping:** The unified functional requirements need to be mapped to the *Functional View* (FV) where one or more *Functional Groups (FG)* (e.g., Decision Making FG) and *Functional Components (FC)* (e.g., Analytics FC or Coverage Extension FCs) can be identified (see as an illustration the "green" right-most part of the VOLERE template sample in Figure 3. This will result into the functional decomposition of the targeted system.

[2] The CV is described in more detail in Section 2.6.2

Some of the non-functional requirements can be mapped to the Information and Deployment Views. In a nutshell the requirement mapping is about:

1. mapping Functional Requirements (**FREQs**) to the Functional View performing the so-called functional decomposition;
2. mapping Technology and Design Constraints to Design Choices;
3. mapping Non-Functional Requirements (**NFREQs**) to other views (bar functional) and perspectives.

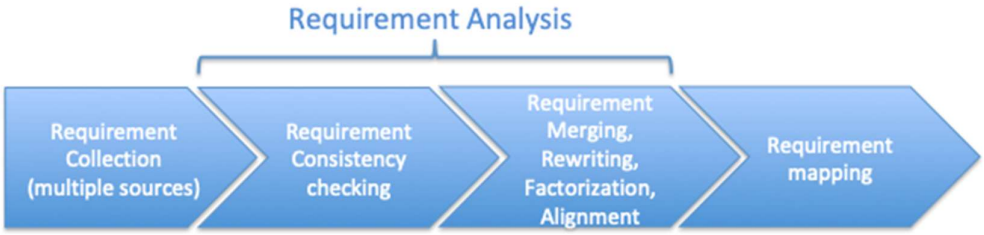


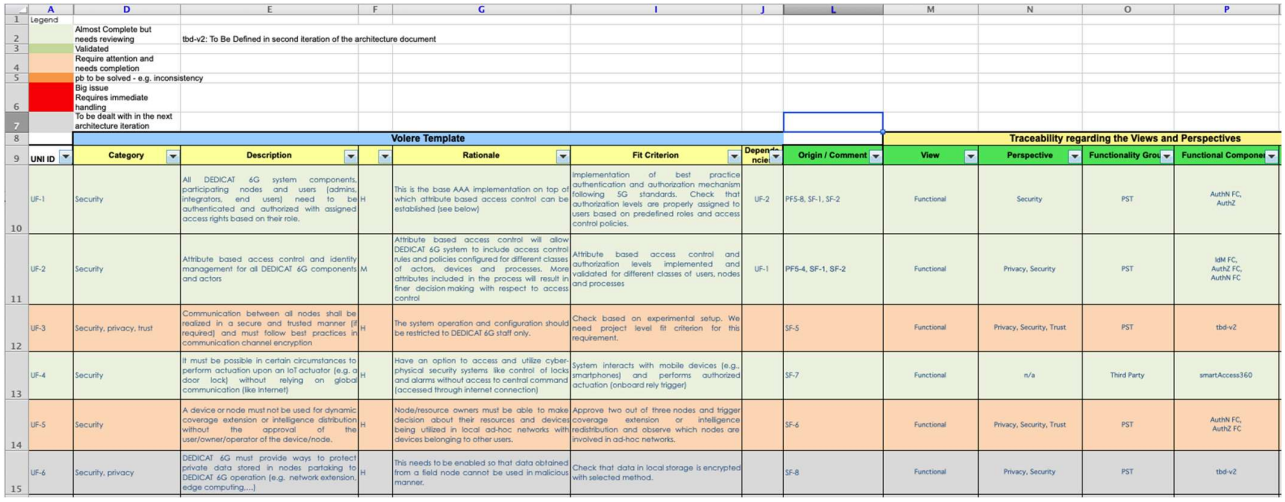
Figure 2: Requirement engineering steps

2.5 Requirement engineering supporting Tools

This additional section introduces a supporting tool used for summarizing the outcomes of the various steps described above, in the form of an Excel sheet. This is an outcome of Task 2.2, after various requirements have been unified. It is then updated during the mapping phase.

The VOLERE template used in DEDICAT 6G [5] has been adapted from the version used by the IoT-A project for collecting requirements (see Figure 3 below) which is itself an extension of the original VOLERE template [8], augmented in order to comply with the Rozanski & Woods methodology using Views, Viewpoints and Perspectives [7].

In particular this extension allows us to capture the essence of the View / Perspective mappings as explained in Sections 2.4 & 3.4.



	A	D	E	F	G	I	J	L	M	N	O	P
1	Legend											
2		Almost Complete but needs reviewing	tbd-v2: To Be Defined in second iteration of the architecture document									
3		Validated										
4		Require attention and needs completion										
5		pb to be solved - e.g. inconsistency										
6		Big issue Requires immediate handling										
7		To be dealt with in the next architecture iteration										
8		Volere Template							Traceability regarding the Views and Perspectives			
9	UNI ID	Category	Description		Rationale	Fit Criterion	Dependencie	Origin / Comment	View	Perspective	Functionality Gro	Functional Componer
10	UF-1	Security	All DEDICAT 6G system components, participating nodes and users (admins, integrators, end users) need to be authenticated and authorized with assigned access rights based on their role.	H	This is the base AAA implementation on top of which attribute based access control can be established (see below)	Implementation of best practice authentication and authorization mechanism following 5G standards. Check that authorization levels are properly assigned to users based on predefined roles and access control policies.	UF-2	PF5-8, SF-1, SF-2	Functional	Security	PST	AuthN FC, AuthZ
11	UF-2	Security	Attribute based access control and identity management for all DEDICAT 6G components and actors	M	Attribute based access control will allow DEDICAT 6G system to include access control rules and policies configured for different classes of actors, devices and processes. More attributes included in the process will result in finer decision making with respect to access control	Attribute based access control and authorization levels implemented and validated for different classes of users, nodes and processes	UF-1	PF5-4, SF-1, SF-2	Functional	Privacy, Security	PST	IdM FC, AuthZ FC, AuthN FC
12	UF-3	Security, privacy, trust	Communication between all nodes shall be realized in a secure and trusted manner (if required) and must follow best practices in communication channel encryption	H	The system operation and configuration should be restricted to DEDICAT 6G staff only.	Check based on experimental setup. We need project level fit criterion for this requirement.		SF-5	Functional	Privacy, Security, Trust	PST	tbd-v2
13	UF-4	Security	It must be possible in certain circumstances to perform actuation upon an IoT actuator (e.g. a door lock) without relying on global communication (like Internet)	H	Have an option to access and utilize cyber-physical security systems like control of locks and alarms without access to central command (accessed through internet connection)	System interacts with mobile devices (e.g., smartphones) and performs authorized actuation (onboard rely trigger)		SF-7	Functional	n/a	Third Party	smartAccess360
14	UF-5	Security	A device or node must not be used for dynamic coverage extension or intelligence distribution without the approval of the user/owner/operator of the device/node.	H	Node/resource owners must be able to make decision about their resources and devices being utilized in local ad-hoc networks with devices belonging to other users.	Approve two out of three nodes and trigger coverage extension or intelligence redistribution and observe which nodes are involved in ad-hoc networks.		SF-6	Functional	Privacy, Security, Trust	PST	AuthN FC, AuthZ FC
15	UF-6	Security, privacy	DEDICAT 6G must provide ways to protect private data stored in nodes partaking to DEDICAT 6G operation (e.g. network extension, edge computing,...)	H	This needs to be enabled so that data obtained from a field node cannot be used in malicious manner.	Check that data in local storage is encrypted with selected method.		SF-8	Functional	Privacy, Security	PST	tbd-v2

Figure 3: Glimpse at the VOLERE template

2.6 Introduction to the Architecture Views

This section introduces the six main architecture views, which will be used for the DEDICAT 6G architecture. We particularly focus on their purposes and on the viewpoints that can be used for elucidating them.

It is worth reminding that not all views are deal with in this first iteration of the deliverable; the Information and instantiation views will be tacked in the second and third iteration of his document, respectively.

2.6.1 Physical-Entity View

The purposes of the Physical-Entity View are:

- To identify the *Physical Entities* (PE) of interest for the DEDICAT 6G system. Those entities can be human or physical objects;
- To describe their properties of interest and how those PE will be kept track by the DEDICAT 6G system;
- In case some PEs are associated with sensors, to give detail about how the sensors relate to the object, if they are physically attached to the PEs or not and finally what quantities are measured;
- To give an exact list of the information captured by the DEDICAT 6G system either it is via sensors or personal devices (e.g., smart phone).

It is worth noting that having such information early directly impacts 1/ the NFREQ, especially on the Privacy aspects, and 2/ the Context View (as we will see in the next section) while providing essential early inputs to the data management Deliverable 1.3 [9] part of WP1.

As for viewpoints, we are using essentially textual description and tables.

2.6.2 Context View

According to Rozanski & Woods, the Context View ought to achieve the following tasks:

- To clearly define the perimeter of the DEDICAT 6G system, identifying external entities to the DEDICAT 6G platform (called Physical Systems later on);
- To define the nature and characteristics of those external entities
- To identify human actors and roles and their relation to the DEDICAT 6G system;
- To define external interfaces, please note that those interfaces are pretty much Scenario dependent, we will therefore focus on those required by UC1-UC4;
- To elucidate any external interdependencies, e.g., with legacy systems used.

Viewpoint-wise, we will mainly use UML Use-Cases for elucidating actor – system interactions.

2.6.3 Functional View

The Functional View is probably the view requesting the most of work as it covers many different (still related) aspects. The activities for building up that view are:

- To elaborate and describe a *Functional Model (FM)* that consists of a set of Functional Groups organized in layers, usually from the less to the most abstract following the well-known and widely referred to, *Data-Information-Knowledge-Wisdom (DIKW)* paradigm [10]; the FGs identified in the FM are the same FG found in the VOLERE template and used for requirement mapping;
- Based on the FM, to identify per FG the functional components that are needed to cover the FG objectives. Of course, at this stage the collected functional requirements are a main source of information for completing the activity. This results into functional

decomposition that eventually provides the main viewpoint of the FV embodied into the functional model filled up with all relating FCs (as result of the requirement mapping on one side and Perspectives elicitation and outcome on the other side);
- To describe all FCs with intended API (high-level);
- Through a set of system UML-based diagrams, to identify typical essential patterns resulting from either person-to-system or physical object-to-system interactions or from internal autonomous process like e.g., "decision making leading to the migration of intelligence to the edge nodes". Those UCs will be essential for the common understanding of what the system does and will be therefore a very meaningful input to the technical WPs, ensuring that they follow the architecture principles;

As far as viewpoints are concerned, we will use the UML notation for static and dynamic inter-FG interactions, e.g., sequence diagrams and UML use-cases for interactions taking place across the system boundary box.

Please note that whenever human actors partake into Human-System interactions, it is important to mention what particular role is endorsed by the Human counterpart.

2.6.4 Information View

As the name suggests, the IV is all about data and information. This view will therefore elucidate the following information-related aspects:

- To elucidate data flows occurring between system FCs and those occurring across the boundary box of the system (e.g., a person smartphone, should we decide smartphone are outside the DEDICAT 6G perimeter);
- Describe strategies about data storage;
- Provide data modelling. Please note that part of this data is partly scenario dependent.

The viewpoints used for the IV are 1) UML data flow diagrams and 2) UML data class/object modelling.

2.6.5 Network Deployment View

The *Network Deployment View* (NDV) aims at describing how FCs are physically deployed in both DEDICAT 6G cloud & edge, and alongside the 5G network architecture.

It is paramount when 1) describing the edge-computing aspects of the DEDICAT 6G system and its dynamic nature relying on complex decision making and 2) when elucidating how the DEDICAT 6G components interact with the 5G legacy components.

The main viewpoint will be an extension of the FV main viewpoints where edge devices and external entities are explicitly pictured alongside the typical: `Access -> Far Edge -> Edge -> Cloud` deployment.

Additional viewpoints are used to picture the deployment itself linked to technical use-cases as already done in the FV.

2.6.6 Instantiation View

This last view shows how the developed software components instantiates and deploy upon the DEDICAT 6G architecture. Because there is not a one-to-one mapping between logical FCs and developed components (usually several FCs are implemented in one bigger software component though the converse may happen as well) the instantiation view acts as an overlay to the functional view and shows how developed software concrete components map to the logical FCs resulting from the functional decomposition.

2.7 Introduction to the Architecture Perspectives

According to Rozanski & Woods, an architectural Perspective "is a collection of activities, tactics and guidelines that are used to ensure that a system exhibits a particular set of related quality properties that require consideration across a number of the system's architectural views" [7].

In this definition, a quality property is meant to be "an externally visible, non-functional property of a system such as performance, security or scalability" [7].

As we can see, architectural Perspectives are orthogonal to architectural Views; therefore, any architecture or design decision pertaining to non-functional or quality requirements often spans more than one architectural View, if not all.

Then we identify a comprehensive list of perspectives which are relevant for DEDICAT 6G. Each perspective focuses on specific non-functional requirements or desired quality properties of the architecture. The following list is a set of perspectives (already introduced shortly in Section 2.1.3 that can be of interest for DEDICAT 6G though probably not all will be eventually covered:

- **Evolution** (or Evolvability): is a quality of a system that has been designed in such a way it can easily be adapted to new technologies;
- **Interoperability**: ability of a system to easily interoperate with other systems at various levels like technical, syntactical, semantic and organizational;
- **Availability**: ability of a system to be fully (or partly) available when required;
- **Resilience**: ability of a system to effectively handle failure or attacks that could affect the system availability;
- **Privacy**, **Security** and **Trust**:
    - *Privacy*: ability of a system to deal with all kinds of personal data and in particular to implement reliably privacy policies about accessing, sharing that data or hiding people's identity;
    - *Security*: ability of the system to reliably control, monitor and audit who can perform what actions on what resources, to detect and recover from failures insecurity mechanisms and to resist to cyber attacks;
    - *Trust*: ability of a system to establish and enforce trusted relation between the different parties involved in a system (end-users, component, data) in such a way system operation and behaviours comply to expected ones;
- **Performance**: ability of a system to predictably perform its operations within its mandated performance requirements and profile;
- **Scalability**: ability of the system to cope with increasing demand in computing, networking, storage resulting from increasing volume of system usage;
- **Usability**: quality that illustrate how easy a system can be used, how easy data can be apprehended by the end-users, how easy the GUI is understandable and ergonomic while maintaining efficient work.

Of course, the list of qualities can be updated or adapted according to the architects' needs.

Each desired quality will be then associated with a set of activities (for instance activities associated with Trust, Security and Privacy are the collection of trust requirements, the conduction of risk and threat analysis, the definition of a trust model, etc.)

Then defining a certain number of tactics allows showing how the desired system quality can be eventually reached. Because a tactic can span more than one view, the implementation of a tactic through *Design CHoices* (DCH) can lead to more than one of those DCHs (e.g., a tactic for realizing Anonymity can lead to a collection of DCHs relating to Data Structure for the Information View and DCHs relating to interfaces, storage and security-related functionality in the Functional View).

As shown in Figure 4 below, architecture Perspectives (the grey horizontal boxes) are focusing on system properties/qualities and are orthogonal to the architecture Views. As a consequence, when deciding to consider a tactic that would allow the system to reach a desired quality, results in the definition and implementation of concrete DCHs that impact more than one view, if not all.

Figure 4: Architecture Views and Perspective

It is worth reminding that only the Privacy, Security and Trust Perspectives are dealt with in the first iteration of this document.

In the Perspective section of the DEDICAT 6G (Section 5) we will describe perspectives using a table structure as shown in Table 2 below[3]:

Table 2: Perspective description

Targeted System Quality	Describes the overall objectives of the considered perspective (say Privacy), considered as a Category. From the requirement analysis phase, we will come up with several objectives falling under one of the lists of perspectives (see above), each one of these objectives (say privacy related objective) will be declined into one or several **tactics** (say anonymisation, pseudonymisation, etc.), which can be considered as high-level DCH.
Requirement(s)	Gives the list of NFREQs concerned with that perspective.
Activities	Gives a list of activities needed when dealing with the perspective. It includes activities like: • Performing a threat analysis, • Performing system / network stress assessment, • Simulations, • Updating list of requirements, • Validating against requirement (especially for any NFREQ associated with performance thresholds), etc.
Tactics	Consists of a set of high-level abstract design choices that can be used to reach a desired property. Then each one of these tactics binds to a set of DCHs which relate to a particular view as explained earlier. Such DCHs can be: • Adopting certain algorithm; • Adopting specific deployment strategies; • Adopting a certain architecting choice; • Introducing specific FCs, etc.

As far as DCH description is concerned we will be using the following Table 3 structure:

[3] inspired from the IoT-A Architectural Reference Model [11]

Table 3: Example of Design Choice descriptions

Design Choice ID	View	FG/FC	Technical description
PRIV-01	FV	Security/ xyz FC	This component is responsible for…
PERF-01	NDV	n/a	In order to fulfill this desired quality, the deployment of….

3 DEDICAT 6G Requirement Engineering

As we mentioned in the introduction Section 2.4, the requirement engineering process is the sole purpose of Task 2.2. However, the results of the first activity of that task, namely Requirement Collection, are fed into two deliverables:

- D2.1: Scenario Requirements from the WP6 point of view (scenario work package);
- D2.2: Platform Requirements from WP3, 4 and 5 points of view (technical work packages).

It will be the purpose of the Section 3.2.1 to provide a list of platform requirements that translate the technical project ambitions as described in the DoA. Like for the Scenario requirements, platform requirements can be functional or non-functional. However, we also collect potentially additional new scenario requirements as explained later on.

It is worth reminding that the platform technical ambitions have been motivated after a thorough *State Of The Art* (SOTA) analysis applied to the corresponding technical fields. The SOTA conclusions are documented in the DEDICAT 6G DoA as a justification to our technical ambitions. Those platform requirements are a translation of those legitimate technical objectives.

The second activity takes all available requirements from the Requirement Collection phase and produces a list of *UNIfied requirements* (UNIs) (cf. Section 3.3). The unification process consists of aligning the vocabulary (the requirements are collected by various project partners with different technical backgrounds), identifying replicates, factorizing and rewriting. We also pay particular attention to identifying dependencies and possible conflicts, which need to be eventually dealt with.

Finally, the third requirement-related activity, namely requirement mapping map all requirements (resp. Functional, Non-Functional) to specific Views and FG/FC (FREQ), or/and perspectives (NFREQ).

Before delving into those specific requirement-engineering activities, it is worth reminding a special case that applies to Privacy, Security and Trust.

Traditionally, before elucidating requirements applying to those three system qualities, one usually engages first into a Threat Analysis, which –in a nutshell- aims at:

1. Evaluating the vulnerabilities of a system constituents;
2. Elucidating potential threats and attacks towards those identified vulnerabilities;
3. Assessing the impact of such threats and
4. Assessing the resulting impact.

Conducting a threat analysis prior (or at least in parallel) to requirement collection is crucial as its conclusions actually drive the identification of functional and non-functional requirement relating to Privacy, Security and Trust.

3.1 Threat Analysis

A threat analysis consists of understanding and identifying the assets to be protected, as well as identifying and evaluating possible threats. To assess the security of a system, we must look at all the possible risks and warnings. The STRIDE (Spoofing identity, Tampering with data, Repudiation threats, Information disclosure, (Distributed) Denial of service and Elevation of privileges) [4] model is a useful tool for threats classification.

A STRIDE analysis can be used in the early phase. A threat analysis based on an attacker's perspective was conducted to derive the hazard scenario. STRIDE is based on a reference architecture for determining the overall image of a system. The purpose of threat modelling is to understand how an attacker could penetrate the system.

The following Table 4 gives some examples of threats, their definition, potential scenarios and the counter-measure that could be undertaken in order to face the threat.

Table 4: STRIDE model with general scenarios and measures

Threat	Property Violated	Definition	Expected scenarios	Measures
Spoofing	Authentication	Impersonalizing something or someone else.	If the system user settings are not set properly, attackers might spoof them	Set the password appropriately: SSH Login with private key
Tampering	Integrity	Modifying data or code	If an illegal program has access to a cryptographic key or an encryption mechanism that holds the cryptographic key, the software replaced will misuse the real ID of device	MAC Applying a tamper-proof mechanism to the device
Repudiation	Accountability	Claiming to have not performed an action.	If the user does not have a log of the communication, it is likely to negate the fact of the operation that the user performed improperly	Acquisition and maintenance of various logs
Information disclosure	Confidentiality	Exposing information to someone not authorized to see it	The attacker exploits the encrypted key and obtains the encryption key and decryption key between nodes	Implemented Anti-malware, Secure Key Management
Denial of service	Availability	Deny or degrade Service to users	The function might be stopped if unauthorized access is performed over a network	Apply response limit
Elevation of privileges	Authorization	Gain capabilities without proper authorization	Allowing a user to run commands as admin	Restrict users who can get administrator rights

Threats are caused by attackers and result from the exploitation of various assets vulnerabilities which then become the target of such threats. The nature of a threat usually depends on the very nature of the targeted vulnerability. Using STRIDE enables analysis based on attributes such as confidentiality other than availability or integrity. Here follows a list of system elements and assets that must be protected:

- User workstations;
- Mobile devices and assets;
- Network devices (hubs, switches, routers, AP);
- Servers;
- Specialized devices;
- Software and services (OS, applications, client programs);
- Data (stored, archived, databases, data in-transit);
- Communications.

A list of possible threats targeting those general system elements and assets can be:

- Physical damage;
- Unauthorized access to data and services;
- Unauthorized disclosure of information;
- *Denial of service (DoS)*;
- Theft of data and services;
- Corruption of data and services;
- Viruses, worms, Trojan horses.

Focusing more on the networking aspects, possible network threats are for instance:

- Redirects the flow of data to attacker machine;
- Modifies data flowing over the network;
- IP and DNS spoofing;
- DNS compromise;
- Spoofing a user account;
- Spoofing a role.

The examples above are very general threats, however the DEDICAT 6G Threat Analysis (Table 5 and Table 6) shows that some of those general threats, in addition to more DEDICAT 6G-specific threats, need being considered.

Risk assessment relies very much on an appropriate preceding categorization and classification of threats. The result of the risk assessment procedure should be security requirements specification.

The Figure 5 below elucidates the process of risk assessment [4].

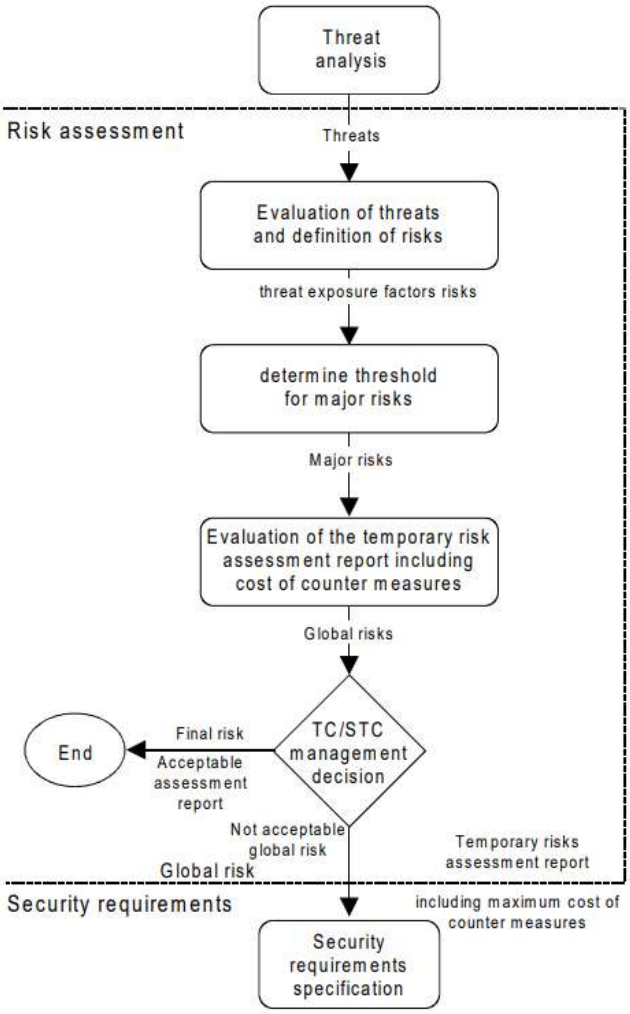


Figure 5: Methodology for risk assessment

Considering the nature of the DEDICAT 6G projects we have come up with the following general risk assessment (see Table 5).

Table 5: General risk definition and the assignment of evaluation values

Risks	Likelihood of occurrence	Potential impact
loss of integrity or confidentiality	High	High
data interception of signalling and user data	Low	Medium
Modifying data or code	Low	High
Hardware failure caused by cyber attack	Low	High
Data leaks	Low	Medium
loss of privacy	Medium	Medium
loss of availability of resources or service	Medium	High

Loss of trustworthiness to authorities	Low	Medium
Destruction of components	Medium	High
Installation of intentional malfunction, sabotage	Low	High

However, the **Table 6** below gives a much clearer focus on the physical systems (as described in **Table 15**) laying at the edge of the DEDICAT 6G platform. It provides the risk definition and assessment pertaining to those physical systems.

Table 6: Risk definition and the assignment of evaluation values to the Physical Systems

Physical system name	Risks	Likelihood of occurrence	Potential impact
Edge-terminal	• Loss of availability of resources or service • Destruction of components	• Low • Medium	• Medium • Medium
AGVs	• Loss of integrity or confidentiality • Hardware failure caused by cyber attack • Loss of availability of resources or service • Modifying data or code • Loss of trustworthiness • Installation of intentional malfunction, sabotage	• Low • Medium • Medium • Medium • Low • Low	• Medium • High • High • Medium • Low • High
Forklift/machine	• Hardware failure caused by cyber attack	• Medium	• High
SmartAccess360 controller	• Loss of integrity or confidentiality • Hardware failure caused by cyber attack • Loss of availability of resources or service • Modifying data or code • Loss of trustworthiness	• Low • Medium • Medium • Medium • Low	• Medium • High • High • Medium • Low
Warehouse personnel smartphone/mobile device	• Loss of availability of resources or service • Loss of integrity or confidentiality • Data leaks • Loss of privacy	• Medium • Low • Low • Medium	• High • Low • Medium • Medium
(B)5G Networking Equipment	• Loss of integrity or confidentiality • Hardware failure caused by cyber attack • Loss of availability of resources or service • Data leaks • Installation of intentional malfunction, sabotage	• Low • Medium • Medium • Low • Low	• Medium • High • High • Medium • High
Video streaming platform	• Loss of availability of resources or service • Modifying data or code • Loss of trustworthiness	• Medium • Medium • Low	• High • Medium • Low
Drones	• Loss of integrity or confidentiality • Hardware failure caused by cyber attack • Loss of availability of resources or service	• Low • Medium	• Medium • High

	• Data leaks • Loss of trustworthiness • Installation of intentional mal-function, sabotage	• Medium • Low • Low • Low	• High • Medium • Low • High
Smart phones	• Loss of availability of resources or service • Data leaks • Loss of privacy	• Medium • Low • Medium	• High • Medium • Medium
smartGlass	• Modifying data or code • Data leaks • Loss of privacy • Installation of intentional mal-function, sabotage	• Medium • Low • Medium • Low	• Medium • Medium • Medium • High
Connected Car (maybe different from UC1)	• Hardware failure caused by cyber attack • Loss of availability of resources or service	• Medium • Medium	• High • High
MCS mobile server	• Hardware failure caused by cyber attack • Loss of availability of resources or service • Modifying data or code • Data leaks	• Medium • Medium • Medium • Low	• High • High • Medium • Medium
Attendee smartphone	• Loss of integrity or confidentiality • Data leaks • Loss of privacy	• Low • Low • Medium	• Low • Medium • Medium
1st Responder smart phone	• Loss of availability of resources or service • Loss of integrity or confidentiality • Data leaks • Loss of privacy	• Medium • Low • Low • Medium	• High • Low • Medium • Medium
SmartGate	• Loss of integrity or confidentiality • Loss of trustworthiness • Installation of intentional mal-function, sabotage	• Low • Low • Low	• Low • Low • High
Smart vehicle	• Hardware failure caused by cyber attack • Loss of availability of resources or service • Modifying data or code	• Medium • Medium • Medium	• High • High • Medium
Smarter vehicle (incl. tablet-like terminal)	• Loss of availability of resources or service • Modifying data or code	• Medium • Medium	• High • Medium
IoT Nodes	• Loss of availability of resources or service • Modifying data or code • Data leaks	• Medium • Medium • Low	• High • Medium • Medium
RSU	• Data leaks	• Low	• Medium

As the very purpose of a risk analysis is to understand which threats a system needs to mitigate, the logical next step is to provide a list of security requirements.

It is worth mentioning here that the threat analysis in this document only focuses on security threats. Privacy and Trust are first handled in the requirement collection/analysis process and then dealt with in their respective perspectives (in Section 5).

Security requirements will be associated with the security features. Requirements must be implemented early in the development phase and the appropriate security features are mounted on the devices themselves.

The two following tables (respectively Table 7 and Table 8) give the list of general security requirements and also those applying to the DEDICAT 6G physical systems. Those requirements are fully embodied into the Privacy Security and Trust FREQ and NFREQ (see the unified requirements in Section 3.3, respectively Table 11 and Table 12)

Table 7: List of general security requirements

Security Requirement	Description
Access, Authentication, and Authorization Management	Authenticate users through central AuthN/AuthZ systems, grant the minimum, sufficient access, or privileges, employ role-based access controls, access sensitive data only as necessary for job duties, encrypt authentication and authorization mechanisms
Audit logging and analysis	Enable logging for endpoints, include essential events and elements in logs, restrict log access to authorized individuals, automate alerting on logging failures
Cryptography and key management	Protect digital assets and communications, implement GDPR, user/role access to the encryption keys
Network and data security	Implement default-deny, least-privilege policies on network devices, encrypt network traffic, securely configure network infrastructure devices
Code integrity	Validate the integrity of a component/driver or system file each time it is loaded into device memory, encrypt external transmission of data, Implement application logs with important event data
Data validation and sanitization	Validate on Input - ensuring that incoming data is uncompromised before it is allowed to be processed, sanitize device/storage media before transfer, Ensure sanitization methods meet the Standard's requirements

Table 8: List of security requirements for physical systems

Physical system name	Security Requirement
Edge-terminal	• Access, Authentication, and Authorization Management • Network and data security • Audit logging and analysis
AGVs	• Access, Authentication, and Authorization Management • Audit logging and analysis • Network and data security • Code integrity
Forklift/machine	• Access, Authentication, and Authorization Management
SmartAccess360 controller	• Access, Authentication, and Authorization Management • Audit logging and analysis • Cryptography and key management • Network and data security • Code integrity • Data validation and sanitization
Warehouse personnel smartphone / mobile device	• Access, Authentication, and Authorization Management • Audit logging and analysis • Data validation and sanitization

(B)5G Networking Equipment	• Access, Authentication, and Authorization Management • Audit logging and analysis • Cryptography and key management • Network and data security • Code integrity
Video streaming platform	• Audit logging and analysis • Code integrity
Drones	• Access, Authentication, and Authorization Management • Audit logging and analysis • Network and data security • Code integrity
Smart phones	• Access, Authentication, and Authorization Management • Audit logging and analysis • Data validation and sanitization
SmartGlass	• Access, Authentication, and Authorization Management • Audit logging and analysis
Connected Car (maybe different from UC1)	• Access, Authentication, and Authorization Management • Audit logging and analysis
MCS mobile server	• Access, Authentication, and Authorization Management • Audit logging and analysis • Network and data security • Code integrity • Data validation and sanitization
Attendee smartphone	• Access, Authentication, and Authorization Management • Audit logging and analysis
1st Responder smart phone	• Access, Authentication, and Authorization Management • Audit logging and analysis
SmartGate	• Access, Authentication, and Authorization Management • Audit logging and analysis
Smart vehicle	• Access, Authentication, and Authorization Management • Audit logging and analysis
Smarter vehicle (incl. tablet-like terminal)	• Access, Authentication, and Authorization Management • Audit logging and analysis
IoT Nodes	• Access, Authentication, and Authorization Management • Audit logging and analysis • Network and data security • Code integrity • Data validation and sanitization
RSU	• Audit logging and analysis

3.2 Requirement Collection

The requirement collection has indeed started in D2.1 with the collection of the **scenario-focused** requirements where the use-case holder takes the stance of a DEDICAT 6G customer deciding about 1) what are the needed functionalities (which features the targeted system must provide) and 2) overall system qualities (qualifying how the targeted system must behave).

Then another stance has to be taken, the platform provider's, in accordance with the technical objectives we have stated in the DoA [1]. Providing a list of functional (respectively non-functional) **platform-focused** requirements is the purpose of the next section.

As a reminder, The FREQs and NFREQs are split into two tables focusing on functional requirements on one hand and on non-functional & non-technical (e.g., Business or societal) requirements on the other hand.

In the following requirement tables, we have assigned a priority to the Non-Functional Requirements (NFREQ) and Functional Requirements (FREQ) where H(IGH), M(EDIUM), L(OW) correspond to the respective priorities. Therefore, the respective wording used to describe those requirements ought to use respectively "Must", "Should" and "Could".

It is also worth noting that assuming the iterative nature of the architecture development, the architecture main focus will be primarily on HIGH priority requirements, still trying to fulfill as many as possible of the lower priority ones in further architecture iterations.

3.2.1 Platform/System requirements

This section elucidates FREQs (Table 9) and NFREQs (Table 10) from the platform point of view (based on a technical analysis of the DoA technical objectives and challenges [1]).

3.2.1.1 Platform/System functional requirements

Table 9: List of platform functional requirements

ID	Category	Description	P	Rationale	Fit Criterion	Comment
PF3-1	Edge processing	The edge computing system shall provide a module specially devoted to host migration and distribution of intelligence algorithms. The module should support the hosting and execution of algorithms in multiple languages	H	Hosting and executing algorithms in a main functional component will reduce the load of the decision-making components	Software skeleton/framework designed to host and execute the multi-language algorithms	
PF3-2	Edge processing	The module shall offer a set of algorithms that can handle computation distribution/migration in B5G/6G unicast, multicast, broadcast traffic flows for both edge and datacenter levels	H	Solving problems related on migration and distribution of intelligence is essential to assist the Decision-Making FG	Set of algorithms on migration and distribution of intelligence written in several languages. The algorithms hosted will consider distributed, centralized and ML-based approaches to be suitable in all the scenarios where the platform will be applied	
PF3-3	Communication	The module shall have as many communication channels (interfaces) as needed to properly collect data to be used as input for the algorithms as well as notifying the decision-making agents	H	Set of interfaces and communication mechanisms to enable communication with external agents or components. The incoming data shall include information about applications requirements, computational resource availability in both fixed APs and MAPs (e.g., CPU, RAM or storage) nodes and information on MAPs geo-location, among others, and to communicate with the decision-making agents involved in the process of computational resources management, such as NVF Orchestrators, VIM/PoP managers or centralized database	Check interfaces in testing environment	

PF3-4	Context-awareness	The edge computing system must monitor the necessary metrics to provide enough information as input context to enable the execution of the MEC/VEC & V2X algorithms set	H	Providing the necessary data to the edge computing system is mandatory to feed the MEC/VEC & V2X algorithms to be used as inputs	Exemplary metrics: - Application analytics. E2E latency threshold, computational needs, bandwidth or connection life-time. - Computational resource availability and consumption in both fixed APs and MAPs (e.g., CPU, RAM or storage) nodes - Energy capacity, availability and consumption. MAPs battery life-time, Computing power consumption. - Positioning. APs and MAPs geolocation, charging platform location ranges or consumer devices positioning	Related to PNF3-2
PF3-5	Intelligence distribution	The system shall be able to make decisions on how intelligence should be distributed among nodes	H	The DEDICAT 6G system must be able to decide when it is required to perform distribution of intelligence processes (AI / DA / ML), which nodes should be used, which functions should be distributed to which nodes, etc.	Given a specific context and information on a set of functional entities/ fog applications, a set of available nodes that can act as edge entities, the corresponding network graph, cost parameters and respective weights (depending on info availability and service type) on energy consumption, data latency, computational latency and QoS requirements observe the system finding the optimal allocation of functional entities to network elements and nodes that satisfies all capacity and performance constraints, at minimum cost (energy, latency, etc.)	

PF3-6	Intelligence distribution	It must be possible to identify the need for (re-)distribution of intelligence through monitoring and analysis of what is happening in the network and the system as a whole	H	The DEDICAT 6G system needs to be capable of identifying needs and opportunities for intelligence distribution while relying on AGVs, Cars and mobile devices	Check based on defined experiments. Check that the system is able to infer the current system context/situation	
PF4-1	Coverage Extension	AGVs/Robots, Drones and other devices should be able to communicate with each other and with the "central" network infrastructure	H	This is required for setting up an ad-hoc network where an AGV/robot or drone may be playing the role of a MAP	Move MAP in an area without sufficient coverage and observe other nodes establish communication link towards the MAPs. MAP maintains access to core services	
PF4-2	Coverage Extension, Decision making	Decision making for coverage extension. The system must be able to make decisions on the creation, reconfiguration and termination of an ad-hoc coverage extension network. It will also reduce network management for infrastructure deployment	H	DEDICAT 6G system must be able to automatically decide on the creation, update and termination of ad-hoc networks for coverage extension and for auxiliary communication paths for critical system elements to enable uninterrupted access to key resources and services by all participating nodes. It must also ensure that the target KPIs are achieved for coverage extension. DEDICAT 6G will support application specific deployment and will define a self-organizing network (support of deactivation / activation of available innovative devices)	To trigger the coverage extension decision making mechanism and observe a mesh/ad-hoc network being formed. To change the conditions in the network or system that render the ad-hoc network as not useful anymore and observe its termination. Set one node to "leave" the network and observe the reconfiguration. Algorithms to find optimal placements for the MAPs and also be aware about their potential trajectories. Selection of docking/charging points for the MAPs when needed. Check that the network is able to self-organized itself	
PF4-3	Coverage extension	Relaying shall be supported by central nodes or by edge nodes	M	This will allow forwarding of data and control signalling in the scope of dynamic coverage	Check data propagation between end points (ping messages between points)	

				extension through an ad-hoc network		
PF4-4	Context-awareness,	The system must be able to monitor what is happening in the network and the system as a whole and must constantly infer what the current status is and whether decision making for coverage extension, intelligence distribution or security needs to be triggered. It must be possible to identify the need for a dynamic coverage extension through monitoring and analysis of what is happening in the network and the system as a whole	H	The system shall be able to obtain and monitor information on, application, service and network goals and objectives to be achieved, as well as potential policies. The system shall be able to monitor information on capabilities of network elements, MAPs and edge devices in terms of communication networking (e.g., *Radio Access Technologies* (RAT) and spectrum, capacity, and coverage), physical movement, the type of the MAP, computation capabilities, storage capabilities and available power. The system should maintain information and knowledge on the context that has to be addressed in terms of computation tasks, power consumption requirements, a set of mobile nodes that need coverage, mobility and traffic profiles of the different nodes, radio quality experienced by client nodes, options for connecting to wide area networks, the locations of docking and charging stations for drone and robot MAPs and the current locations of the terminals and MAPs elements. The system shall monitor coverage extension metrics (e.g., capacity that they offer, network availability) and MAP metrics (e.g., Battery status)	Check based on defined experiments. Check that the system is able to infer the current system context/situation	Monitoring and Analysis

				Moreover, the DEDICAT 6G system needs to be capable of identifying coverage extension needs and opportunities while relying on AGVs, Drones and Cars		
PF4-5	Coverage extension	Device and infrastructure capable to set-up connection	H	A device in an ad-hoc coverage extension network shall be able to set-up a connection with the central infrastructure. The infrastructure shall be able to trigger a device in an ad-hoc coverage extension network to set-up a connection. To provide connectivity, it is necessary to deploy some specific Virtual Network Functions and some specific interface to communicate with the NFV Orchestration, NFV-O (new requirement here) which is typically in charge of orchestrate the instantiation of the VNF in the devices is needed. Then, the computational resources of the device can be part of the NVF infrastructure in order to be manageable by the NFV-O	Check that a device in an ad-hoc network can ping the central infrastructure. Check that the infrastructure can trigger the device to set up a connection with other devices. Deploy VNFs and check orchestration	End-to-end connection
PF4-6	Coverage extension	More than one coverage extension networks shall be supported at the same time	H	Different ad-hoc networks established across shared nodes and in close vicinity must minimize mutual interference and share resources	Setup two ad-hoc networks and monitor communication performance metrics (delay, packet drop rate, throughput)	Several coverage extensions
PF4-7	Networking	The module shall offer the resource allocation including multi-connectivity configuration to adapt to dynamic environment	H	Solving problems related to QoS provisioning and dynamic coverage within a given radio resource. Considering varying channel conditions and traffic loads, the efficient resource allocation including multi-connectivity will be configured for UEs	An algorithm to dynamically configure multi-connectivity with ground fixed BS and mobile BS(s) and allocate radio resources to UEs	Support Dynamic environment

PF4-8	Coverage extension	The system must be able to monitor what is happening in the network and the system as a whole and must constantly infer what the current status is and whether decision making for coverage extension, intelligence distribution or security needs to be triggered	H	DEDICAT 6G will exploit MAP according to several mobility management agreements (Stationary, stationary during a period and nomadic, mobile within well-defined space, fully mobile with assistance, fully mobile without assistance…). Some levels of agreement could be defined DEDICAT 6G will consider devices with small battery limitation. DEDICAT 6G will also manage the lifecycle of MAP (charging, docking, moving, active mode, etc.) DEDICAT 6G system will make the inventory of the capacities of the AGV/drones for creating a "plan for the deployment" (e.g., depending on the devices that are available for the deployment, their capacity and the proximity to a charging point)	Evaluation of the performance gain according to the mobility class of the MAP Define the mechanisms to check the drones available and create a plan that calculates the time that the coverage extension will be supported	MAP Capabilities
PF4-9	Coverage Extension	Detect uncovered devices or low experienced QoS Users from the decision making or from the application		DEDICAT 6G will define additional strategies dedicated to network discovery. The decision can come from the decision making or directly from the application in case of public safety use-case	Evaluation of the latency to discover new devices (uncovered in the network)	Identification/detection of the need for coverage extension
PF4-10	Coverage Extension, Intelligence distribution	The system should command the *NFV Orchestrator* (NFV-O) in the deployment of the needed VNFs to enable connectivity when extending the connectivity		In most of 5G scenarios to provide connectivity is necessary to deploy some specific *Virtual Network Functions* (VNFs). To enable this capability, the computational resources of the AGVs, drones or robots have to be included as part of the *NFV Infrastructure* (NFV-I) to be handled and managed by the NFV-O. Then, the DEDICAT 6G platform	This functionality can be tested in two stages: i) interface testing: check that the recommendations are received by the NFV-O coming from the DEDICAT 6G platform; and ii) functionality testing: check that the recommendations are translated to the network	

				must command the NFV-O not only about what VNFs have to be deployed to enable connectivity (coverage extension), but also where to deploy them (intelligence distribution)		
PF5-1	Security	AI mechanism for threat detection and classification realized with federated learning approach taking advantage of edge processing and intelligence distribution	H	The security protection (threat identification and prevention) approach needs to take advantage of the intelligence distribution mechanisms provided by the project. Federated learning approach allows for globally defined ML models to be distributed closer to the data sources, perform updates/re-training on the collected data and report tuned parameters to the global model for further performance improvements	Federated learning mechanisms implemented (global model, metadata, APIs, data format and models, local model update policy, ML model performance metrics): one for each project use-case and threat detection scenario	
PF5-2	Security	Proactive mechanisms for threat prevention	M	The AI models for threat detection and classification should support proactive decision making, meaning that threat related policies should be supported with AI models which analyse and act on collected system logs.	AI models implemented in code and validated with collected datasets for each project use-case	PF5-4
PF5-3	Security	Reactive mechanisms for threat mitigation	H	DEDICAT 6G system needs to include AI mechanism which will identify and classify threats and incidents during the operation of DEDICAT 6G system instance. Each threat class will be mapped onto threat handling policy	Threat identification and classification mechanism with corresponding policies implemented in code	
PF5-4	Security	Attribute-based access control and identity management for all DEDICAT 6G components and actors	M	Attribute based access control will allow DEDICAT 6G system to include access control rules and policies configured for different classes of actors, devices and processes. More attributes	Attribute based access control and authorization levels implemented and validated for different classes of users, nodes and processes	

				included in the process will result in finer decision making with respect to access control		
PF5-5	Security	Deterministic and probabilistic behaviour analysis for systems and actors	M	DEDICAT 6G AI component for threat detection and classification relies on behaviour analysis during and after a DEDICAT 6G system instance lifecycle	ML models implemented for behaviour analysis and characterization.	
PF5-6	Security	Anomaly detection in sub-systems operation (e.g., IoT systems, robots, etc.) to ensure security of the system in use. Monitoring system behaviour to avoid any risks of hijacking or injection. System behaviour is monitored at three different layers, hardware-level, network-level and service-level	M	Detection of anomaly hardware behaviour of IoT systems / devices by finding abnormal patterns from the monitored data stream. At the network level, network behaviour will be monitored, and malicious communications will be detected. Based on the monitored communication, spread of threats/malwares could be predicted. At the service level, micro-services, which are combined to form a service, will be executed on a virtual machine. The anomaly service behaviour could be detected by monitoring such in-virtual-machine micro-services from outside of the virtual machine	Securing sub-systems that are participating in the overall system	
PF5-7	Security	Detect physical integrity status of deployed DEDICAT 6G systems	M	DEDICAT 6G system should be able to detect that deployed resources (edge processing nodes, AGVs/robots, drones, network and IoT equipment) have not been physically compromised by replacing storage, adding/removing communication interface or by other detectable system integrity changes	Implement system integrity check enabler for all field systems and perform tests by replacing system components and assessing if the DEDICAT 6G system detects/identifies changes	
PF5-8	Security	Access, Authentication, and Authorization Management	H	All DEDICAT 6G system components, participating nodes and users (admins, integrators, end-users) need to be authenticated	Implementation of best practice authentication and authorization mechanism following 5G standards. Check that authorization	

				and authorized with assigned access rights based on their role. This is the base AAA implementation on top of which attribute based access control can be established (see PF5-9)	levels are properly assigned to users based on predefined roles and access control policies.	
PF5-9	Security	Storage of logs of all transactions that took place during communication of system components and subsystems should be organized using secure and trustworthy blockchain technology	H	Storage of transaction logs, audits and other security-related information is needed to enable post-incident forensic research and threat analysis by AI threat detection components and human security experts. Blockchain will ensure that data is protected from deletion and modification	The solution that would proxy and store all the communication that takes place in DEDICAT 6G project	
PF5-10	Security	Automated threat detection model training based on stored transaction logs, session audits and reports data	M	If an incident has taken place, the system should be able to automatically train threat detection models using logs and audit data marked by security specialist as a malicious intrusion attempt or other security issue	Component that would allow automated threat detection model training and distribution of models across the edges	
PF5-11	Security, Trustworthiness	Automated incident reporting	M	DEDICAT 6G system should identify and report on any incident during instance lifecycle	Reports generated and sent to system administrators or stored in system backend	
PF5-12	Security, Trustworthiness	Trust management for federated learning model updates processes	M	Trust management mechanisms for federated learning procedures so that local model update and parameter reporting is done in trustworthy manner so that none of the local nodes can steer global model update in its malicious direction	Trust metrics implemented and realized as part of the trust management platform	
PF5-13	Security, Privacy	Encryption of data at rest	H	All sensitive information (privacy and business sensitive) stored in any location (edge, fog, core/cloud) must be encrypted using industry best practices. All databases and file storage systems must be protected from	Data encryption and database access mechanisms applied using industry best practices. Selection of tools to be documented in security and privacy protection plan. Periodic stress / breach	

				unauthorized access and manipulation	tests to be performed and reported	
PF5-14	Security, Privacy	Encryption of data in transit – end to end encryption	H	All information exchanged between DEDICAT 6G system entities and between DEDICAT 6G system and outside world, must be encrypted with industry best practice standards. All radio network access interfaces need to apply encryption while all data transfer between system elements (e.g., through APIs) needs to utilize encryption standards (e.g., https for REST APIs, other SSL/TLS approaches for data tunnelling through Internet)	Confirm that encryption is applied on all communication channels and interfaces. Exact standards to be used will be documented in security and privacy protection plan	
PF5-15	Trustworthiness	Trust management solution utilizing private permissioned blockchain as immutable record of transactions and smart contract executions	H	The private permissioned blockchain allows DEDICAT 6G project to configure and manage its blockchain network and ensure high performance transactions (read/write) needed for decision-making	Trust management platform based on private permissioned blockchain deployed using ChainRider tool for fast prototyping and deployment of private permissioned blockchains	
PF5-16	Trustworthiness	Trust management solution utilizing smart contracts for trustworthiness metrics and integration with DEDICAT 6G system components.	H	All interactions with the blockchain network are realized through smart contracts exposing REST APIs. Trustworthiness procedures interacting with the blockchain network will rely on smart contracts. Also, trustworthiness metric will be calculated, and their results will be written to blockchain through corresponding smart contracts	A collection of smart contracts with REST API implemented and available for configuration as part of the trust management platform	Different levels of device trustworthiness will be configured: relay node (only relaying encrypted information end extending range), bridge node (translating between systems and protocols), computation node (processing exchanged/collected data – including local federated learning entity), decision making node (acts on data analysis results) and orchestrator node (responsible for managing established networks). Each node type will have specific compliance test and will receive certificate which is updated

						based on performance of the node within networks
PF5-17	Trustworthiness	Automated compliance and trust certification for participating nodes and processes	H	Security and privacy protection attributes of each actor/process/node as well as incident reports will comprise trustworthiness metrics, which will be calculated and stored in blockchain. The result of this process will be certificates indicating the level of compliance (with common security and data protection KPIs) and trustworthiness so that decision making process can consider if a component to be included into a specific network/system/process can be trusted	Compliance test automation mechanism implemented per trustworthiness level and validated in project use-cases	
PF5-18	Trustworthiness	Calculation of trust metrics for all system components (HW and SW) and actors	H	The trustworthiness certificates will be based on trust metrics which, will be calculated with predefined set of parameters. The trustworthiness metrics will be calculated before, during and after node/actor participates in a DEDICAT 6G system instance	Implemented four trust metrics (device, connection, behaviour and context) and three trustworthiness mechanisms (device, service and data flow levels)	
PF5-19	Privacy	Threat detection mechanisms will be based on federated learning consequently boosting privacy protection by moving ML model training process to the source of data instead of transferring data to a centralized entity	H	Federated learning approach for threat detection will ensure that distributed ML models handle privacy sensitive data at the edge/source while centralized/global models receive only local model training parameters, and no privacy sensitive data is transferred to them	Analysing and comparing data collected and processed by local ML models against data that is available at the point of the global model	

3.2.1.2 Platform/System non-functional or non-technical requirements

Table 10: List of platform non-functional or non-technical requirements

ID	Category	Description	P	Rationale	Fit Criterion	Comment
PNF3-1	Interoperability	The edge computing system must export a server-client-based API to remotely manage the hosting and execution of algorithms in the migration and distribution of intelligence	M	Remote management provided by an API is essential to, first, assure interoperability in the hosting/execution of algorithms by different external actors, and second it may facilitate the development of algorithms that can be written in several programming languages regardless edge computing system implementation	Multi-client support	Related to PF3-1 and PF3-2
PNF3-2	Interoperability / Performance	Interfaces to enable the connectivity among the edge computing system and external agents should be established by using high-performance standardized communication mechanisms	M	High-performance standardized communication methods will ensure the interoperability in a distributed system and the ones based on micro services. Additionally, it may have impact in reducing the end-to-end latency, essential in a B5G/6G environment	Some example of potential communication options: JSON-over-HTTP (REST), gRPC, Kafka or RabbitMQ	Related to PF3-3 and PF3-4
PNF3-3,	Usability	The user perceived quality of service/quality of experience shall not be negatively affected by the dynamic coverage extension and intelligence distribution	H	The coverage extensions and distributed intelligence must improve or maintain perceived QoE and QoS in order to justify creation of ad-hoc opportunistic systems	We need project level fit criterion for user QoS and QoE assessment	
PNF4-1	Usability	The user perceived quality of service/quality of experience shall not be negatively affected by the dynamic	H	The coverage extensions and distributed intelligence must improve or maintain perceived QoE and QoS in order to justify	We need project level fit criterion for user QoS and QoE assessment	

		coverage extension and intelligence distribution		creation of ad-hoc opportunistic systems.		
PNF4-2	Usability	End-users shall not be involved in the processes for dynamic coverage extension, intelligence distribution and security, privacy and trust assurance	H	The system complexity should be hidden from the user	Check that coverage extension and intelligence redistribution is performed automatically without user intervention and that these processes are transparent to the user	
PNF4-3	Performance	The system shall ensure network performance such as a seamless mobility in the extended coverage, support of dynamic peak of demands, imperceptible end-to-end latency and fast response time, energy efficiency, reliability	H	DEDICAT 6G will ensure communication service continuity and seamless handover between fixed infrastructure AP and MAP DEDICAT 6G will dynamically deploy MAP according to the current traffic request. DEDICAT 6G will improve the latency and the responsiveness of the network by exploiting MAP DEDICAT 6G System with support (dis-)appearance or (dis)activation of AP (e.g., during disaster, during management of MAPs) DEDICAT 6G will ensure reliability with elastic network infrastructure	Monitor the Communication service availability, the Communication service reliability Check based on specific scenario (e.g., during attack terrorist, deploy MAP depending on the user location and where data is critical) Evaluate the end-to-end latency gain and compare latency through MAP and directly through fixed infrastructure	
PNF4-4	Fairness	The system shall provide equal opportunity to citizens and applications regardless location		DEDICAT 6G will ensure fairness between users and define some policies to manage heterogeneity of service	Map the performance according to the users position	
PNF5-1	Privacy	Privacy by design should be followed when designing and implementing DEDICAT 6G platform and use-cases	M	Data and privacy protection should be addressed and clearly indicated in all data transfer and storage procedures to be defined by the project	Security and privacy protection plan with related KPIs defined and referenced in technical reports	
PNF5-2	Privacy	Privacy categories should be introduced for data	M	All data to be collected, analysed and stored in the DEDICAT	Categories introduced in security and privacy protection	

		collected, analysed and stored by the DEDICAT 6G system		6G system and its instances should be put in predefined privacy sensitivity category with predefined privacy protection policy for that category including KPIs for proper data management	plan and referenced in all technical documentation where data flows are presented	
PNF5-3	Security	Security by design should be followed when designing and implementing DEDICAT 6G platform and use-cases	M	The security protection, system integrity and threat management should be addressed during DEDICAT 6G platform specification and instantiation in the use-cases	Security and privacy protection plan with related KPIs defined and referenced in technical reports	
PNF5-4	Security	Threat categorization for DEDICAT 6G system	H	All identified threats must be categories according to severity/impact and mapped onto threat management policy to be implemented and monitored	Security and privacy protection plan must include threat categories and mitigation measures – this should be referenced in all DEDICAT 6G system instances (use-cases)	
PNF5-5	Trustworthiness	Trust certification for devices, stakeholders and processes participating in DEDICAT 6G system and its instances	M	Each system component (SW and HW) and actor should have a valid trust certificate to be used when deciding to include it into DEDICAT 6G network/process/instance	Trust management plan will be produced including trustworthiness categories and methods for their assessment. Trust certificates will be implemented in a form of smart contracts stored in the DEDICAT 6G private permissioned blockchain	
PNF5-6	Reporting	Automated auditing and reports generation after each opportunistic network ends	M	AI system logs and incident reports are automatically collected and sent at the end of predefined cycle (or with lifecycle end for an opportunistic 6G network) to dedicated system entity performing their analysis and policy updates	Reports prepared and available for system administrators.	
PNF5-7	Security and privacy	Security and privacy protection plan for the DEDICAT 6G system	H	The project will establish and maintain security and privacy protection plan which, will be periodically updated based on the project progress and	Documented SPP periodically updated based on the project progress. It needs to be referenced in all technical use-cases	This is part of the DEDICAT 6G threat analysis process

				validation results in the use-cases. This plan will guide technical developments to follow defined security and data/privacy protection specifications and policies		
PNF5-8	Security	Physical security and tempering prevention for deployed DEDICAT 6G infrastructure	H	All deployed DEDICAT 6G resources and field equipment (access points, robots/AGVs, drones, IoT controllers etc.) must be secured from physical tempering. Set of physical security policies to be followed must be defined	Periodically inspect physical status of deployed systems in the scope of the project use-cases	
PNF5-9	Security	Ensure network security at all layers of the DEDICAT 6G system	H	DEDICAT 6G system and its deployments in the use-cases need to apply and address network security measures (firewalls, protection from DDoS attacks, security zones etc.) in order to prevent breaches and ensure proper execution of the specified security and data protection plan	Check networking equipment and firewall rules at each DEDICAT 6G use-case instance and in the cloud hosting platform level	

At this stage of the whole requirement process we have 1) two lists of unified scenario requirements and 2) two lists of platform requirements. We need now to unify all those requirements into two unique lists (one FREQ and one NFREQ).

3.3 Requirement Analysis

This next step of the requirement process, namely requirement analysis, consists of dealing with duplicates/redundancies, rewriting, alignment of vocabulary etc. the result of that analysis is embodied into the two following tables (FREQ in Table 11 and NFREQ in Table 12).

Note: a new column ("Link to") allows cross-referencing the requirements (ID) which each other when applicable.

3.3.1 Unified functional requirements (FREQ)

Table 11: List of Unified functional requirements

ID	Category	Description	P	Rationale	Fit Criterion	Link to	Origin / Comment
UF-1	Security	All DEDICAT 6G system components, participating nodes and users (admins, integrators, end-users) need to be authenticated and authorized with assigned access rights based on their role	H	This is the base AAA implementation on top of which attribute based access control can be established (see below)	Implementation of best practice authentication and authorization mechanism following 5G standards. Check that authorization levels are properly assigned to users based on predefined roles and access control policies	UF-2	PF5-8, SF-1, SF-2
UF-2	Security	Attribute based access control and identity management for all DEDICAT 6G components and actors	M	Attribute based access control will allow DEDICAT 6G system to include access control rules and policies configured for different classes of actors, devices and processes. More attributes included in the process will result in finer decision making with respect to access control	Attribute based access control and authorization levels implemented and validated for different classes of users, nodes and processes	UF-1	PF5-4, SF-1, SF-2
UF-3	Security, privacy, trust	Communication between all nodes shall be realized in a secure and trusted manner (if required) and must follow best practices in communication channel encryption	H	The system operation and configuration should be restricted to DEDICAT 6G staff only	Check based on experimental setup. We need project level fit criterion for this requirement		SF-5
UF-4	Security	It must be possible in certain circumstances to perform actuation upon an IoT actuator (e.g., a door lock) without relying on global communication (like Internet)	H	Have an option to access and utilize cyber-physical security systems like control of locks and alarms without access to central command (accessed through internet connection)	System interacts with mobile devices (e.g., smartphones) and performs authorized actuation (onboard relay trigger)		SF-7
UF-5	Security	A device or node must not be used for dynamic coverage extension or intelligence distribution without the approval of	H	Node/resource owners must be able to make decision about their resources and devices being utilized in local	Approve two out of three nodes and trigger coverage extension or intelligence redistribution and observe which nodes are involved in ad-hoc networks		SF-6

		the user/owner/operator of the device/node		ad-hoc networks with devices belonging to other users			
UF-6	Security, privacy	DEDICAT 6G must provide ways to protect private data stored in nodes partaking to DEDICAT 6G operation (e.g., network extension, edge computing…)	H	This needs to be enabled so that data obtained from a field node cannot be used in malicious manner	Check that data in local storage is encrypted with selected method		SF-8
UF-7	Security and privacy	Encryption of data at rest	H	All sensitive information (privacy and business sensitive) stored in any location (edge, fog, core/cloud) must be encrypted using industry best practices. All databases and file storage systems must be protected from unauthorized access and manipulation	Data encryption and database access mechanisms applied using industry best practices. Selection of tools to be documented in security and privacy protection plan. Periodic stress/breach tests to be performed and reported	UF-6	PF5-13
UF-8	Security and privacy	Encryption of data in transit – end to end encryption	H	All information exchanged between DEDICAT 6G system entities and between DEDICAT 6G system and outside world, must be encrypted with industry best practice standards. All radio network access interfaces need to apply encryption while all data transfer between system elements (e.g., through APIs) needs to utilize encryption standards (e.g., https for REST APIs, other SSL/TLS approaches for data tunnelling through Internet)	Confirm that encryption is applied on all communication channels and interfaces. Exact standards to be used will be documented in security and privacy protection plan	UF-3	PF5-14
UF-9	Log / Audit	Collection and storage of logs of all transactions that took place during communication of system components and subsystems should be organized using secure and trustworthy blockchain technology	H	Storage of transaction logs, audits and other security-related information is needed to enable post-incident forensic research and threat analysis by AI threat detection components and human security experts. Blockchain	Solution that would proxy and store all the communication that takes place in DEDICAT 6G project	UF-10	PF5-9

				will ensure that data is protected from deletion and modification			
UF-10	Log / Audit	Collecting performance logs from edge computing and communication nodes and systems in the backend. Local edge computing systems must be able to log performance of processes and resource utilization in every operational context	H	Locally deployed computation and communication systems must be able to perform monitoring of established emergency processes and act on collected information in line with pre-defined set of rules. Collected data is sent to central platform for performance analysis and updates for local decision-making models. Exact performance metrics will be defined within project	Access and completeness analysis of collected logs	UF-9	SF-9
UF-11	Log / Audit	Automated auditing and reports generation after each opportunistic network ends	M	AI system logs and incident reports are automatically collected and sent at the end of predefined cycle (or with lifecycle end for an opportunistic 6G network) to dedicated system entity performing their analysis and policy updates	Reports prepared and available for system administrators		PNF5-6
UF-12	Security	DEDICAT 6G should provide automated incident reporting and logging	M	DEDICAT 6G system should identify, report and log any incident during instance lifecycle	Reports generated and sent to system administrators or stored in system backend		PF5-11
UF-13	Security	DEDICAT 6G should provide proactive mechanisms for threat prevention	M	The AI models for threat detection and classification should support proactive decision making, meaning that threat related policies should be supported with AI models which analyse and act on collected system logs	AI models implemented in code and validated with collected datasets for each project use-case		PF5-2

UF-14	Security	DEDICAT 6G must provide reactive mechanisms for threat mitigation	H	DEDICAT 6G system needs to include AI mechanism which will identify and classify threats and incidents during the operation of DEDICAT 6G system instance. Each threat class will be mapped onto threat handling policy	Threat identification and classification mechanism with corresponding policies implemented in code		PF5-3
UF-15	Security	Automated threat detection model training based on stored transaction logs, session audits and reports data	M	If an incident has taken place, the system should be able to automatically train threat detection models using logs and audit data marked by security specialist as a malicious intrusion attempt or other security issue	Component that would allow automated threat detection model training and distribution of models across the edges		PF5-10
UF-16	Security	Threat detection mechanisms will be based on federated learning consequently boosting privacy protection by moving ML model training process to the source of data instead of transferring data to a centralized entity	H	Federated learning approach for threat detection will ensure that distributed ML models handle privacy sensitive data at the edge/source while centralized/global models receive only local model training parameters, and no privacy sensitive data is transferred to them	Analysing and comparing data collected and processed by local ML models against data that is available at the point of the global model		PF5-19
UF-17	Security	AI mechanism for threat detection and classification realized with federated learning approach taking advantage of edge processing and intelligence distribution	H	The security protection (threat identification and prevention) approach needs to take advantage of the intelligence distribution mechanisms provided by the project. Federated learning approach allows for globally defined ML models to be distributed closer to the data sources, perform updates/retraining on the collected data and report tuned parameters to the global model for further performance improvements	Federated learning mechanisms implemented (global model, metadata, APIs, data format and models, local model update policy, ML model performance metrics): one for each project use-case and threat detection scenario		PF5-1

UF-18	Security	DEDICAT 6G should be able to assess the physical integrity status of its deployed resources and detect those which are compromised	M	DEDICAT 6G system should be able to detect that deployed resources (edge processing nodes, AGVs/robots, drones, network and IoT equipment) have not be physically compromised by replacing storage, adding/removing communication interface or by other detectable system integrity changes	Implement system integrity check enabler for all field systems and perform tests by replacing system components and assessing if the DEDICAT 6G system detects/identifies changes		PF5-7
UF-19	Security	Deterministic and probabilistic behaviour analysis for systems and actors	M	DEDICAT 6G AI component for threat detection and classification relies on behaviour analysis during and after a DEDICAT 6G system instance lifecycle	ML models implemented for behaviour analysis and characterization	UF-20	PF5-5
UF-20	Security	Anomaly detection in sub-systems operation (e.g., IoT systems, robots, etc.) to ensure security of the system in use. Monitoring system behaviour to avoid any risks of hijacking or injection. System behaviour is monitored at three different layers, hardware-level, network-level and service-level	M	Detection of anomaly hardware behaviour of IoT systems/devices by finding abnormal patterns from the monitored data stream. At the network level, network behaviour will be monitored, and malicious communications will be detected. Based on the monitored communication, spread of threats/malwares could be predicted. At the service level, micro-services, which are combined to form a service, will be executed on a virtual machine. The anomaly service behaviour could be detected by monitoring such in-virtual-machine micro-services from outside of the virtual machine	Securing sub-systems that are participating in the overall system	UF-19	PF5-6
UF-21	Trust	It must be possible to assess and assign a level of trust to	H	Devices and services must establish and confirm trust	Trust metrics calculated and tested in experimental setups		SF3, SF-4

		each entity, node and actor participating to DEDICAT 6G operation. This trust level shall be based on a DEDICAT 6G dedicated metrics. In addition, it must be possible to access end-to-end trust based on those individual trust levels		before engaging in data exchange or any sort of interaction. Trustworthiness will be assessed with trust metrics (for devices, interfaces, users, processes, decisions, etc.) to be implemented within DEDICAT 6G trust management system			
UF-22	Security, Trustworthiness	Trust management for federated learning model updates processes	M	Trust management mechanisms for federated learning procedures so that local model update and parameter reporting is done in trustworthy manner so that none of the local nodes can steer global model update in its malicious direction	Trust metrics implemented and realized as part of the trust management platform		PF5-12
UF-23	Trustworthiness	Trust management solution utilizing private permissioned blockchain as immutable record of transactions and smart contract executions	H	The private permissioned blockchain allows DEDICAT 6G project to configure and manage its blockchain network and ensure high performance transactions (read/write) needed for decision making	Trust management platform based on private permissioned blockchain deployed using ChainRider tool for fast prototyping and deployment of private permissioned blockchains		PF5-15
UF-24	Trustworthiness	Trust management solution utilizing smart contracts for trustworthiness metrics and integration with DEDICAT 6G system components	H	All interactions with the blockchain network are realized through smart contracts exposing REST APIs. Trustworthiness procedures interacting with the blockchain network will rely on smart contracts. Also, trustworthiness metric will be calculated, and their results will be written to blockchain through corresponding smart contracts	A collection of smart contracts with REST API implemented and available for configuration as part of the trust management platform		PF5-16
UF-25	Trustworthiness	Calculation of trust metrics for all system components (H/W and S/W) and actors	H	The trustworthiness certificates will be based on trust metrics, which, will be	Implemented four trust metrics (device, connection, behaviour and context) and three		PF5-18

				calculated with predefined set of parameters. The trustworthiness metrics will be calculated before, during and after node/actor participates in a DEDICAT 6G system instance	trustworthiness mechanisms (device, service and data flow levels)		
UF-26	Trustworthiness	Automated compliance and trust certification for participating nodes and processes	H	Security and privacy protection attributes of each actor/process/node as well as incident reports will comprise trustworthiness metrics, which will be calculated and stored in blockchain. The result of this process will be certificates indicating the level of compliance (with common security and data protection KPIs) and trustworthiness so that decision making process can consider if a component to be included into a specific network/system/process can be trusted	Compliance test automation mechanism implemented per trustworthiness level and validated in project use-cases		PF5-17
UF-31	Context-awareness	The edge computing system must monitor the necessary metrics to provide enough information as input context to enable the execution of the MEC/VEC & V2X algorithms set	H	Providing the necessary data to the edge computing system is mandatory to feed the MEC/VEC & V2X algorithms to be used as inputs	Exemplary metrics: Application analytics. E2E latency threshold, computational needs, bandwidth or connection lifetime. - Computational resource availability and consumption in both fixed APs and MAPs (e.g., CPU, RAM or storage) nodes; - Energy capacity, availability and consumption. MAPs battery	UNF-24	PF3-4

					lifetime, Computing power consumption; - Positioning. APs and MAPs geolocation, charging platform location ranges or consumer devices positioning		
UF-32	Context awareness,	I The system must be able to monitor what is happening in the network and the system as a whole and must constantly infer what the current status is and whether decision making for coverage extension, intelligence distribution or security needs to be triggered. It must be possible to identify the need for a dynamic coverage extension through monitoring and analysis of what is happening in the network and the system as a whole	H	The system shall be able to obtain and monitor information on, application, service and network goals and objectives to be achieved, as well as potential policies. The system shall be able to monitor information on capabilities of network elements, MAPs and edge devices in terms of communication networking (e.g., *Radio Access Technologies* and spectrum, capacity, and coverage), physical movement, the type of the MAP, computation capabilities, storage capabilities and available power. The system should maintain information and knowledge on the context that has to be addressed in terms of computation tasks, power consumption requirements, a set of mobile nodes that need coverage, mobility and traffic profiles of the different nodes, radio quality experienced by client nodes, options for connecting to wide area networks, the locations of docking and charging stations for drone and robot MAPs and the current	Check based on defined experiments. Check that the system is able to infer the current system context/situation		PF4-4, SF-42

				locations of the terminals and MAPs elements. The system shall monitor coverage extension metrics (e.g., capacity that they offer, network availability) and MAP metrics (e.g., Battery status) Moreover, the DEDICAT 6G system needs to be capable of identifying coverage extension needs and opportunities while relying on AGVs, Drones and Cars			
UF-33	Context-Awareness	DEDICAT 6G must provide high precision indoor positioning performed with edge computing and utilizing fixed, mobile nodes and BLE beacons	H	The indoor positioning will be used for tracking mobile assets and for triggering safety rules based on proximity of tracked assets and personnel	DEDICAT 6G web dashboard displays precise location of tracked assets and personnel and their BLE beacons on the warehouse layout. Location precision is in radius of 1 meter		SF-43
UF-34	Context-Awareness	The car should be able to recognize the presence of a VRU via the LIDAR/camera	H	Detection of VRU is essential for increasing the road safety	VRU is detected within specified timing and range constraints		SF-44
UF-41	Communication	The module shall have as many communication channels (interfaces) as needed to properly collect data to be used as input for the algorithms as well as notifying the decision-making agents	H	Set of interfaces and communication mechanisms to enable communication with external agents or components. The incoming data shall include information about applications requirements, computational resource availability in both fixed APs and MAPs (e.g., CPU, RAM or storage) nodes and information on MAPs geo-location, among others, and to communicate with the decision-making	Set of interfaces and communication mechanisms to enable communication with external agents or components		PF3-3

				agents involved in the process of computational resources management, such as NVF Orchestrators, VIM / PoP managers or centralized database			
UF-51	Management/Monitoring	DEDICAT 6G web dashboard for administration of the system instances and monitoring performance metrics of DEDICAT 6G resources and services (metrics to be specified within project)	H	Web dashboard to be provided for administrating the overall DEDICAT 6G system, performance monitoring and maintenance. It can be specialized for specific stakeholders of the project use-cases	Web dashboard available on URL and tested in experimental setups		SF-10
UF-52	Management	DEDICAT 6G could provide a way to access incident log on demand through a dedicated dashboard	L	As part of the F of FCAPS	Trigger reporting procedure, receive test report and check its content		SF-11
UF-53	Management	DEDICAT 6G smart warehousing procedures can send push notifications to managers and personnel	H	Push notifications provide information on daily tasks, alerts and status of the DEDICAT 6G resources	Check that push notifications are delivered to DEDICAT 6G mobile application		SF-12
UF-54	Management	Configurable safety zones and parameters	H	IoT system needs to support configurable safety zones through web dashboard interface where digitalized warehouse layout is provided. These zones need to be configured by warehouse manager in line with operating context (e.g., offloading of dangerous products)	DEDICAT 6G web dashboard provides interface for safety zone configuration. IoT system monitors location/movement of mobile assets and personnel and sends triggers when a mobile asset or personnel member enters safety zone		SF-13
UF-55	Management	AGVs can be shut down remotely	M	Warehouse managers need to be able to remotely shut down AGV in case it is faulty in any way or in case energy needs to be reserved	Trigger AGV shutdown through web dashboard and observe AGV ceasing all operation.		SF-14
UF-56	Management	It must be possible to configure existing node in such a way they can be become part (or		New devices or piece of equipment can be added as candidate for intelligence	Check GUI		SF-15

		leave) of the DEDICAT 6G ecosystem		migration, edge networking or any other specific DEDICAT 6G operation			
UF-57	Management	The system must be able to be remotely controlled and configured	H	To allow testing and evaluation, the systems will be configured and controlled remotely	Checked that the system can be accessed remotely		SF-16
UF-58	Management	Remote access to deployed DEDICAT 6G resources and equipment must be enabled	H	Warehouse managers must be able to manage deployed resources (AGVs, IoT system) remotely with minimal latency	Warehouse manager sends command (e.g., make sound signal) to AGV through web dashboard accessed over Internet. Warehouse manager can trigger onboard relays of IoT controllers remotely – door opens		SF-17
UF-61	MMI	DEDICAT 6G mobile app for configuring and utilizing the deployed solution instance. Used by warehouse personnel and management	H	Mobile app to be developed to support smart warehousing use-case. It will be the main interface through which end-users interact with the system	Mobile app published and tested in experimental setups		SF-45
UF-62	MMI	AR interface for smart warehouse use-case for mobile apps	H	Smart warehouse use-case scenarios require AR interface for realization of the objectives. This interface will be part of DEDICAT 6G mobile application	AR interface implemented as part of DEDICAT 6G mobile app and tested in experimental setups		SF-46
UF-63	MMI	The Smart Glasses must display vital and essential information to the bearer amid crisis management	H	During crisis management visualizing essential information must be possible without hand manipulation of the smart phone	Vital and essential information, as described in the final users' requirements document, are displayed on the Smart Glasses		SF-47
UF-64	MMI	The Smart Glasses must be fully integrated with the overall system and interfaced with the smart phone	H	Indeed, a rescuer or first responder is connected with the DEDICAT 6G platform with the smart phone	The Smart Glasses device is connected to the user's Smartphone device Information displayed on Smart Glasses is duplicated on Smartphone device		SF-48

UF-65	MMI	The car must be able to warn the driver about the presence of a VRU on an HMI	H	The driver must get a visual warning when VRU is present	Check that the driver can get a warning about VRU presence		SF-49
UF-66	MMI	The system must be able to present information on the presence of a car to the VRU	H	The VRU must be warned when a car is on a colliding path.	Checked that the VRU is warned when a car is on a colliding path		SF-50
UF-71	Edge processing	The edge computing system must provide a module specially devoted to host migration and distribution of intelligence algorithms	H	Hosting and executing algorithms in a main functional component will reduce the load of the decision-making components	Software skeleton/framework designed to host and execute the multi-language algorithms		PF3-1 The module should support the hosting and execution of algorithms in multiple languages.
UF-72	Edge processing	The module shall offer a set of algorithms that can handle computation distribution/migration in B5G/6G unicast, multicast, broadcast traffic flows for both edge and datacenter levels	H	Solving problems related on migration and distribution of intelligence is essential to assist the Decision-Making FG. The algorithms hosted will consider distributed, centralized and ML-based approaches to be suitable in all the scenarios where the platform will be applied	Set of algorithms on migration and distribution of intelligence written in several languages		PF3-2
UF-73	Edge processing	AGV performs edge processing for self navigation and interaction with personnel and warehouse systems	H	AGV will act as a mobile computing node capable of analyzing collected information and making decisions in context of smart warehouse operation and DEDICAT 6G system operation	Software developed and deployed. Data analysis and decision-making algorithms implemented in code as part of AGV firmware/subsystem		SF-20
UF-74	Edge processing	DEDICAT 6G mobile app performs processing necessary for AR interface	M	DEDICAT 6G mobile app should be able to perform data analysis processes and decision making by using computing and data storage resources of mobile devices (smartphone or tablet) on which it is deployed. This way the AR features can be	Check in experimental setup. Mobile app installed on a mobile device and check that it is capable of performing implemented ML tasks required for AR functionality		SF-21

				supported with and without access to centralized services			
UF-75	Edge Computing	Gait analysis for attendees must be operated at the attendee's UE side	H	Abnormal Crowd movement detection is based on individual gait analysis and must be handled at the edge to minimize both bandwidth consumption and computation utilization at the cloud side	Crowd movement detection performs as expected		SF-24
UF-76	Edge Computing	DEDICAT 6G must provide Context-aware Decision-making algorithms to support and enable the dynamic migration of intelligence towards the edge, when it is required (like cars, drones, AGVs) Those mechanisms must consider which nodes should be used, which functions should be distributed to which nodes, etc.)	H	DEDICAT 6G system must run algorithms for load balancing decision making in order to balance workload between the cloud and edges depending on context and policies. Given a specific context and information on a set of functional entities/ fog applications, a set of available nodes that can act as edge entities (SE), the corresponding network graph, cost parameters and respective weights (depending on info availability and service type) on energy consumption, data latency, computational latency and QoS requirements observe the system finding the optimal allocation of functional entities to network elements and nodes that satisfies all capacity and performance constraints, at minimum cost (energy, latency, etc.)	Check that trigger is properly recognized. We need project level fit-criterion for identifying the need for redistribution of intelligence Check in experimental set-up		SF-25, SF-22, SF-23, PF3-6, PF3-5
UF-77	Edge Computing	IoT controllers perform edge processing and decision making for indoor positioning and	H	Deployed IoT system should include edge IoT controllers capable of performing data analysis and decision making	Software developed and deployed. Data analysis and decision-making algorithms		SF-26

		monitoring of environmental parameters		in context of smart warehouse operation and DEDICAT 6G system operation. Edge IoT controllers will allow smart warehousing operation to be performed with and without support or access to the server side processes	implemented in code as part of IoT controller's firmware/subsystem		
UF-81	Decision Making	DEDICAT 6G must provide context-aware decision-making algorithm based on a variety of context data (networking, load, performance, QoS, loss of service, weather-related, etc.)	H	DEDICAT 6G system needs to be able to provide decisions / alerts / notifications based on results of analysis of collected data at various levels in the whole system	Emulate sensory data out of predefined range and observe decision making algorithms result in triggering event		SF-27
UF-82	Decision Making	DEDICAT 6G should provide algorithm that recalculate AGV route according to changes in warehouse layout	M	AGVs need to adapt to changes in warehouse layout as result of offloading and placement of products – dynamic obstacles. Precise indoor positioning will be used to feed the algorithm	Set mobility route (point A to point B) for AGV, put obstacle on the rout and monitor AGV ability to reach destination without manual reconfiguration		SF-28
UF-83	Decision Making	Crowd Movement analysis must be provided in order to trigger emergency response	H	Natural disaster or terror attack generally results in hectic crowd movements	Such simulated crowd movements are detected		SF-29
UF-91	Networking	The module shall offer the resource allocation including multi-connectivity configuration to adapt to dynamic environment	H	Solving problems related on QoS provisioning and dynamic coverage within a given radio resource. Considering varying channel conditions and traffic loads, the efficient resource allocation including multi-connectivity will be configured for UEs	An algorithm to dynamically configure multi-connectivity with ground fixed BS and mobile BS(s) and allocate radio resources to UEs		PF4-7 Support Dynamic environment
UF-92	Networking	IoT controllers should be able to reach servers/cloud system through auxiliary communication paths	M	If a direct communication channel (wired or wireless) between IoT controller and IoT system server/cloud is disabled or overloaded, the	Disconnect/ disable primary interface and observe that IoT controller is able to connect with the cloud system		SF-30

				controller should be able to utilize local wireless communication network to reach a node with access to the Internet/cloud services			
UF-93	Networking	A vehicle or device in the proximity of the MAP should be able to receive information transmitted by the MAP. Thus, these should be in the same network	H	A vehicle in specific proximity of the roundabout should be able to receive information	It is tested that information can be received in a specific proximity from the MAP		SF-31
UF-94	Networking, Load balancing	The live streaming from the event to multiple simultaneous users relying on the ability to dynamically switch from unicast to multicast	H	The mobile multicast feature usage needs support from the operating network and requires guaranteed input throughput and latency. According to number of simultaneous users' handover from unicast to multicast is done for bandwidth savings	BMSC server messages help to resolve possible interoperability issues. A decrease in mobile data traffic will be monitored and measured		SF-32
UF-95	Networking, Load balancing	When UE devices support the multi-connectivity feature, UE association solution is required to fully utilized network resources	H	Depending on a given condition (including the traffic congestion levels of networks, channel conditions, etc.), UE can be connected to networks via multiple links at the same time (e.g., a MAP and macro-BS)	Measured: The efficiency of load balancing will be derived from the measured network performance		SF-33
UF-101	Coverage Extension	AGVs/Robots, Drones and other devices should be able to communicate with each other and with the "central" network infrastructure	H	This is required for setting up an ad-hoc network where an AGV/robot or drone may be playing the role of a MAP	Move MAP in an area without sufficient coverage and observe other nodes establish communication link towards the MAPs. MAP maintains access to core services		PF4-1, SF-37 MAP to MAP/I Communications
UF-102	Coverage Extension, Decision making	Decision making for coverage extension. The system must be able to make decisions on the creation, reconfiguration and termination of an ad-hoc coverage extension network. It	H	DEDICAT 6G system must be able to automatically decide on the creation, update and termination of ad-hoc networks for coverage extension and for auxiliary	Trigger the coverage extension decision making mechanism and observe a mesh/ad-hoc network being formed. Change the conditions in the network or system that render the ad-hoc		PF4-2

		will also reduce network management for infrastructure deployment		communication paths for critical system elements to enable uninterrupted access to key resources and services by all participating nodes. It must also ensure that the target KPIs are achieved for coverage extension. DEDICAT 6G will support application specific deployment and will define a self-organizing network (support of deactivation/activation of available innovative devices)	network as not useful anymore and observe its termination. Set one node to "leave" the network and observe the reconfiguration. Algorithms to find optimal placements for the MAPs and be aware about their potential trajectories. Selection of docking/charging points for the MAPs when needed Check that the network is able to self-organized		
UF-103	Coverage extension	Relaying shall be supported by central nodes or by edge nodes	M	This will allow forwarding of data and control signalling in the scope of dynamic coverage extension through an ad-hoc network	Check data propagation between end points (ping messages between points)		PF4-3, SF-39 Backhauling with Relaying
UF-104	Coverage extension	A device in an ad-hoc coverage extension network must be able to set-up a connection with the central infrastructure. The infrastructure must be able to trigger a device in an ad-hoc coverage extension network to set-up a connection	H	To provide connectivity, it is necessary to deploy some specific Virtual Network Functions and some specific interface to communicate with the NFV Orchestration, NFV-O (new requirement here) which is typically in charge of orchestrate the instantiation of the VNF in the devices is needed. Then, the computational resources of the device can be part of the NFV infrastructure in order to be manageable by the NFV-O	Check that a device in an ad-hoc network can ping the central infrastructure. Check that the infrastructure can trigger the device to set up a connection with other devices. Deploy VNFs and check orchestration		PF4-5, SF-38 End-to-end connection
UF-105	Coverage extension	More than one coverage extension networks could be supported at the same time	L	Different ad-hoc networks established across shared nodes and in close vicinity could minimize mutual interference and share resources	Setup two ad-hoc networks and monitor communication performance metrics (delay, packet drop rate, throughput)		PF4-6, SF40 Several coverage extensions

UF-106	Coverage extension	The Decision Making for Coverage extension (creation/update/termination) must be based on different sorts of contexts build-up from the information flowing to the Context-Awareness components. Including capabilities, autonomy and status of MAP, location of docking stations, etc.	H	DEDICAT 6G will exploit MAP according to several mobility management agreement (Stationary, stationary during a period and nomadic, mobile within well-defined space, fully mobile with assistance, fully mobile without assistance…). Some levels of agreement could be defined	Evaluation of the performance gain according to the mobility class of the MAP Define the mechanisms to check the drones available and create a plan that calculates the time that the coverage extension will be supported. Move AGV in warehouse area without fixed wireless network (the main network used within warehouse) coverage and observe other communication nodes establish communication link towards the AGV. AGV maintains access to core services		PF4-8, SF-35, SF-34 MAP Capabilities
UF-107	Coverage Extension	The system could detect uncovered devices or low experienced QoS Users from the decision making or from the application	L	DEDICAT 6G will define additional strategies dedicated to network discovery. The decision can come from the decision making or directly from the application in case of public safety use-case	Evaluation of the latency to discover new devices (uncovered in the network)		PF4-9
UF-108	Coverage Extension, Intelligence distribution	The system should command the NFV Orchestrator (NFV-O) in the deployment of the needed VNFs to enable connectivity when extending the connectivity	M	In most of 5G scenarios to provide connectivity is necessary to deploy some specific *Virtual Network Functions* (VNFs). To enable this capability, the computational resources of the AGVs, drones or robots have to be included as part of the *NFV Infrastructure* (NFV-I) to be handled and managed by the NFV-O. Then, the DEDICAT 6G platform must command the NFV-O not only about what VNFs have to be deployed to	This functionality can be tested in two stages: 1) interface testing: check that the recommendations are received by the NFV-O coming from the DEDICAT 6G platform; and 2) functionality testing: check that the recommendations are translated to the network		PF4-10 An interface DEDICAT 6G - NFV-O has to be assumed to permit recommendations in the NFV part of the network.

				enable connectivity (coverage extension), but also where to deploy them (intelligence distribution)			
UF-109	Coverage Extension	DEDICAT 6G could be able to determine the optimal geographical distribution of MAP when initiating network coverage extension, according to the current context	L	MAPs positions will impact on various network performance (e.g., the num. of served UEs, sum data rate, spectral efficiency, energy efficiency, etc.)	Measured: When the locations of heavy data traffic generation vary over time, whether MAPs position can be decided		SF-41
UF-110	Coverage Extension.	In some circumstances the coverage extension must be self-organized without help from cloud-based mechanisms	H	During crisis management there is no time and qualified tech for network configuration	Ad-hoc network performs as expected and bear the load		SF-36

3.3.2 Unified Non-Functional and Non-Technical Requirements (NFREQ)

Table 12: List of Unified Non-Functional and Non-Technical Requirements

ID	Category	Description	P	Rationale	Fit Criterion	Link To	Comment
UNF-1	Usability	The user perceived quality of service/quality of experience shall not be negatively affected by the dynamic coverage extension and intelligence distribution	H	The coverage extensions and distributed intelligence must improve or maintain perceived QoE and QoS in order to justify creation of ad-hoc opportunistic systems	We need project level fit criterion for user QoS and QoE assessment		PNF3-3, PNF4-1
UNF-2	Usability	End-users shall not be involved in the processes for dynamic coverage extension, intelligence distribution and security, privacy and trust assurance	H	The system complexity should be hidden from the user	Check that coverage extension and intelligence redistribution is performed automatically without user intervention and that these processes are transparent to the user		PNF4-2
UNF-3	Usability	End-users must not be involved in the processes for dynamic coverage extension, intelligence distribution and security, privacy and trust assurance	H	The system complexity should be hidden from the user	Check that coverage extension and intelligence redistribution is performed automatically without user intervention and that these processes are transparent to the user		SNF-18

UNF-11	Fairness	The system should provide equal opportunity to citizens and applications regardless location	M	DEDICAT 6G should ensure fairness between users and define some policies to manage heterogeneity of service	Map the performance according to the users position		PNF4-4
UNF-21	Interoperability	The edge computing system must export a server-client-based API to remotely manage the hosting and execution of algorithms in the migration and distribution of intelligence	M	Remote management provided by an API is essential to, first, assure interoperability in the hosting/execution of algorithms by different external actors, and second it may facilitate the development of algorithms that can be written in several programming languages regardless edge computing system implementation	Multi-client support		PNF3-1 Related to PF3-1 and PF3-2
UNF-22	Interoperability	DEDICAT 6G should be able to interface with selected systems already deployed in locations where use-cases are realized	M	Interfacing can be done through existing APIs, control points, databases etc. Interoperability with key services and resources already deployed in a warehouse is needed	Integration completed and tested with message exchanges between end points		SNF-19
UNF-23	Interoperability	The technology promoted by DEDICAT 6G to supporting dynamic edge computing, should ensure that it is deployable and interoperable with **any** Edge node	M	To support the load balancing requirement, applications should be able to be run by any nodes	VRU Application components can be executed on RSUs and vehicles, independent of software and hardware architectures		SNF-20
UNF-24	Interoperability, performance	Interfaces to enable the connectivity among the edge computing system and external agents should be established by using high-performance standardized communication mechanisms	M	High-performance standardized communication methods will ensure the interoperability in a distributed system and the ones based on micro-services. Additionally, it may have impact in reducing the end-to-end latency, essential in a B5G/6G environment	Some example of potential communication options: JSON-over-HTTP (REST), grips, Kafka or RabbitMQ		PNF3-2 Related to PF3-3 and PF3-4

UNF-31	Scalability, Interoperability	DEDICAT 6G should be designed in such a way interoperability with new IT system or equipment is possible and minimized in term of cost	M	It should be able to elect new IT system or pieces of equipment as part of the cloud architecture or as part of the edge, e.g., new drones, robots from different providers	Field trial based on interface documentation and architecture document		SNF-22
UNF-32	Scalability	The specific solutions developed amid the different DEDICAT 6G scenarios must encourage minimum configuration time in order to maximize applicability/reuse in different contexts	H	It is important that solutions developed for e.g., one smart warehouse, one smart Highway configuration or a specific event can be deployed easily to a different smart warehouse, different highway or event, with minimum re-configurations	Still to be defined		SNF-21
UNF-41	Performance	The system shall ensure network performance such as a seamless mobility in the extended coverage, support of dynamic peak of demands, imperceptible end-to-end latency and fast response time, energy efficiency, reliability	H	DEDICAT 6G will ensure communication service continuity and seamless handover between fixed infrastructure AP and MAP. DEDICAT 6G will dynamically deploy MAP according to the current traffic request. DEDICAT 6G will improve the latency and the responsiveness of the network by exploiting MAP DEDICAT 6G System with support (dis-)appearance or (dis)activation of AP (e.g., during disaster, during management of MAPs) DEDICAT 6G will ensure reliability with elastic network infrastructure	Monitor the Communication service availability, the communication service reliability, Check based on specific scenario (e.g., during attack terrorist, deploy MAP depending on the user location and where data is critical) Evaluate the end to end latency gain and compare latency through MAP and directly through fixed infrastructure		PNF4-3

UNF-42	Deployment, Performance	On loss of network infrastructure after a natural disaster, the DEDICAT 6G infrastructure should be deployed as fast as possible	M	Depending on publication and reports on disaster response, the deployment of DEDICAT 6G shall be faster than legacy solution (divided by 2)	Evaluation of deployment time during recovery phase. Results should improve Response Times during the Recovery phase compared to legacy methods		SNF-23
UNF-43	Performance	The system should be able to balance load distributed on the edge nodes	M	To avoid too much load on specific devices, especially when computing power is limited	Load distribution should happen within application-specific timing constraints		SNF-11
UNF-44	Performance	The user perceived quality of service/quality of experience shall not be negatively affected by the dynamic coverage extension and intelligence distribution	H	The coverage extensions and distributed intelligence must improve or maintain perceived QoE and QoS in order to justify creation of ad-hoc opportunistic systems	We need project level fit criterion for user QoS and QoE assessment		SNF-12
UNF-45	Performance	Critical communication shall not be decreased when DEDICAT 6G is deployed on the scene	H	Based on legacy and 5G specifications, the average time to response has to be equal or less than existing specification in 3GPP Mission Critical (MCX) standards	Measure the latency between UE during a MC-PTT call. The time shall not be decreased		SNF-13
UNF-46	Performance	On multiple connection, the system has to support the QoS and shall not decrease during crisis management	M	When the worst happened, the Quality of Services shall keep similar value compared to 3GPP MCS standards in any cases	Measure of QoS. QoS measured shall not be decreased regarding the 3GPP MCS standards		SNF-14
UNF-47	Performance	Latency for Crowd movement analysis must be reasonably low (e.g., a few seconds max)	H	Casualty count can depend on the response time	Measured		SNF-15
UNF-48	Performance	DEDICAT 6G must provide reliable communication	H	Communication between all the devices in all circumstances should be high reliable (99.999%)	No loss of information should be occurred between actors and no delays in the communication due to instable situations		SNF-16
UNF-49	Performance	DEDICAT 6G must provide overall performance metrics and implement mechanisms that can assess the platform performance against those metrics	H	How the DEDICAT 6G system or sub-system performs, what succeeded and what did not	Pass/Fail criteria		SNF-17

UNF-51	Privacy	Privacy by design should be followed when designing and implementing DEDICAT 6G platform and use-cases	M	Data and privacy protection should be addressed and clearly indicated in all data transfer and storage procedures to be defined by the project	Security and privacy protection plan with related KPIs defined and referenced in technical reports		PNF5-1
UNF-52	Privacy	Privacy categories should be introduced for data collected, analysed and stored by the DEDICAT 6G system	M	All data to be collected, analysed and stored in the DEDICAT 6G system and its instances should be put in predefined privacy sensitivity category with predefined privacy protection policy for that category including KPIs for proper data management	Categories introduced in security and privacy protection plan and referenced in all technical documentation where data flows are presented		PNF5-2
UNF-53	Privacy	Privacy sensitive information from personnel must be anonymized when stored and processed	H	Privacy protection must be ensured with best practice approaches for anonymization of the personally identifiable information when transferred and stored	Check data collected at source (personal data) and check data when stored in database – confirm that data is anonymized		SNF-1
UNF-54	Privacy	The system should keep a log of places, moments and trajectories where personal data is compiled, transferred, stored, deleted, anonymized (or pseudonymized) or processed in any other way	H	This is important for privacy and data protection audits that can be requested by regulatory bodies	Setup logging procedure, generate logs and check their completeness in different experimental setups		SNF-5
UNF-55	Privacy	Depending on the context, it should be able to decide where and whether certain data can be stored depending on its very nature (private, sensitive, classified etc.)	M	Warehouse managers can select data that need to remain within warehouse logical perimeter and not transferred to 3rd parties. Event organizer may forbid the storage of live stream videos	Check depending on context and associated policy		SNF-2
UNF-56	Privacy, ethnics	DEDICAT 6G must provide mechanism for handling selected privacy issues using Consent Forms (e.g., amid the various Android Apps used in	H	In certain circumstances it may be very difficult or even impossible to guaranty full privacy without asking for formal permission. In other	Compliance to regulations		SNF-6

		the project) and Term & Condition		cases, the use, transfer and storage of personal data may also require user's permission (this does not prevent the use of anonymization and encryption)			
UNF-57	Privacy, Ethics	DEDICAT 6G must provide mechanisms that enforces data usage policies (use of Term & Condition forms, nonrepudiation, accountability, etc.)	H	Data potentially captured or exchange may be subject to restriction or even may be forbidden by event organizers			SNF-7
UNF-58	Privacy, ethics	Position information of road users must be collected for locating the nodes in the map and must be handled in such a way the privacy of the user is maintained	H	App displayed on the HMI of the UEs must continuously gather location information of the users	Compliance to regulation		SNF-8
UNF-59	Privacy, Ethics	Video feed should be collected by cameras on the car and their treatment should comply to regulation	M	Camera on the car will continuously record the situation at the intersection	Compliance to regulation		SNF-9
UNF-61	Ethics	The system shall follow appropriate health and safety procedures conforming to relevant local/national/EU guidelines/legislation in order to protect the environment and people	H	Health and safety procedures need to be translated into system automation and decision-making processes provided by DEDICAT 6G system	Translate selected regulation into specific set of automation and decision-making rules. Confirm completeness		SNF-3
UNF-62	Ethics	The system shall include measures and tools to safeguard from misuse of data collected in alignment with the GDPR	H				SNF-4
UNF-71	Security	Security by design should be followed when designing and implementing DEDICAT 6G platform and use-cases	M	The security protection, system integrity and threat management should be addressed during DEDICAT 6G	Security and privacy protection plan with related KPIs defined and referenced in technical reports		PNF5-3

				platform specification and instantiation in the use-cases			
UNF-72	Security	Threat categorization for DEDICAT 6G system	H	All identified threats must be categories according to severity/impact and mapped onto threat management policy to be implemented and monitored	Security and privacy protection plan must include threat categories and mitigation measures – this should be referenced in all DEDICAT 6G system instances (use-cases)		PNF5-4
UNF-73	Security	Physical security and tempering prevention for deployed DEDICAT 6G infrastructure	H	All deployed DEDICAT 6G resources and field equipment (access points, robots/AGVs, drones, IoT controllers etc.) must be secured from physical tempering. Set of physical security policies to be followed must be defined	Periodically inspect physical status of deployed systems in the scope of the project use-cases		PNF5-8
UNF-74	Security	Ensure network security at all layers of the DEDICAT 6G system	H	DEDICAT 6G system and its deployments in the use-cases need to apply and address network security measures (firewalls, protection from DDoS attacks, security zones etc.) in order to prevent breaches and ensure proper execution of the specified security and data protection plan.	Check networking equipment and firewall rules at each DEDICAT 6G use-case instance and in the cloud hosting platform level		PNF5-9
UNF-81	Trust	Trust certification for devices, stakeholders and processes participating in DEDICAT 6G system and its instances	M	Each system component (SW and HW) and actor should have a valid trust certificate to be used when deciding to include it into DEDICAT 6G network/process/instance	Trust management plan will be produced including trustworthiness categories and methods for their assessment. Trust certificates will be implemented in a form of smart contracts stored in the DEDICAT 6G private permissioned blockchain		PNF5-5
UNF-91	Context-awareness	The system shall be context aware	H	The system shall be able to obtain information on:	Check based on defined experiments. Check that the system is able to infer the current system context/situation		SNF-10

				• application, service and network goals and objectives to be achieved, as well as potential policies. • capabilities of network elements, MAPs and edge devices in terms of communication networking (e.g., radio access technologies (RATs) and spectrum, capacity, and coverage), physical movement, the type of the MAP, computation capabilities, storage capabilities and available power. The system should maintain information and knowledge on the context that has to be addressed in terms of • computation tasks, • power consumption requirements, • set of mobile nodes that need coverage, • mobility and traffic profiles of the different nodes, • radio quality experienced by client nodes, options for connecting to wide area networks, • the locations of docking and charging stations for drone and robot MAPs and • the current locations of the terminals and MAPs' elements, cars...			

				Knowledge about floor plan, system layout			

3.4 Requirement Mapping

The final step of the requirement engineering consists of:

- For all FREQs:
  - To assign the requirement to its proper view: Functional / Information / Network Deployment. For requirements assigned to the FV:
    - To assign the requirement to a Functional Group (as defined by the Functional Model in Section 4.3.1.
    - To assign the requirement to one or several FCs which 1) are relating to the requirement 2) are expected to cover it;
- For all NFREQs:
  - To assign the requirements to the perspective which covers it (examples are given in Section 2.1.3

The result of this task is embodied into a VOLERE template (Excel™ sheet) and is not shown in this deliverable due to its structure (very wide table), which does not fit the format of a Word™ document.

This VOLERE template is accessible from a public page of the project web site [5].

4 DEDICAT 6G Architecture Views

4.1 Physical-Entity View

As introduced in Section 2.6.1, the main purposes of the PE View are:

- To make an inventory of external entities involved in DEDICAT 6G operation;
- To identify which information is exchanged and discuss the privacy related issues;
- To define the roles and natures of interactions taking place between the *Physical Entities (PE)* and the DEDICAT 6G system (edge and Cloud).

We first perform the inventory of physical entities and then address the nature of data the DEDICAT 6G either captures (e.g., via sensors) or has access to, with emphasis on potential existing data privacy issues.

4.1.1 Inventory of Physical Entities

This first section provides an inventory of, so-called, Physical Entities, which are people/objects/network equipment that are in the focus of an IT system and carry information of interest for the targeting IT system, e.g., in the process of building up a context (in the sense of context-awareness). PEs are paramount for IoT system because intrinsic characteristics of the PEs are tracked down by sensors and translated into properties of their cyber-space counter parts Virtual Entities. However, PEs are also important for DEDICAT 6G as human PEs, robots, cars and legacy network equipment are interacting with the system and indeed also carry information of interest to the DEDICAT 6G system. This is the purpose of respectively Table 13 and Table 14 to identify such PEs and to identify the information of interest and their required levels of privacy.

Making an inventory of those various PEs and roles helps:

1. Understanding which entities partake into DEDICAT 6G operation and identifying the nature of exchange information;
2. Steering privacy / Security / Trust-related requirements and technical objectives;
3. Feeding important information into GDPR-related documents;
4. Defining the Context View (e.g., Human/System interface) by elucidating the nature of interactions taking place between entities and DEDICAT 6G.

Examples of such entities we are dealing with in DEDICAT 6G range widely in nature, e.g.:

- **People/individuals:** e.g., tracking people position and gait;
- **Crowd:** e.g., determining whether the crowd is in panic mode;
- **Network** (pieces of equipment or sub-systems): if DEDICAT 6G "senses" network condition in order to feed the Decision Making FC before triggering some network extension-related activities;
- **Cars, Robots, AGVs** etc.

So most importantly, **an entity can indeed be considered as a PE in the PE view and also as a *Physical System* (PS) in the Context View** when it comes to identifying entities, which are 1) either at the edge of DEDICAT 6G or, 2) definitely outside the DEDICAT 6G perimeter (as elucidated in the Context View in Section 4.2.1).

Table 13: Actors / Roles / Relation to the system

UC	Actor/Entity	Description	Role	Description of Interaction (short)
All	Network operator	Operator and owner of network infrastructure (core, radio access network)	Managing and operating the network	Provides policies i.e., high-level rules that should be followed in context handling by intelligence distribution or coverage extension. These also include potential rules and priorities on goals to be achieved, such as the maximization of QoS levels, and the minimization of cost factors (e.g., resource consumption)
All	Service provider	Entity offering wireless communications services over a network infrastructure that it does not own	Managing and operating the wireless communication service in coordination with the infrastructure owner	Similar to the network provider it provides policies, i.e., high-level goals and rules that need to be achieved and followed by the mechanisms for intelligence distribution and coverage extension
All	Vertical actor (a.k.a. DEDICAT 6G customer)	A third party that relies on DEDICAT 6G functionalities to improve its business operation. Examples of such services are Intelligence Distribution as a Service or Coverage Extension as a Service	The role of the Vertical operator is about potentially anything. The 4 DEDICAT 6G scenarios provide 4 realistic and relevant examples of such vertical actor, and the kind of services it relies on	A vertical can rely on DEDICAT 6G to manage the deployment of its own components using its own edge nodes or the one operated by DEDICAT 6G. It can also require Network Extension whenever it needs temporary extra capacity in order to operate its business
All	Owner of edge node (e.g., small server/car/drone etc.)	Actor engaged in a DEDICAT 6G scenario who provides H/W devices that can be used as edge nodes by DEDICAT 6G. It can be e.g., the Network Operator or a Vertical customer	Provides his/her edge devices for edge processing potentially based on some offered incentives	Registers his/her edge devices as potential edge nodes allowing a basic set up that will allow edge processing in the scope of intelligence distribution
3	Event attendee	Person attending an organized event e.g., concert	n/a	Attendees are sharing personal information including potentially heath condition in order to ease the 1st responder's action in case health condition deteriorates during the concert. They also may (subject to formal consent) participate in crowd analysis by

				feeding DEDICAT 6G system with location and gait information
3	Connected Cars	Vehicle acting as edge processing and mobile communication node in the DEDICAT 6G system. Performing Public Safety Critical Communication processes	Mobile communication node, edge processing	As an edge node it may Runs run DEDICAT 6G components for networking and decision making. It may act as a Mobile Access Point
All	Network Equipment	5G legacy equipment provided by the Network Operator	Provides the Core and RAN 5G components that DEDICAT 6G relies on as for Intelligence Distribution and Coverage Extension	A lot of interactions take place between 5G legacy pieces of equipment and Software in both directions. This includes receiving and exploiting various sort of information coming from the 5G network, especially concerning its operation and performance. DEDICAT 6G also needs to instrument some functions supported by the legacy network like e.g., slicing. It also has to inform the 5G network when coverage extension is performed. It also deploys some of the RAN and Core components as part of Intelligence Distribution and coverage extension support
1	Warehouse worker	Person working in the smart warehouse and directly interacting with deployed DEDICAT 6G resources and other warehouse systems	Implementing warehouse processes e.g., picking, packing, checking, loading/unloading	Registers on smart warehousing mobile app on work mobile device. Signs consent form. Gets assigned with a role and access rights. Uses mobile app to organize daily tasks. Interacts with AGVs in line with a task. Receives notifications and alerts based on smart warehousing decision making.
1	Warehouse managers	Person managing and supervising smart warehouse processes and resources. Utilized management features of the DEDICAT 6G system deployed for the smart warehouse	Overall management. Training, conformance to safety measures/standards etc. Supervision of flows and processes within the warehouse	Registers and gets corresponding role in the smart warehousing DEDICAT 6G system. Utilizes DEDICAT 6G smart warehousing management system and dashboard as well as DEDICAT 6G mobile app to configure smart

				warehouse processes (AGVs, IoT system, schedules and notifications). Utilizes the dashboard and mobile app to assign roles to workers. Issues digital keys through SmartAccess360 system. Defines safety zones through the dashboard. Sends and receives push notification
1	AGV	Automated guided vehicle acting as edge processing and mobile communication node in the DEDICAT 6G system. Directly performing smart warehousing processes (loading, offloading, inspection)	Mobile communication node, edge processing, IoT platform (sensing/actuating capabilities)	As an IoT platform it directly interacts with smart warehousing systems and workers. As an edge node it may Runs run DEDICAT 6G components for Analytics, networking and decision making. It may collect, store and analyse data. It may act as a Mobile Access Point
1&3	IoT controller	Edge IoT controller interacting with smart sensing and actuation systems in smart warehouse setting. Can run edge processing component and participate in range extension and provide auxiliary communication paths	Fixed communication node and edge processing node	It directly interacts with smart warehousing systems and workers. Runs DEDICAT 6G components for AI, networking and decision making. It collects, stores and analyses data
2,3	OPTIN/ SmartGlasses	The Smart glasses will be connected to smart phone to have access to the network. Each application will be built by Optinvent and adapted to the use-cases for message, photo, exchange as well as for video streaming	Provide the ORA-2 smart glasses to the use-cases along with dedicated application for each use-case	Interact with core DEDICAT 6G system for use-case and provide AR overlay
All	Smartphone/ mobile device	Mobile device (smartphone, tablet) running DEDICAT 6G application or application directly interfacing with DEDICAT 6G system. Provides the main user interface for interacting with the performed processes and deployed resources	Edge processing and the main interface towards end- users, node of ad-hoc network, relay	Interacts with core DEDICAT 6G system for use-case and provide AR overlay. It is the main interface for end-users

1	Environmental sensors	Temperature, humidity, light intensity	Measuring environmental parameters	IoT controller and AGV collect information from sensors for edge based processing and decision making, or to be transferred to centralized decision making process
1	Bluetooth low energy location beacon	Low energy beacon is provided to workers, installed on mobile assets (e.g., forklift) for detecting indoor location and proximity to points of interest.	Used to detect proximity or derive indoor position	Beacons work with IoT controllers in BLEMAT solution for indoor positioning
3	Victim	The victim is a person who happens to have his life at risk due to various reason like an accident or a natural disaster. She waits for being rescued by so-called, first responders or asks security staff for assistance. The victim is a person attending an event or a civilian caught in a natural disaster	People who need rescue (First Responders) or assistance (Security staff)	After software acknowledgement by the victim, data (such as name, surname, age, localization, video, picture) through victims' smartphone is shared with DEDICAT 6G platform. The data are used for injuries evaluation and precise localization of victims by DEDICAT 6G system (e.g., decision making or mission management)
3	Event operator	After the event and on Rescue team request, the Event operator is responsible to give authorization to access to some attendees data (Name, Gate, Place)	Authority for sharing attendee data	Collection of data (including name, surname, disability, attendee localization) shared with DEDICAT 6G system which will support the evaluation of the situation
3	Member of Security staff	Person working in the smart warehouse and directly interacting with deployed DEDICAT 6G resources and other Event place systems	Applying Security rules during an event	Security staff is able to perform requested tasks and send status through the DEDICAT 6G platform. The radio coverage is provided by either Connected Car or available AVG and provides connectivity to the Security Staff where the accident or disaster took place
3	Doctor	Doctor who coordinates the medical staff on the scene. Taking the decision for different operation to take for the care of victims. Using the DEDICAT 6G to monitor the	Manage the care's operation of victims	Doctor gets situational awareness from Mobile C&C supported by Connected Cars networking and node edge computing in order to stay connected during the Crisis Management process

		situation and communicate with the Medical team. Communicate with other authorities using DEDICAT 6G system		
3	Medical staff member	Applying the decision and strategy of the doctor and interact with him using DEDICAT 6G system	Working under the commandment of doctor	Based on Mobile Client installed on Smartphone, Policeman is able to perform requested tasks and send status through the DEDICAT 6G platform. The coverage is provided by the Connected Car and available AVG in order to provide connectivity to the Medical staff at the incident location
3	Police Operator	The Police Operator receives call and defines the mission which is sent to Policemen. Keeps contact with the Police Team on the field. He uses a C&C system which is interconnected to DEDICAT 6G	Receives call from public and victims. Organizes the mission	Operator gets situational awareness from Mobile C&C supported by Connected Cars networking and node edge computing in order to stay connected during all the Crisis Management process
3	Police Field Officer	Receives the mission from the C&C, manage the mission on the field and its team on the field using DEDICAT 6G system. Keeps the contact with the C&C and share the evolution of the situation	Manage the Police team on the film and the mission	Field officer gets situational awareness from Mobile C&C supported by Connected Cars networking and node edge computing in order to stay connected during the Crisis Management process
3	Policeman	Executes the order shared by the Police Field Officer using the DEDICAT 6G system. Reports the ongoing situation to the Officer. Some data are captured and share automatically with the DEDICAT 6G system in order to receive information from DEDICAT 6G Intelligence	Executing orders from Police Field officer	Based on Mobile Client installed on Smartphone, Policeman is able to perform requested tasks and send status through the DEDICAT 6G platform. The coverage is provided by the Connected Car and available AVG in order to provide connectivity to the Policeman at the incident location
3	Firefighter Operator	The Firefighter Operator receives call and defines the mission which is sent to Firefighters.	Receives call from public and victims. Organizes the mission	Operator gets situational awareness from Mobile C&C supported by Connected Cars networking and node edge computing in

		Keeps contact with the Firefighters team on the field. He uses a C&C system which is interconnected to DEDICAT 6G		order to stay connected during all the Crisis Management process
3	Firefighter Field Officer	Receives the mission from the C&C, manage the mission on the field and its team on the field using DEDICAT 6G system. Keeps the contact with the C&C and share the evolution of the situation	Manage the Firefighter team on the film and the mission	Field officer gets situational awareness from Mobile C&C supported by Connected Cars networking and node edge computing in order to stay connected during all the Crisis Management process
3	Firefighter	Executes the order shared by the Firefighter Field Officer using the DEDICAT 6G system. Reports the ongoing situation to the Officer. Some data are captured and share automatically with the DEDICAT 6G system in order to receive information from DEDICAT 6G Intelligence	Executing orders from Firefighter Field officer.	Based on Mobile Client installed on Smartphone, Firefighter is able to perform requested tasks and send status through the DEDICAT 6G platform. The coverage is provided by the Connected Car and available AVG in order Firefighter is connected to the network while he is closed to the incident
3	MCX App	Client application allowing contextual information sharing and communication between users during Mission Management Such information displays Resources position, picture or other files, voice or video communication	Main interfaces for Public Safety or Private Security users to the MCX system. Allow authentication and manage security for information sharing	The MCX Client interfaces with MCX FC which is part of DEDICAT 6G platform in order to benefit from MCX features delivered by the platform
2, 3	Drones	Drone equipped with 5G and WIFI radio interface, computing capability (depending on UC specific needs). Drones are an efficient mean of use in order to get information from the crisis as they come up on the scene quicker than First Responders. During the crisis management, drones can continuously deliver information on	The main purpose of the drone (considering the baseline scenario) is to provide 5G coverage extension. Additional purposes can include WIFI hotspot, some advanced IA-based algorithms like sudden crowd movement detection or video-monitoring (in crisis context for example). In the context of UC3, the drones will share their positions in order to leverage the awareness of the situation with the shared images	The drone is integral part of the baseline DEDICAT 6G architecture. There is a wide range of interactions involving dynamic migration of intelligence to the Edge part of the Drone, interaction with the legacy 5G network to ensure the coverage extension, plus additional interaction depending on the embedded scenario-related FCs (e.g., use MCX Client to connect to MCX Server which

		the evolution of the situation during Mission Management		are part of DEDICAT 6G platform in order to use the resilient connection to upload video and share position
3	Site Environment ("Large Event" UC3 scenario)	During the crisis management, Sensors like video camera surveillance can deliver information on the situation during Mission Management	DEDICAT 6G will offer connectivity capability to third party devices in order to make data sharing available for First Responders	Camera surveillance device from site will connect to DEDICAT 6G platform in order to get through a gateway the video flow and make it available for sharing with MCX data and video features
3	Emergency Vehicle (Police car, fire truck, ambulance…)	Integrated device running DEDICAT 6G application or application directly interfacing with DEDICAT 6G system. Provides the user connectivity for interacting with the performed processes and deployed resources.	Edge processing and the main interface towards end-users, node of ad-hoc network, relay	As an edge node it may Runs run DEDICAT 6G components for networking and decision making. It may act as a Mobile Access Point.
3	MCX Smartphone	The device is used on the field by rescuers and runs the MCX applications.	Devices running MCX App for users on the field	MCX Smartphones are connected to DEDICAT 6G platform in order to get 6G/B5G connectivity while Commercial or other private network can't ensure connectivity services. MCX Smartphone are connected to Connected Cars or AVG.
3	MCX Server	The MCX Server host all MCX services and support Critical Group Communications	Server running MCX services	MCX Server is part of DEDICAT 6G platform and can deliver MCX services through DEDICAT 6G Node, AVG or Connected Cars.
4	Vulnerable Road Unit (VRU)	Road users such as pedestrian or cyclists	Moving around the road using a handheld device	VRUs are connected to the network notifying their presence on the road by providing their location
4	Driver	Road user using a motorized vehicle (car)	Moving around the road guided by an On-Board Unit (OBU)	Drivers are connected to the network notifying their presence on the road by providing their location

4.1.2 Inventory of captured data

The Table 14 below gives a complete inventory of the various pieces of data collected from PEs by either 1) the four DEDICAT 6G scenarios (UC number in 1st column) or 2) by the DEDICAT 6G platform (D6G in first column) for the sake of its own operation (e.g., to build up a B5G network context).

Table 14: Inventory of collected data

UC/D6G	Actor/Entity	Nature of data	Capture Mode {sensed/declared/assigned/measured)	optional {Y/N}	Privacy policy {Y/N}
2, D6G	Network Equipment	Server energy Consumption	Sensed	N	n/a
		Packet latency	Sensed	N	n/a
		Throughput	Sensed	N	n/a
		Number of connected users (to video streamer)	Sensed	N	n/a
3	Event attendee (GA µS)	Pseudonym	Assigned	N	N
		Location	Sensed	N	N
1, D6G	AGV	Location	Declared / sensed	N	n/a
		System status	Declared	N	n/a
		Proximity of points of interest	Declared / Sensed	N	n/a
		Process status	Declared	N	n/a
1	IoT controller	Proximity of points of interest	Declared / Sensed	N	n/a
		System status	Declared	N	n/a
		Process status	Declared	N	n/a
1	Worker	Location	Sensed	N	Y
		Authorization level	Declared	N	Y
		Task	Declared	N	Y
1	Manager	Location	Sensed	N	Y
		Authorization level	Declared	N	Y
		Task	Declared	Y	Y
1	Warehouse environment	Environmental parameters (temperature, humidity, light intensity)	Sensed	N	n/a
		System status	Declared	N	n/a
2	Event Attendee	Location	Sensed	Y	Y
3	Field Officer	Location	Sensed	N	Y
		Mission status	Declared	N	N
		Proximity of points of interest	Declared / Sensed	N	N
		Health status	Sensed	Y	Y
3	Team member	Location	Sensed	N	Y
		Mission status	Declared	N	N
		Health status	Sensed	Y	Y
3, D6G	Drone	Location	Sensed	N	n/a

		Authorization level	Declared	N	n/a
		Video	Sensed	N	Y
3	Site environment	Environmental parameters (temperature, humidity, light intensity)	Sensed	N	n/a
		System status	Declared	N	Y
3	MCX Smartphones	Throughput	Sensed	N	n/a
		Packet latency	Sensed	N	n/a
		Connectivity	Sensed	N	n/a
3	MCX Server	Throughput	Sensed	N	n/a
		Packet latency	Sensed	N	n/a
		Connectivity	Sensed	N	n/a
3	Victim	Localization	Sensed	N	Y
		Health description	Declared	N	Y
		Picture	Declared	Y	Y
3	Event organizer	Attendees list	Declared	Y	Y
		Attendees localization	Declared	N	Y
		Site mapping	Declared	N	Y
		Security Staff Communication ID	Declared	N	N
4	VRU	Position	Sensed	N	Y (but data is anonymised)
4	Smart & Smarter Cars	Position	Sensed	N	Y (but data is anonymised)
		Speed	Sensed	N	N
		Video / Lidar	Sensed	N	N

4.2 Context View

As explained in Section 2.6.2 this view:

1. Identifies the various physical systems outside the DEDICAT 6G cloud platform and decides if they are part of DEDICAT 6G (IN) or not (OUT) depending on whether or not they sit at the edge of the DEDICAT 6G system;
2. (doing so) defines the perimeter of DEDICAT 6G platform (hence made of Edge + Cloud parts);
3. Defines external interfaces between PSs and DEDICAT 6G;
4. Defines external interfaces between human actors (as identified in the PE View) and DEDICAT 6G

4.2.1 Defining the perimeter of the DEDICAT 6G system

In order to help defining the perimeter of the platform, i.e., what components lie inside and outside the system, we start with an inventory of:

1. All physical systems which are not physically part of the platform;

2. All FCs part of those physical systems which are either part of the platform or considered as being at its edge.

The following Table 15 gives this inventory and also provides additional information, whose columns are described below:

- **UC/D6G**: which UC (UC number) is at the origin of the whole table row and/or "D6G" if the PS is a *de facto* B5G or network extension element (used by scenario but considered as integral part of DEDICAT 6G system);
- **PS name**: Physical System name (device/equipment/ smart phone/robot etc.);
- **PS@edge**: PSs which are candidate for edge computing (meaning they could execute FCs dynamically migrated from the platform). Must obviously be "Y" if the list of Edge FC is non-empty;
- **Edge FC**s: FCs which will be hosted by the PS i.e., dynamically migrated from the Cloud;
- **Legacy FCs**: FCs which are provided by the PS by default (excluding migrated components which are listed in Edge FC column);
- **Description/comment:** can be used to describe FCs informally if they are not individually identified yet.

Note 1: Part of this inventory (e.g., Robots, Smart Vehicle) is also described in the PE View, however it is focusing on completely different matter, as explain in the PEV introduction.

Note 2: A PS can be listed as an Edge node (PS@edge="y") even if the list of edge FCs is empty. It simply means that no edge FC has been identified by the scenarios for that particular PS. However, any business application willing to use that particular PS could instruct the DEDICAT 6G system to set-up a migration policy leading to migrating some business-specific µServices to that edge PS (see the IDaaS scenario in Section 4.3.4.6).

Table 15: Inventory of physical systems as identified in the 4 Scenarios

UC / D6G	PS name	PS@ edge (Y/N)	Edge FCs [1..n]	Legacy FCs [1..n]	Description/ comment
D6G	Small server	Y	anything required	n/a	Depends mainly on 1) the verticals and the sort of services they would like to deploy to such servers 2) the 5G components that would have to be deployed in the context of Coverage Extension
1,3 D6G	AGVs	Y	AGV/Robot services such as camera operation, remote control, Image processing, providing wireless connectivity to other nodes deployed as Virtual Network Functions (VNFs)	n/a	AGVs may be used as sensors and actuators as well as MAPs. To support this type of functionality services will be deployed on AGVs as VNFs
1	Forklift/machine	N	n/a	n/a	Mainly "talks" with SmartAccess360 controller/cloud

1, 3	SmartAccess360 controller	Y	• Indoor positioning FC • Env Sensing FC • Threat Analysis FC • Trust metric FC	• IoT controllers FC	IndoorPositioning FC and EnvSensing FC are vertical FC that are meant to be deployed to the edge by D6G EC capabilities. ThreatAnalysis FC will be deployed by D6G by default to all EC nodes as part of the PST strategy
1	Warehouse personnel smartphone/mobile device	Y	• Threat analysis FC • AR FC • Dedicat6G ConsentForm FC • Trust Metric FC	• SmartAccess 360 app FC	SmartAccess360 application used to turn a smart phone into a digital key for smart actuation and managing doors and access control to areas
1,2,3, D6G	(B)5G Networking Equipment	Y	• Multicast-Broadcast Service FC • Unicast-Multicast Controller FC	n/a	5G Network equipment is considered as an external layer of D6G, and further described in section 4.3.3
2	Video streaming platform	Y	• VideoTrans-Coder FC	n/a	Video transcoding from high quality to adaptive streaming
2,3/ D6G	Drones	Y	Services such as camera operation, remote control, Image processing, providing wireless connectivity deployed as Virtual Network Functions	n/a	Similar to AGVs, Drones may be used as sensors and actuators as well as MAPs. To support this type of functionality services will be deployed on Drones as VNFs
2	Smart phones	N	n/a	• video-Streamer FC • any other App (support to SmartGlass)?	Still to be discussed internally
2	smartGlass	N	n/a	• Video&Audio Capture & Compression FC • EventGUI FC	FC that use the Video and Audio capability of the smartGlass to capture a live event
3, D6G	Connected Car (maybe different from UC1)	Y	• MCS FC	n/a	Deliver Mission Critical services in order to add a network coverage in case of infrastructure lost or support the coverage in case of large event and infrastructure overload or failure due to the amount of connection during the disaster
3	MCS mobile server	N	n/a	• MCS FC	In case of a disaster, first responders may have in their vehicles part of the MCS-cloud functionalities deployed to a mobile PC/server in order to maintain the provision of

					needed MCS functionalities despite the likely lack of connectivity. (not deployed by DEDICAT 6G)
3	Attendee smartphone	Y	n/a	• Gait_Analysis FC • Attendee Consent Form FC	FC developed for the sake of UC3 only, reports gait to DecisionMaking FG/crowdAnalysis FC
			n/a	• Attendee App FC	App specially designed for the event attendees (organized context). includes request for personal information that are handled by the event organizers only and a first consent Form (for eventually sharing this information with event deployed medics)
			• Dedicat6G_ConsentForm FC	n/a	As soon as the EventApp consent form has been agreed upon D6G is requested to send a D6G-specific consent form for movement tracking. This FC is deployed to the Attendee Smartphone
3	1st Responder smart phone	N	n/a	• FirstResponderApp FC • SmartAccess 360 mobile app FC	The first responder must be able to reach out to the event organizer system to access a person's health record by scanning the event bracelet (QRcode) as part of the event Context. SmartAccess360 mobile application FC can be integrated into the FirstResponder app to allow interaction with SmartAccess360 controllers
3	smart glass	N	n/a	• GUI_FR FC • Video&Audio Capture & Compression FC	They provide a GUI to first responders
		N	n/a	• GUI_SEC FC • Video&Audio Capture & Compression FC	They provide a GUI to SECurity staff
3	smartAcces360	Y	• AuthZ FC • AuthN FC • IdM FC	• IoT Controller FC • SmartActuation	This H/W-based version of smartAccess360 will be physically deployed at the gate side and run some dynamically deployed DEDICAT 6G FCs (as edge FCs). SmartActuation perform access control based on the AuthN/AuthZ/IdM FCs
3	SmartGate	N	n/a	• GateController FC	They provide interface to the actuable gate / turnstile
3	Event Information System	N	n/a	Gateway service component	Deliver interfaces to connect External System to DEDICAT 6G platform in order a specific

					External System could continue to run its proper security services (e.g., video surveillance during a crisis management on a large event)
4	Smart vehicle	N	n/a	• Driver-Awareness FC	They report information about other cars and VRUs
4	Smarter vehicle (incl. tablet-like terminal)	Y	• Road Information processor FC • Video&Lidar Capture FC	• Driver-Awareness FC	n/a
4	IoT Nodes	Y	• Env Sensing FC	n/a	They also send raw data from other PS if needed
4	RSU	Y	• Road Information processor FC	n/a	A RSU also provides a WIFI accessPoint, therefore connectivity in the surroundings
4	VRU's smart phone	N	n/a	• VRU-Awareness FC	Vulnerable Road User app

This next Table 16 gives additional information about the FCs introduced in the table above.

Table 16: FCs at the edge or outside the DEDICAT 6G perimeter

FC name	FC Edge (Y/N)	Short description
gaitAnalysis FC	Y	Based on attendee's mobile phone 3-axis accelerometer data and compass this FC infers respectively attendee's gait (standing immobile, walking, running, etc.) and her overall direction
Attendee App	Y	Provides a registration page, consent form page and the gait Analysis FC as a µService. This later one gets deployed and activated remotely if and only if the attendee agrees to the T&C of the consent form
Indoor Positioning FC	Y	Provides indoor location of entities/actors based on Bluetooth beacons and triangulation. The associated coordinate system is local to the warehouse map
Env. Sensing FC	Y	Collects and returns elements of environmental context
IoT Controller FC	N	Is a native functionality from the SmartAccess360
Augmented Reality FC	Y	Augmented reality overlay for smart glasses and smartphone applications (using camera) enabling navigation and context-aware notifications and points of interest to users in the context of the use-case
SmartAccess 360 mobile app FC	N	Part of the SmartAccess 360 solution residing on the end-user mobile devices. The app allows users to utilize granted digital access keys for doors and other smart actuation points (e.g., turn on/off lights etc.)
Multicast-Broadcast-Service FC	Y	Provides a video multicast/broadcast service for cellular networking
Unicast-Multicast Controller FC	Y	Part of the video multicast/broadcast service. Provides ability to switch dynamically from unicast mode to multicast and vice versa
Video Transcoder FC	Y	Receives high quality video streams from user devices (uplink) and transcodes the streams to adaptive representations
Threat Analysis FC	Y	FC to be instantiated at all Edge nodes. Runs ML models for cyber security threat detection and identification. Updated/trained on collected system logs. Performed in federated learning mode

Trust Metric FC	Y	FC to be installed at all edge nodes. Trustworthiness metrics are calculated for edge nodes, processes, users and data streams. Trust metric value indicates if a node can join a local network, if process output can be further used, if user can execute specific rule
AuthZ	Y	Native DEDICAT 6G Authorization functionality with role and attribute based authorization and access control. Applied on users and devices
AuthN	Y	Native DEDICAT 6G Authentication functionality applied to end-users. Roles defined on the level of the project and for each UC
IdM	Y	Native DEDICAT 6G identity Management functionality used for assigning identity and roles to systems, devices and users
GateController FC	N	This component offers an interface to lock/unlock a smart actuable door/turnstile
Attendee Consent Form FC	Y	Displays a consent form where the given/Family names are given and where the individual agrees/denies movement tracking. Agreeing will either unlock the tracking functionality
Video&Audio Capture FC	N	Captures ambient audio and video from the smartGlass
Video-Streamer FC	N	Native application in the smartPhone used for video/audio streaming (when smartGlass is not available for that purpose)
MCS FC	N	subset of the MCS cloud based MCS platform (Airbus owned)
DriverAwareness FC	N	Reports information about other cars and VRUs
VRU-Awareness FC	N	Application used to keep the VRU aware of imminent danger or road environment (nearby cars, other VRUs (i.e., pedestrians)
RoadInformation Processor FC	Y	Analyses and processes the information before pushing the result to the RSU smartPhone
Video&LiderCapture FC	Y	Captures video and Lidar streams (i.e., collects information about the car surroundings)
Video&Audio Capture & compression FC	N	Native FC in the smartGlass that performs Video/Audio capture and compression in order to save bandwidth
MCS Audio FC	Y	MCS Audio FC is a functional component, which delivers audio Push-To-Talk and Full-Duplex over IP communication feature to users. The component takes into account *QoS Class Identifier* (QCI) for connectivity priority Several MCS Audio FC can be deployed to support efficiency and resiliency of voice communication
MCS Video FC	Y	MCS Video FC is a functional component, which delivers real-time video over IP communication or streaming feature to users. The component takes into account QCI for connectivity priority. Several MCS Video FC can be deployed to support efficiency and resiliency of video streaming
MCS Situation FC	Y	MCS Situation FC is a functional component, which delivers operational situation feature to users. The component takes into account QCI for connectivity priority. This component transmits operational situation to PPDR or Public Safety organizations' infrastructure
MCS Location FC	Y	MCS Location FC is a functional component, which delivers location and mapping feature. The component takes into account QCI for connectivity priority. This component transmits users position to PPDR or Public Safety organizations' infrastructure
MCS Registration FC	Y	MCS Registration FC is a functional component which delivers registration and authentication features

4.2.2 UML Use-Cases

Those UML use-cases focus on interactions taking place between (external) entities -either they are human actors or physical systems- and the DEDICAT 6G overall system (made of edge-based and cloud-based components). Those UCs are heavily scenario dependent, so we do split this section into 4 sub-sections that tackle each individual scenario in turn.

4.2.2.1 UC1 – Smart Warehousing

In the Smart Warehousing use-case we have two main warehouse personnel types and two system actors which interface with each other through the DEDICAT 6G platform and which interface with the DEDICAT 6G platform and its core functionalities. The two personnel types are (also described in D2.1 [3]):

- Smart warehouse manager – responsible for managing deployed smart warehouse resources and processes. The manager interfaces with DEDICAT 6G system to configure smart warehousing processes, to monitor utilization of resources and to receive notifications about performance of daily tasks and running automation processes;
- Smart warehouse worker – responsible for performing daily warehousing while being supported by the deployed DEDICAT 6G systems.

Now, we introduce a set of use-case UML diagrams describing the interactions existing between different smart warehousing actors through the DEDICAT 6G platform, as well as interactions between system actors and key DEDICAT 6G platform functions.

Figure 6 below shows a UML use-case diagram with key steps and procedures that are taken during warehouse personnel onboarding onto the DEDICAT 6G platform. Two main functional flows are depicted:

- User registration – here a new user account is created. In order to create account and receive assigned role in the platform, user needs to provide credentials and fill and sign DEDICAT 6G smart warehousing consent form. Credentials (e.g., email) need to be verified with implemented verification method. The consent form informs user about the role (s)he is taking in the smart warehousing ecosystem deployment, benefits of participating in the system and privacy protection policy. After successful registration, user is assigned one of the predefined system roles, which further defines how user interacts and interfaces with the deployed DEDICAT 6G systems;
- User login – successfully onboarded/registered user can access the DEDICAT 6G platform and its functionalities anytime through the provided user interfaces (DEDICAT 6G mobile application or web dashboard). By submitting registered credentials, user is granted access to the DEDICAT 6G functionalities according to the role assigned to her during the registration process. It should be possible to update assigned roles for users through DEDICAT 6G administration portal. If user's credentials are forgotten, the user can send a request for password reset. Finally, an end-user can choose to deactivate registered account; this would initialize deletion process for all user related data from the DEDICAT 6G platform.

Once a user is registered, one of the two main roles is assigned – warehouse manager or warehouse worker. Based on the assigned role, the user can interact with a pre-defined set of DEDICAT 6G platform functionalities and with other actors and deployed systems in predefined way.

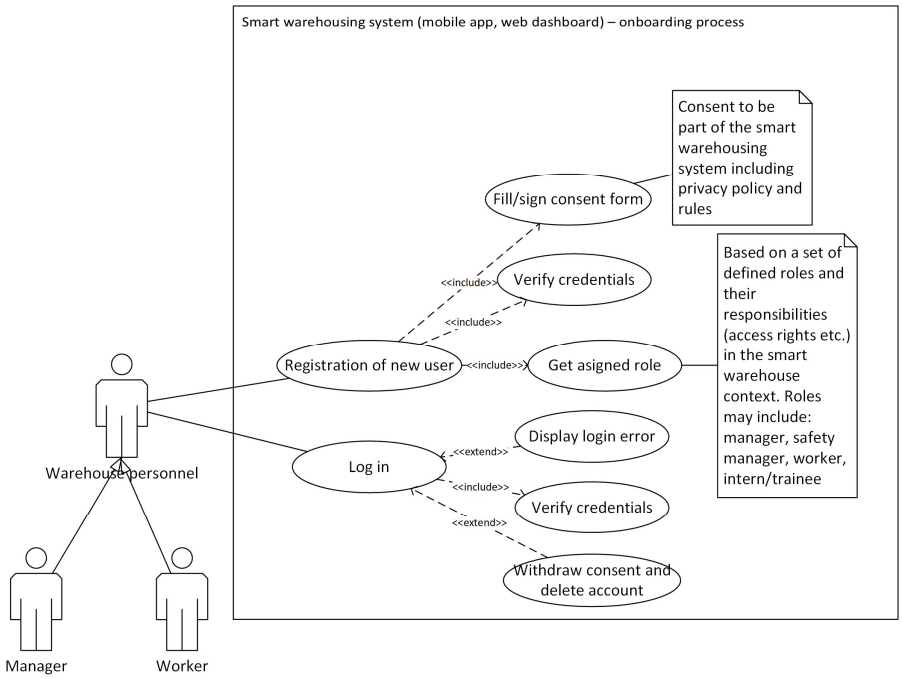


Figure 6 - User onboarding UML diagram for UC1 Smart Warehousing

Figure 7 shows how warehouse manager interacts with the DEDICAT 6G platform functionalities and with other key actors in the smart warehouse use-case supported by the DEDICAT 6G systems. There are five main DEDICAT 6G platform functionalities provided to the warehouse manager (the warehouse manager needs to be authorized in order to access those functionalities):

- Receiving notifications from the DEDICAT 6G platform – the notifications contain predefined messages (set based on predefined set of system triggers) with key information about status of the deployed systems, resources and performed processes. Specific focus is put on the threat analysis and reports generated by this functionality. The threat analysis and other system monitoring functionalities are based on the system logging functionality with which all authorized DEDICAT 6G systems interact to log status or get status reports from other actors and systems;
- Monitoring status of the deployed resources and performed tasks – this functionality also relies on the access to the DEDICAT 6G system logs;
- Monitoring onboarded workers and their status – the warehouse manager can check the current logged status of the selected warehouse worker and get the list of assigned and performed daily tasks. The DEDICAT 6G system will support creation of logs through which workers can report their status. The logging process should be established in line with the privacy protection policies and all necessary information should be disclosed through the consent form;
- Deploying new DEDICAT 6G resources – through this functionality a warehouse manager can configure and deploy additional AGVs and IoT controllers to become part in the DEDICAT 6G smart warehousing ecosystem. After deployment and configuration, AGVs and IoT controllers are authorized to become part of the smart warehousing processes and DEDICAT 6G decision making;
- Configuration of smart warehousing processes – this includes configuration of a daily task for authorized workers, configuration of daily routines for authorized AGVs and

configuration of the IoT processes supported by authorized IoT controllers. These IoT processes include configuration of geo-location safety zones and alerts and configuration and assignment of door/gate/lock digital keys for personnel.

All functionalities for warehouse manager are provided through DEDICAT 6G web dashboard.

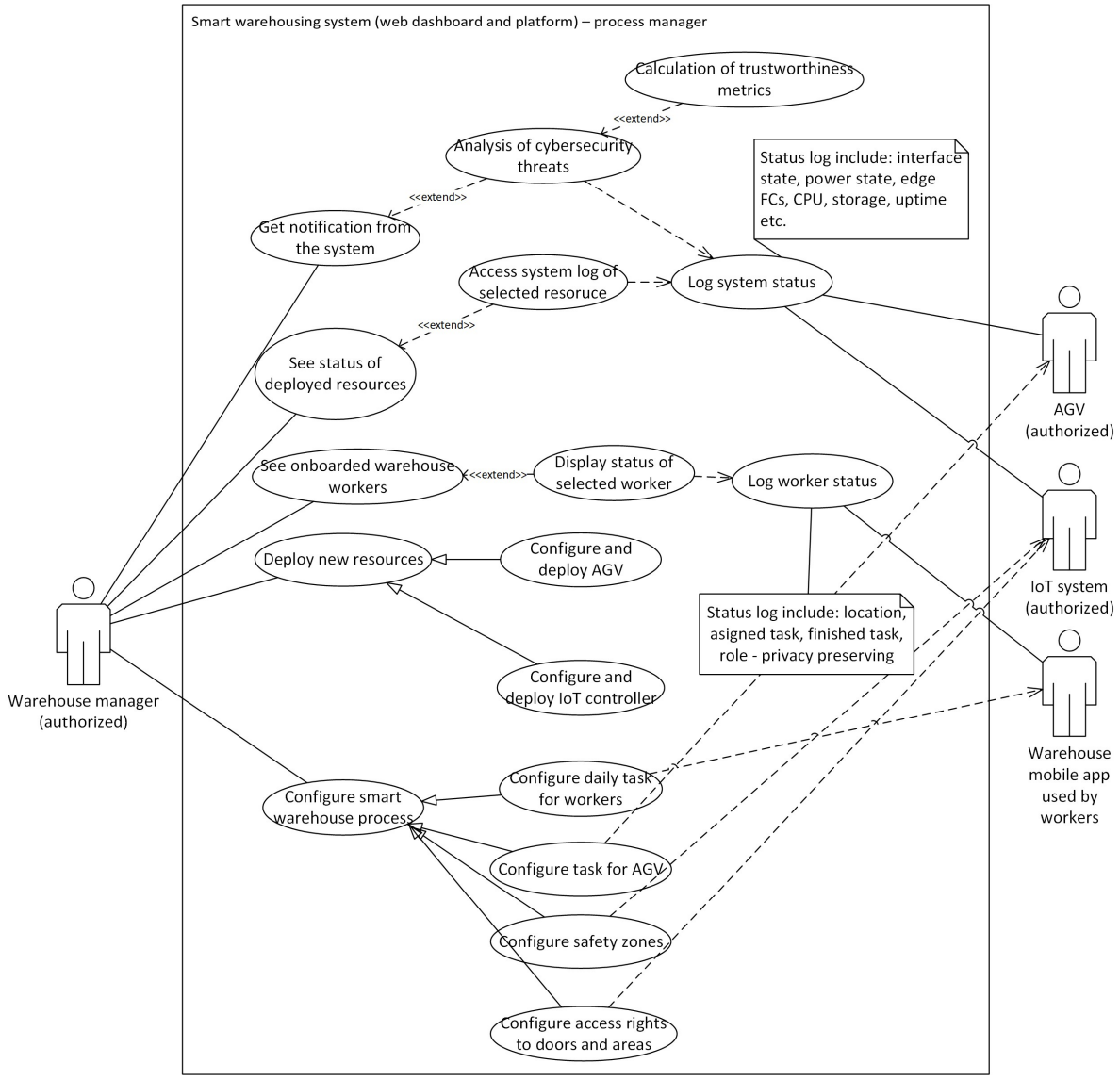


Figure 7 - UC1 Smart Warehousing - UML diagram for warehouse manager actor interactions

Figure 8 shows how a warehouse worker interacts with the DEDICAT 6G platform functionalities and with other key actors in the smart warehouse use-case supported by the DEDICAT 6G system. There are two types of warehouse workers – regular/experienced workers and trainees. Different tasks are assigned to these two types of workers by the warehouse managers, but once authorized, they have access to the same set of DEDICAT 6G functionalities:

- Interacting with AGVs – through this DEDICAT 6G platform functionality, warehouse a worker can configure and assign a new task to an AGV (e.g., go to point A and

inspect box B), or check the AGV status. All status checks and monitoring functionalities are supported with system logs;

- Accessing and using AR interface – through mobile app interface workers can get AR overlay of the camera feed. In this overlay the workers can see status reports of AGVs or other warehouse systems (depending on use-case configuration) and get directions to navigate warehouse from point A to point B (this is particularly important for trainees);
- Tracking indoor location of mobile assets – with this functionality of DEDICAT 6G platform, warehouse workers can check exact location of mobile assets. This functionality relies on indoor location derivation function;
- Report indoor location – allows warehouse workers to log their indoor location through mobile application or provided BLE beacon. This is done in line with DEDICAT 6G platform privacy policies and consent form, and location information is anonymized;
- Get notification – warehouse workers can receive system notification:
    - Notification that they have received new digital key allowing them to use their mobile phones to control electric locks in line with granted access rights;
    - AGV status notification – AGV needs assistance or annual check;
    - Safety zone notification based on current location and defined safety zones – entering into zone where dangerous process is in progress or notification when there are too many workers in close vicinity (COVID-19 social distancing rules);
    - Notification about new task being assigned to warehouse worker by the warehouse manager.

All functionalities for warehouse worker are provided through mobile application and/or web dashboard.

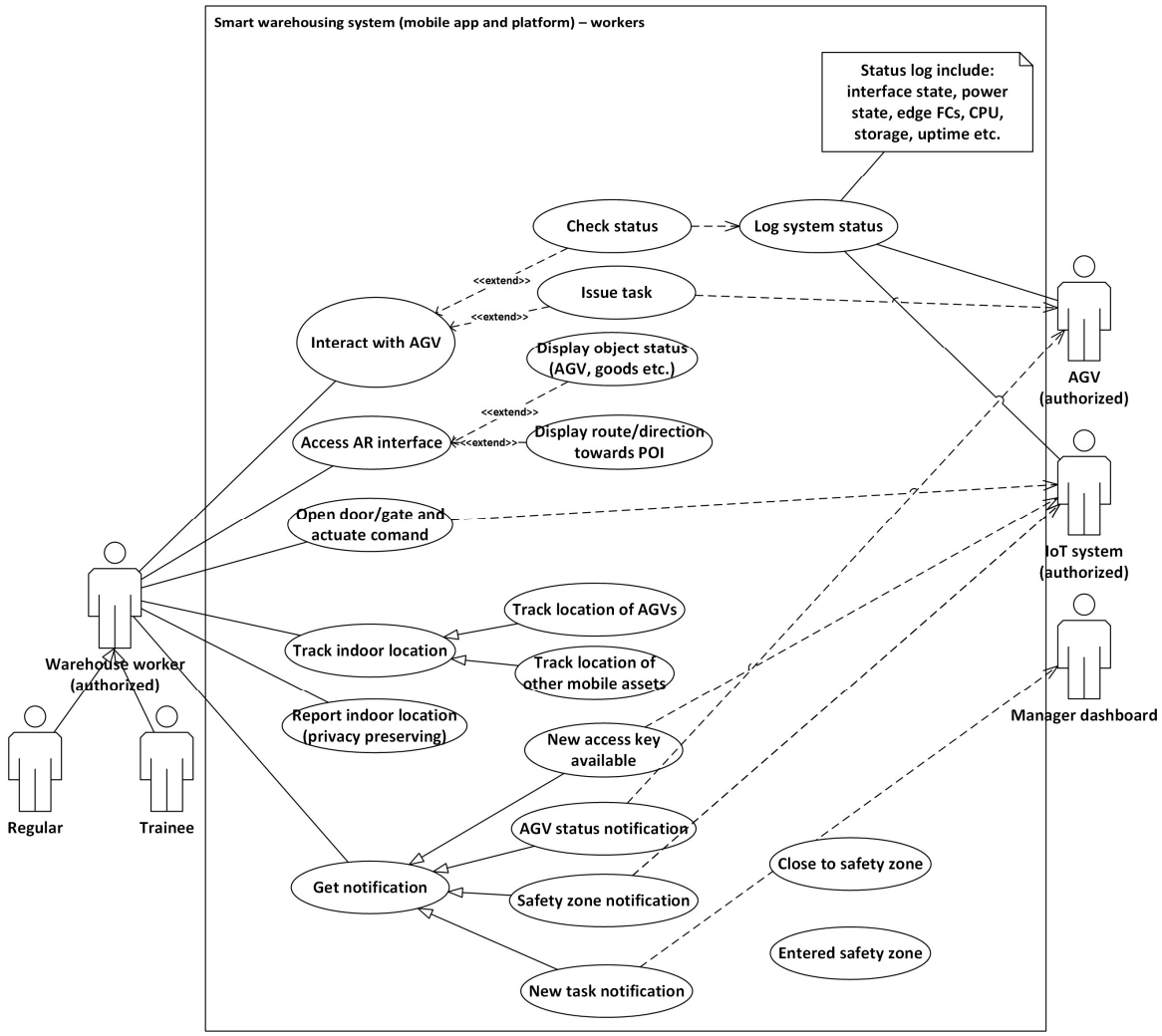


Figure 8 - UC1 Smart Warehousing - UML diagram for warehouse worker actor interactions

Figure 9 shows how a deployed AGV interacts with the DEDICAT 6G platform functionalities and with other key actors in the smart warehouse use-case supported by the DEDICAT 6G systems. The main functionalities that DEDICAT 6G system provides to AGVs include (authorized AGVs have access to these functionalities):

- Go to location functionality – AGVs can be instructed by other actors to go to a specific location in the warehouse. AGVs can also run decision making process that enables them to make decision to navigate to a specific location in the warehouse. Indoor navigation relies on indoor location derivation functionalities of the DEDICAT 6G platform and deployed systems;
- Inspect goods functionality – AGV can utilize integrated sensors and camera to take certain measurements and collect data about goods. Information is analysed for decision making and/or sent to workers/manager for further actions;
- Log system status functionality – this is major functionality for AGVs allowing them to log all system status and sensory readings and perform analysis on the collected data. This functionality extends into threat analysis and trustworthiness metric calculation functionalities which are important for certain decision making operations like coverage extensions or accepting edge computing functional component;

- Coverage extension functionality – AGVs can create communication links with surrounding communication nodes including other AGVs and IoT controllers. Mobile AGV can extend coverage to impacted areas in the warehouse (e.g., blind spots as result of large shipment being stored). Coverage extension links are established only with trusted communication nodes;
- Other edge computing processes – AGV can perform other needed edge computing processes and run edge functional components. These can include but are not limited to context-awareness functional components or smart warehouse process related tasks;
- Get warehouse task/command – AGVs can receive tasks from authorized warehouse mangers or workers.

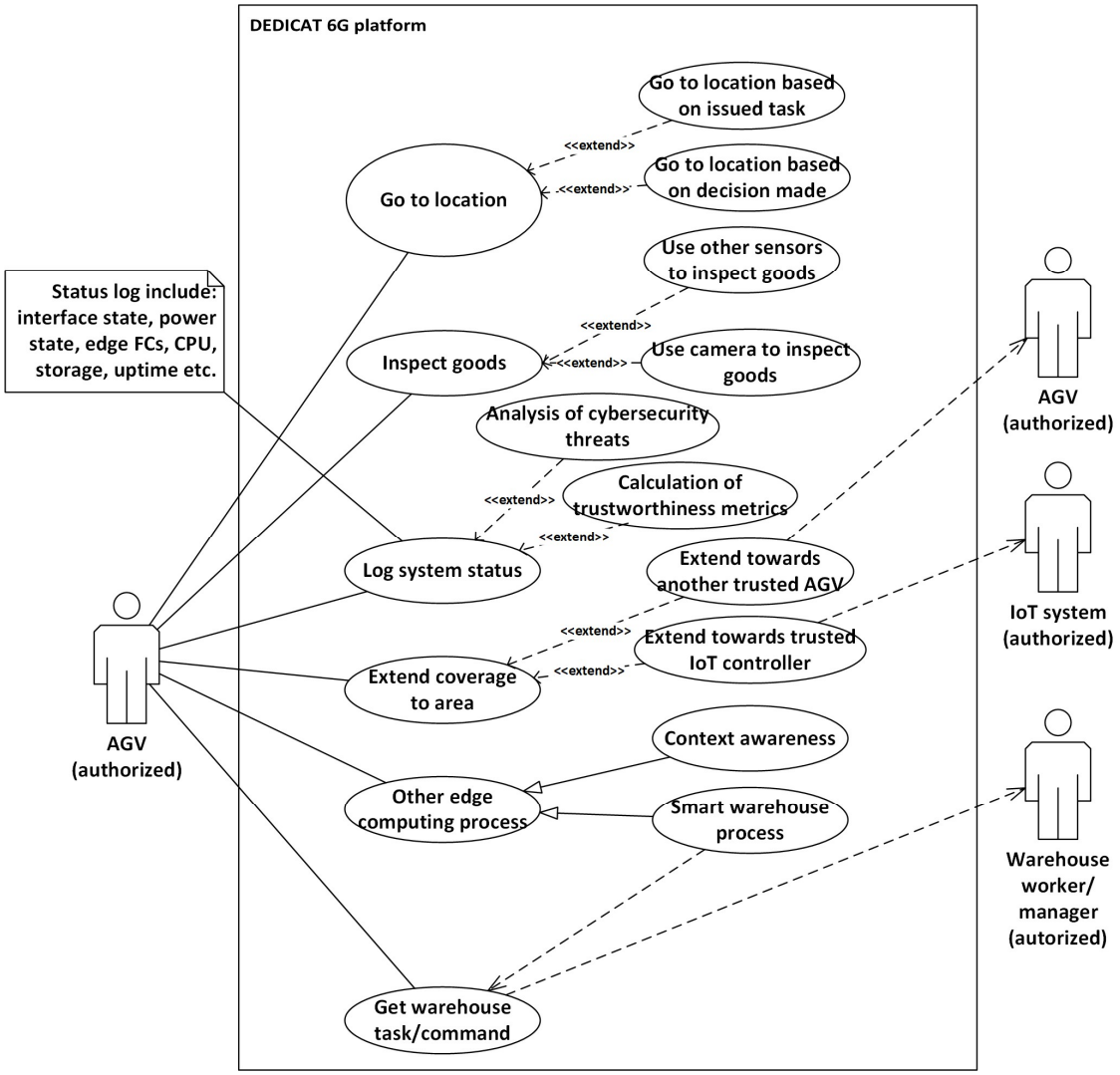


Figure 9 - UC1 Smart Warehousing - UML diagram for AGV interactions

Figure 10 shows how installed IoT controller interacts with the DEDICAT 6G platform functionalities and with other key actors in the smart warehouse use-case supported by the DEDICAT 6G systems. The main functionalities that DEDICAT 6G system provides to authorized IoT controllers include:

- Location derivation functionality – IoT controllers have fixed location in the warehouse and based on known location perform location derivation of mobile assets equipped with BLE beacons by measuring SNR from mobile asset to three fixed IoT controllers. This functionality also includes proximity detection (less precise location assessment that does not need trilateration – measurements from three different controllers). All location derivations of warehouse personnel are done with privacy preserving approaches and in line with accepted privacy policies and consent forms;
- Actuation functionality – IoT controllers are equipped with circuit relays, and they can directly actuate electric locks and control electric circuits, which power systems like alarms and lighting;
- Logging system status functionality – as for AGVs, IoT controllers log their system status and measured status of their surroundings. Important extensions of this functionality are threat analysis and trust metrics calculation performed on the edge;
- Coverage extension functionality – IoT controllers can act as fixed communication gateways for mobile assets like AGVs. IoT controllers can establish multi-hop communication path among themselves in order to reach controller with access to the fixed network or other communication gateway. All coverage extensions are done only towards trusted nodes;
- Environmental monitoring functionality – IoT controllers receive measurements from environmental sensors deployed in warehouse (temperature, humidity). Based on collected data, IoT controllers can perform edge-based assessment of environmental conditions. Based on assessments IoT controllers can send push notifications to other DEDICAT 6G systems and warehouse personnel. Only data from trusted environmental sensors are taken into account when assessing environmental conditions.

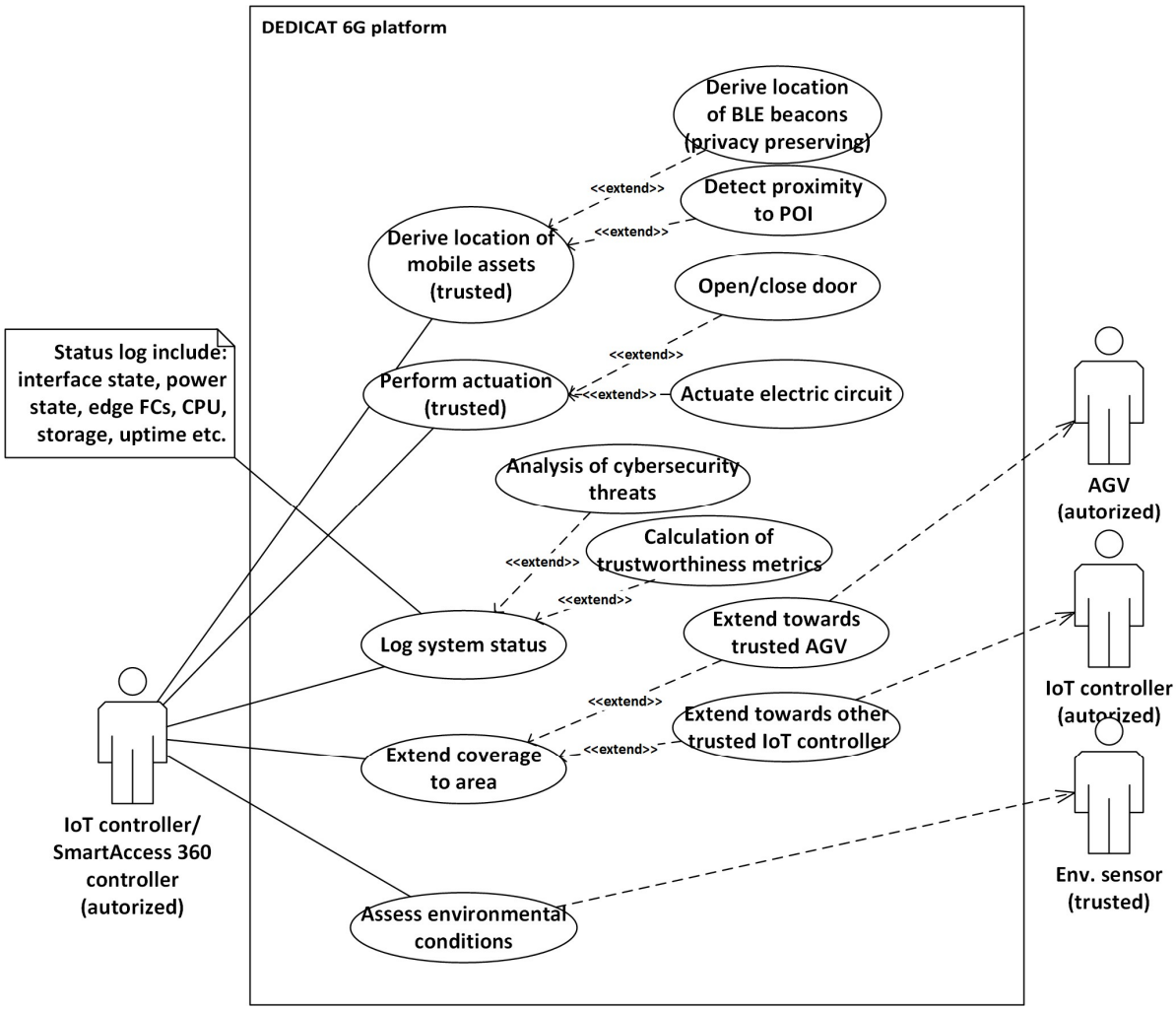


Figure 10 - UC1 Smart Warehousing - UML diagram for IoT controller interactions

4.2.2.2 UC2 – Enhanced Experience

In the Enhanced Experience there are two types as event participants functioning as system actors depending on their physical location. They interface with each other as well as DEDICAT 6G platform functionalities depicted in the following UML diagrams. The main system actors are:

- Local event participant – responsible for producing or consuming live content in the event site. Interacts with the DEDICAT 6G platform by deploying the video application that is connected to the video streaming platform or multicast/unicast video service;
- Remote event participant – acts as the virtual (video) service consumer via remote connection towards the physical event site. Interconnects also with the DEDICAT 6G platform via dedicated video application connected to video streaming platform or multicast/unicast video service.

Figure 11 below presents the UML use-case diagram showing the interactions between the different Enhanced Experience system actors and DEDICAT 6G platform for deploying the dedicated application in this use-case. The main three functional flows depicted in this figure are the following:

- Agreement for terms of usage – Here the user agrees to the terms that DEDICAT 6G platform can see some of the user-specific information when application is launched, such as IP address of the connected device. However, this information is used purely only on setting sufficient quality level of service needed by resource controller, edge processor and/or video streaming services. No strongly confidential data e.g., name is needed for deploying the application;
- Deployment of video application – Here the user first selects either the dedicated video player application for consuming the video feed, or dedicated video streaming application for producing the live content;
- Getting notifications - Here the user obtains the possibility to get push notifications when live content is available. In addition, the user can be informed if data offloading to nearby edge servers is available e.g., for decreasing the user device energy consumption.

After connected to the platform, the user can launch the designated application and DEDICAT 6G will be responsible for realizing the wanted service.

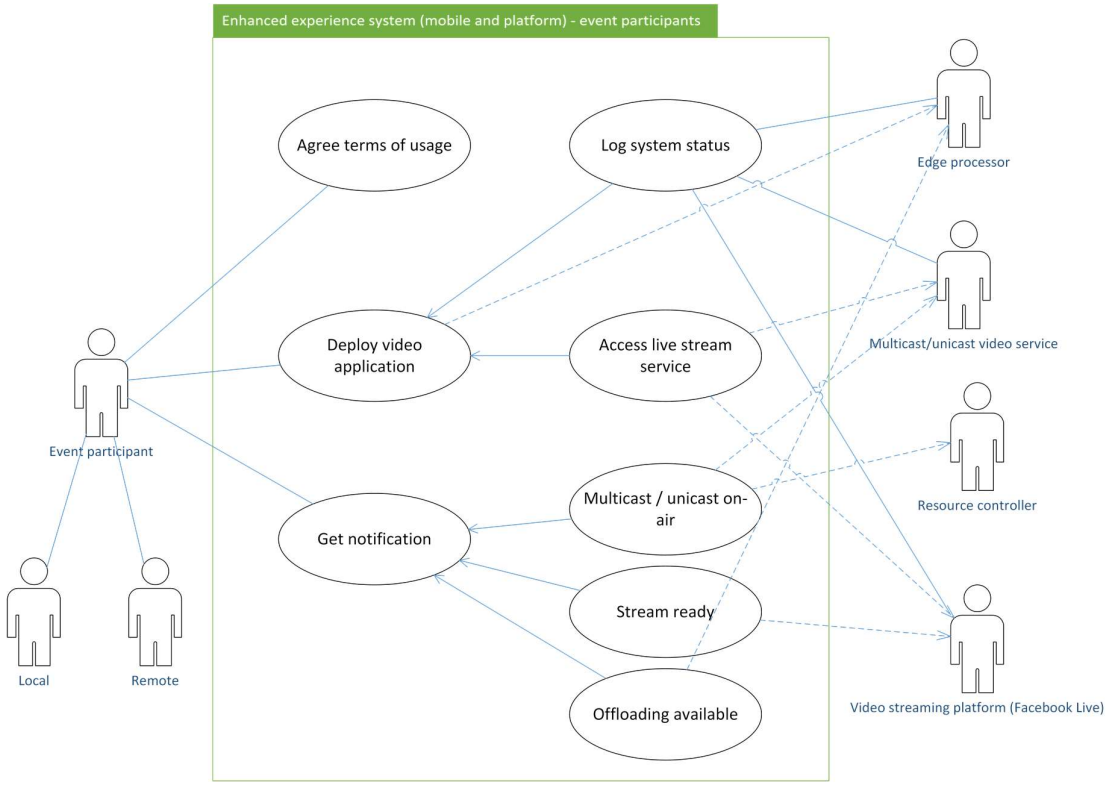


Figure 11 - UC2 Enhanced Experience – UML diagram for event participant interactions.

Figure 12 below shows how the local event participant interacts with the functionalities of the DEDICAT 6G platform. There are two types of local participants acting either as live content producer or live content consumer. Both types of actions are not possible simultaneously. The local user needs to access the following functionalities:

- Adapt terms of edge offloading – here the user consent that the produced or consumed data can be processed partially elsewhere than in UE and some of the network-level data can be identified;

- Deploy Smart Glasses – here the local user possesses the Smart Glasses together with mobile UE connected to DEDICAT 6G platform for producing 'see what I see' content to local and/or remote users via Facebook Live video platform;
- Deploy legacy video application – here the local user deploys legacy video streamer or player and connects with the DEDICAT 6G platform. This option should also outline the baseline for the dedicated enhancements;
- Deploy DEDICAT 6G video application – here the user application possesses the DEDICAT 6G functionalities that enable more efficient playback experience and outperforms the legacy applications in terms of basic KPIs, such as energy or time. The DEDICAT 6G applications are relying on intelligent network management via sophisticated edge processing and resource allocation, or dynamic multicast vs. unicast streaming techniques;
- Get notifications – the user can be informed for essential information via push notifications, such as available live content.

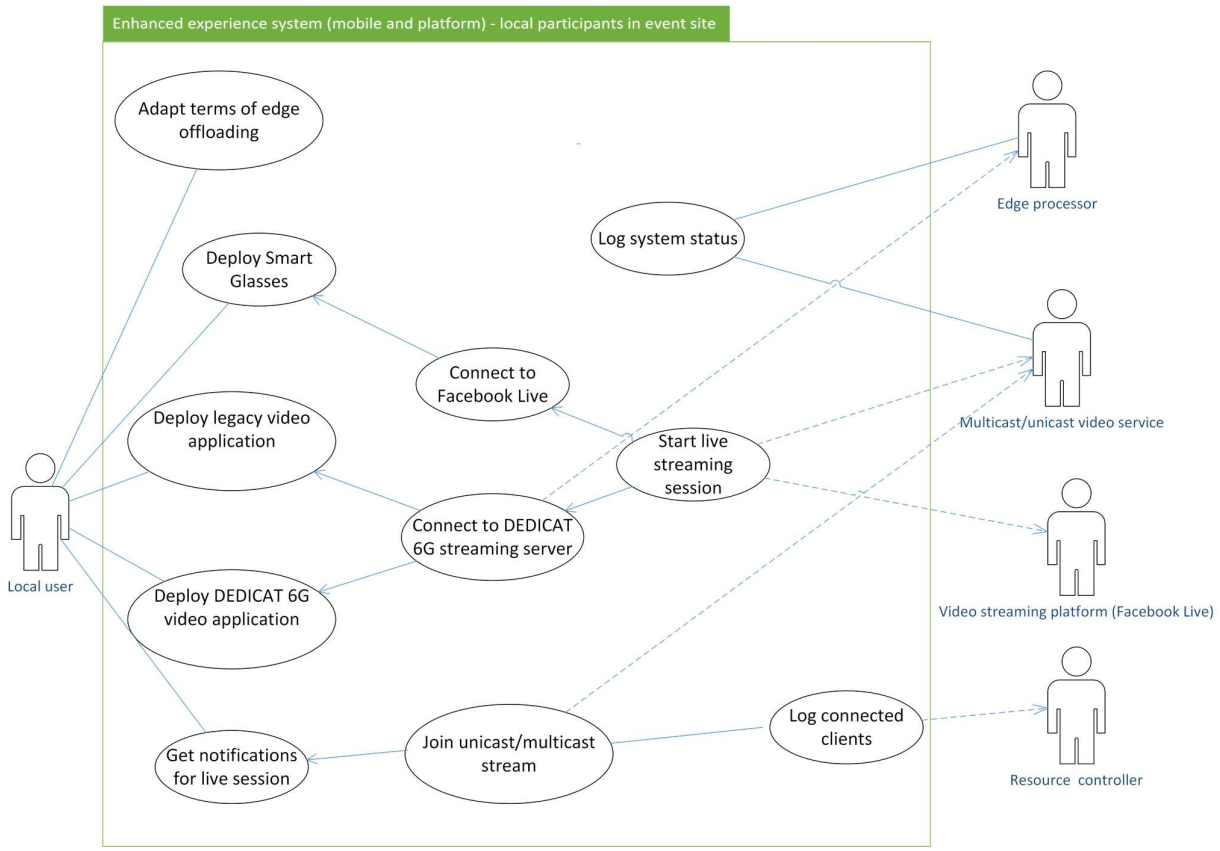


Figure 12 - UC2 Enhanced Experience – UML diagram for local participant interactions.

Figure 13 below shows a somewhat similar figure for remote event participant as the previous one for the local user. The remote user is not considered to produce any content but barely to consume the content offered via DEDICAT 6G platform. The following functionalities are identified:

- Deploy legacy video application – here the remote user selects the wanted player application able to playback the Facebook Live content. The legacy applications can have different characteristics in terms of optimizing latency and quality;

- Deploy DEDICAT 6G video application – here the user possesses the developed video application interconnected with the optimized characteristics of DEDICAT 6G platform. The application should have interconnection with the DEDICAT 6G multicast/unicast streaming server able to switch dynamically between the multicast/unicast channel depending e.g., on the number of simultaneous users or network condition;
- Get notifications for live session – here the user will get push notifications to UE screen when live content is available.

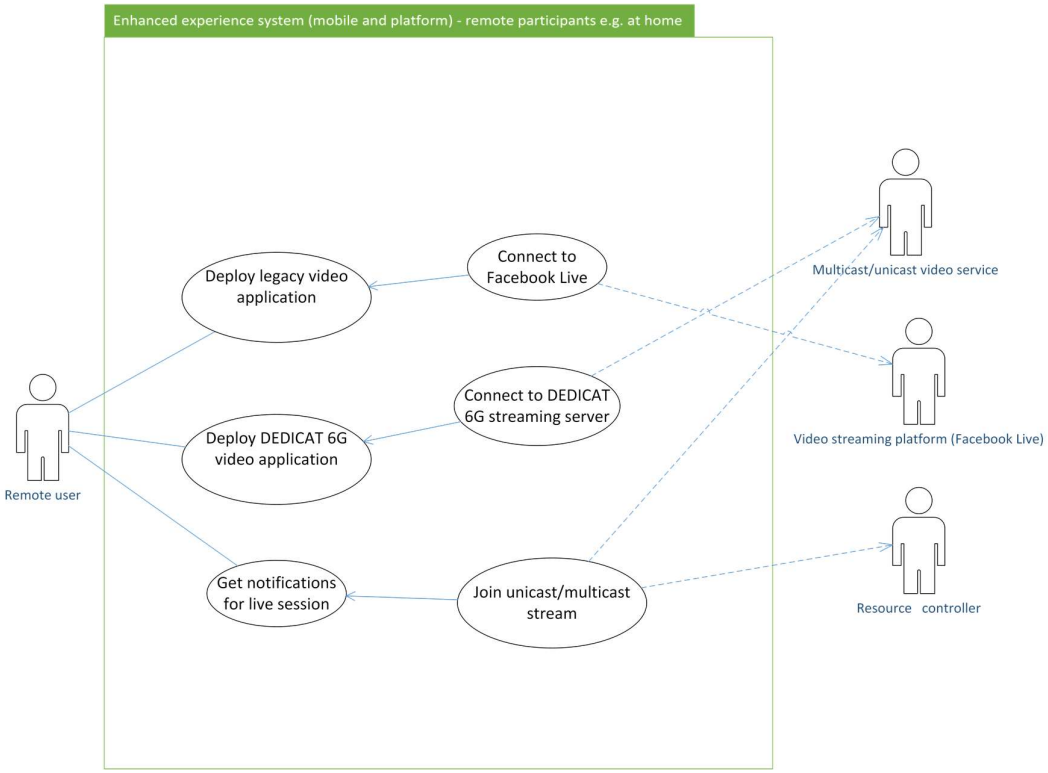


Figure 13 - UC2 Enhanced Experience – UML diagram for remote event participant interactions.

Figure 14 below presents how edge processor interacts with the DEDICAT 6G functionalities by forming a connection between multicast/unicast video services in order to establish enhanced resource allocation for data processing. The main functionalities are:

- Receive data – Edge processor receives video data either in bursts or in steady continuous way and performs video transcoding for multiple qualities (bit rates) for enabling adaptive streaming;
- Receive QoS parameters – The QoS parameter set from users is essential in order to allocate proper resources for the data computing/processing. The QoS parameters basically define the depth of processing, and to which edge the request will be forwarded. The QoS values latency, power, best-effort and price are the main ones in this case;
- Log system statistics – The edge processor should maintain and log the system statistics and provide key essential values, such as processing time and cost.

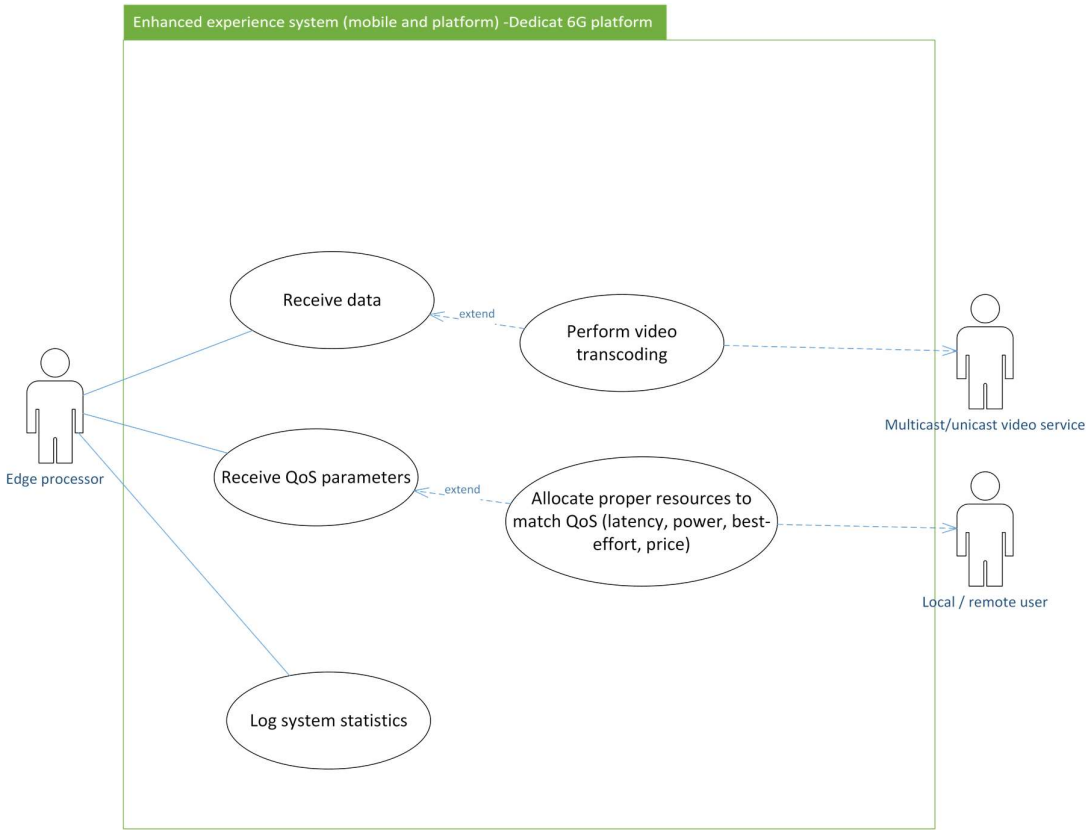


Figure 14 - UC2 Enhanced Experience – UML diagram for Edge Processor interactions.

Figure 15 below shows the UML diagram for the resource controller and its interactions with the DEDICAT 6G platform. The resource controller works closely with the edge processor(s) for selecting the proper edge matching the QoS. The following functionalities are identified:

- Calculate threshold for mode – Here the resource controller defines according to the network statistics whether unicast or multicast mode should be used for the video transmission;
- Log connected clients – The resource controller logs the number of connected clients for the video service;
- Log network statistics – The resource controller logs the network statistics in order to provide better quality for the end-users. This information contains values such as latency and throughput;
- Find suitable edge to match target set of QoS – The resource controller is aware of all the available edge processors and interacts with the QoS parameters for finding the proper edge for specific purposes;
- Inform if offloading is possible – The resource controller informs the user if offloading is even possible in case of all the resources might be in use;
- Find suitable mobile AP – Here the resource controller will search for available mobile access points for coverage enhancements.

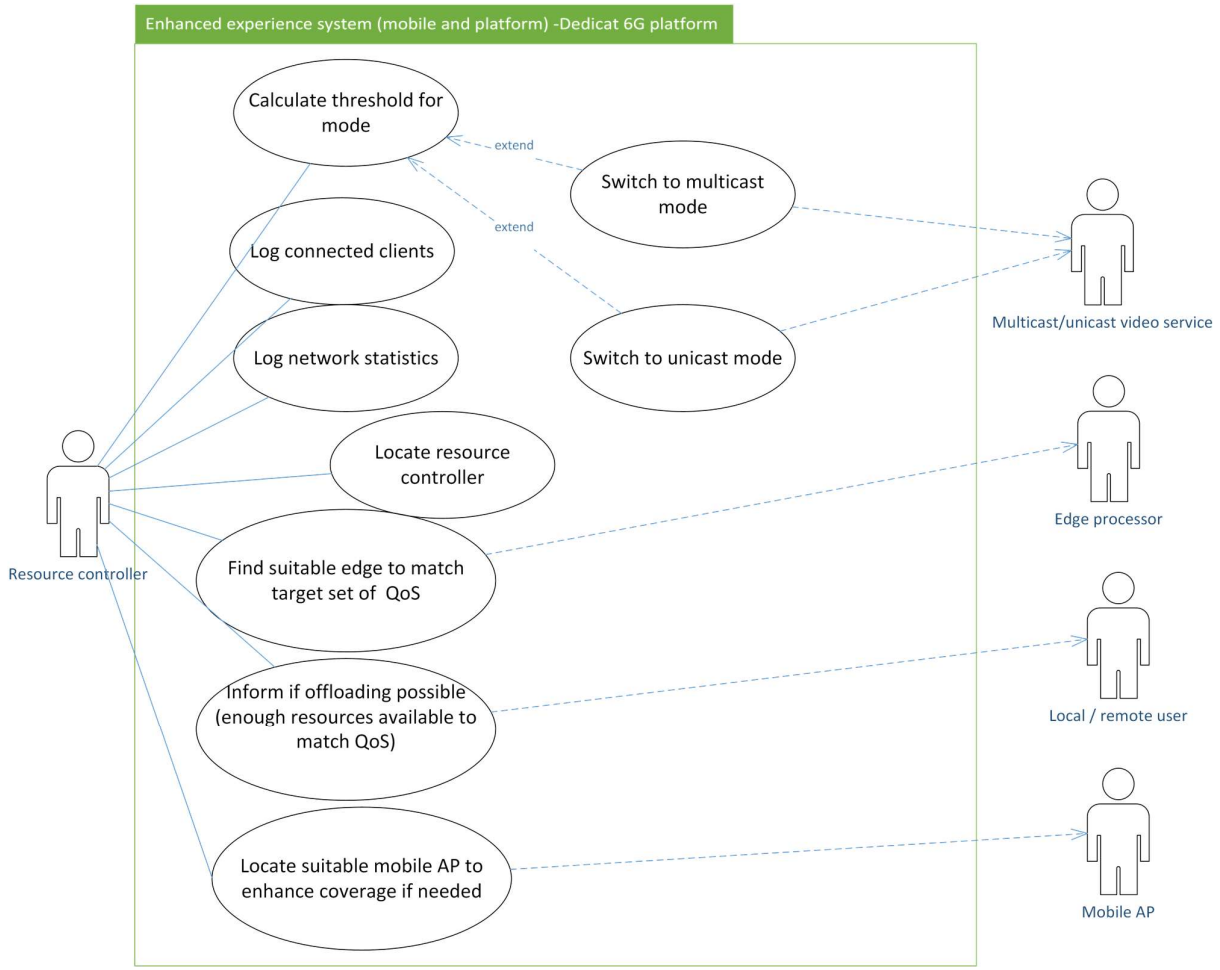


Figure 15 - UC2 Enhanced Experience – UML diagram for the resource controller and its interactions.

4.2.2.3 UC3 – Public Safety

The Public Safety use-case defines two contexts. Each of them encounters different type of safety or security organizations and citizens who are at risk to become a victim. DEDICAT 6G platform delivers to them Edge Communication capability and interfaces to their systems in order to maintain operational information system during the crisis management.

The main actors of the platform are:

- External Operational system: this system which is owned by the organization and interfaces with DEDICAT 6G. This Operational System delivers to First Responders and PPDR users all operational information needed during crisis management;
- Field Officer (Police, Firefighter or Medical): They are responsible for managing resources and assets deployed in order to respond to the crisis. The officer is registered and connected to DEDICAT 6G system to be able to communicate with field operational resources (share information and orders), to monitor the situation and to receive updates on tasks and assets availability;
- Field Resources (Police, Firefighter or Medical): They perform operational tasks on the field to respond to the crisis, support security and safety. They are supported by the DEDICAT 6G platform during the response to crisis;

- Operator manages the situation from Mobile C&C or C&C. He is responsible in operational information sharing;
- Security staff: private security resource who are in charge of managing private area and buildings (event, concert, etc.)

The next Figure 16 describes the high-level interactions between the main DEDICAT 6G functions and the external systems and users who need DEDICAT 6G support for response to crisis.

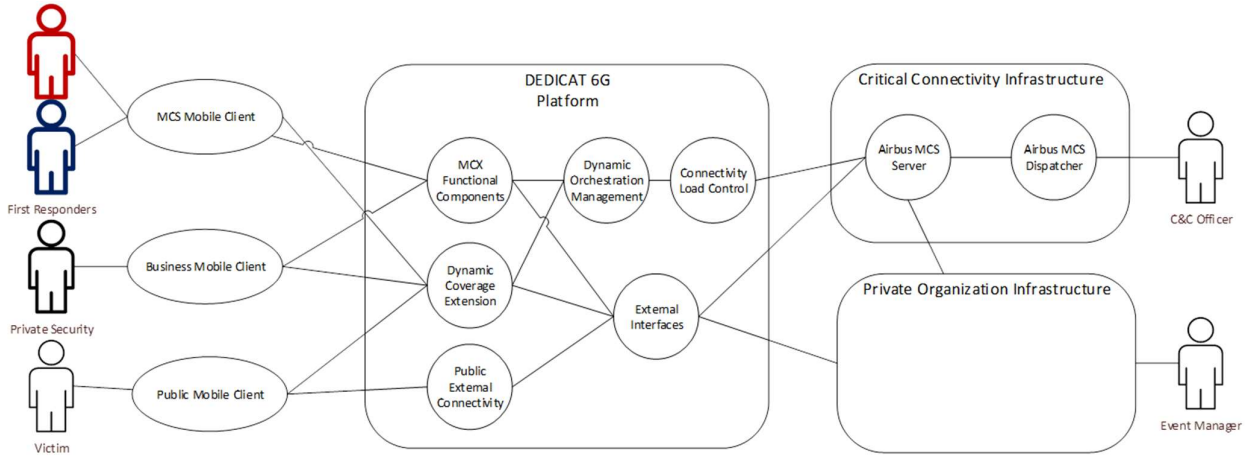


Figure 16: UC3 "Public Safety" - High Level View

Adding to the capability of DEDICAT 6G platform in term of Dynamic Coverage extension, the platform will be able to deliver Mission Critical Communication features to support Response to Crisis.

The key elements presented by the figure are:

- "Mobile Client": the Mobile Client allows First Responders (or PPDR users) to access to the DEDICAT 6G services through a single authentication process;
- "Critical Connectivity Infrastructure": the Critical Connectivity infrastructure offers to First Responders (and PPDR users or Private Security) a secured access to their standards operation information, but which are not available during the crisis (loss of or overloaded communication infrastructure in both UC3 contexts). The Critical Connectivity infrastructure is connected to the DEDICAT 6G platform through external interfaces;
- DEDICAT 6G - External Interfaces: DEDICAT 6G offers a secure connection to First Responders organizations in order 6G users are able to access specific operational and private data for managing the critical situation.
- DEDICAT 6G - Connectivity Load Control: DEDICAT 6G feature allowing the monitoring of the load of the network in order to support First Responders to use the appropriate communication link (DEDICAT 6G or operated if available);
- DEDICAT 6G - Dynamic Orchestration Management: DEDICAT 6G feature orchestrating different MCX components on the DEDICAT 6G Edge;
- DEDICAT 6G - MCX Functional Components: this feature of DEDICAT 6G delivers multiple components in order to offer Multimedia Communication Services, as described in the 3GPP MCX release 13, to DEDICAT 6G users, especially First Responders and PPDR users. This feature will deliver all the services in some independent components in order to make the services resilient and offer best Quality of Services depending on the needs of First Responders on crisis scene.

The following Figure 17 describes the interaction of First Responders on the field with the DEDICAT 6G platform and how the DEDICAT 6G platform will deliver MCS services to First Responders.

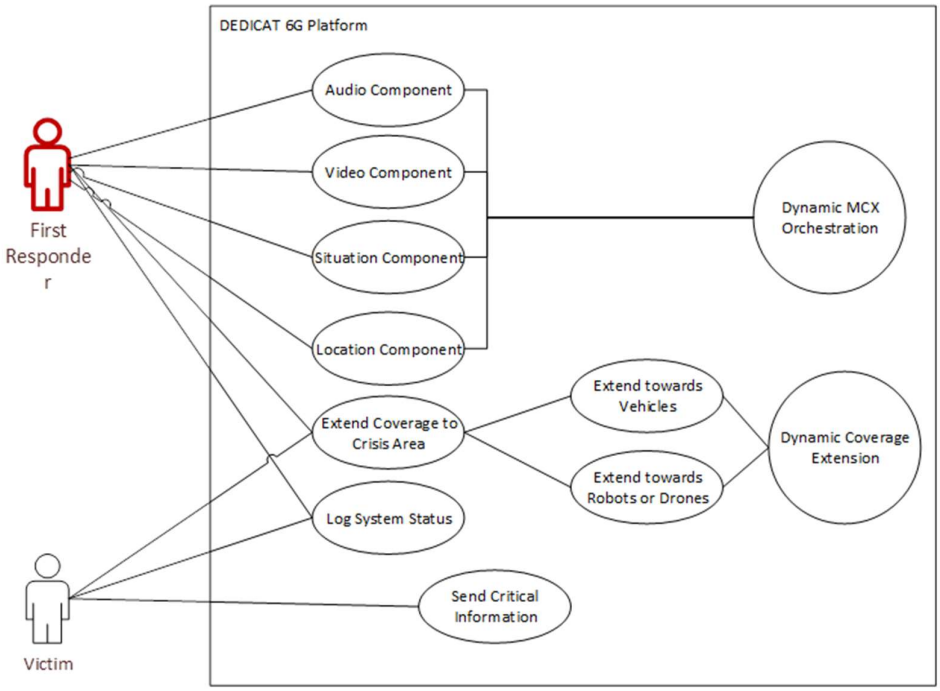


Figure 17: UC3 "Public Safety" – First responder / DEDICAT 6G interactions

The needs for First Responders are to be able to communicate on the scene and share relevant information.

When First Responders (Police, Firefighter, Medical or Private Security) are facing a lack of connectivity, in order to use the DEDICAT 6G platform, they need to:

- Initiate the MCS Mobile Client in order to connect to the DEDICAT 6G platform;
- Authenticate to the MCS services in DEDICAT 6G platform;
- Register in the platform with the level of authorized use;

The key features delivered registered First Responders are:

- Car Connected Extension / AVG Extension: 6G / B5G coverage extension to the scene in order to support MCS services connectivity;
- Audio connectivity: Push-To-Talk over IP feature and full-duplex audio communication. The component can be delivered on the Edge;
- Video connectivity: Real-time video streaming. The component can be delivered on the Edge;
- Situation component: transmits operational situation of First Responders on the scene to organization infrastructure and situation sharing with all responders involved in the crisis management (Responders on the field, Field Officer, Operator) and allows resource management and decision making;
- Location component: transmission of operational location of First Responders on the field to organization infrastructure. The location is shared on the different MCS Mobile Clients and supports the Decision Making during the crisis management.

The following Figure 18 describes how the DEDICAT 6G delivers services for Mission Management and interactions between Responders. During the Crisis Management, the area of intervention can be potentially wide with difficult terrain. DEDICAT 6G, based on Dynamic

Edge deployable component can deliver the best services needed for decision making (video streaming for situation awareness, location and situation for decision making based on situation awareness and voice for Mission Critical Management).

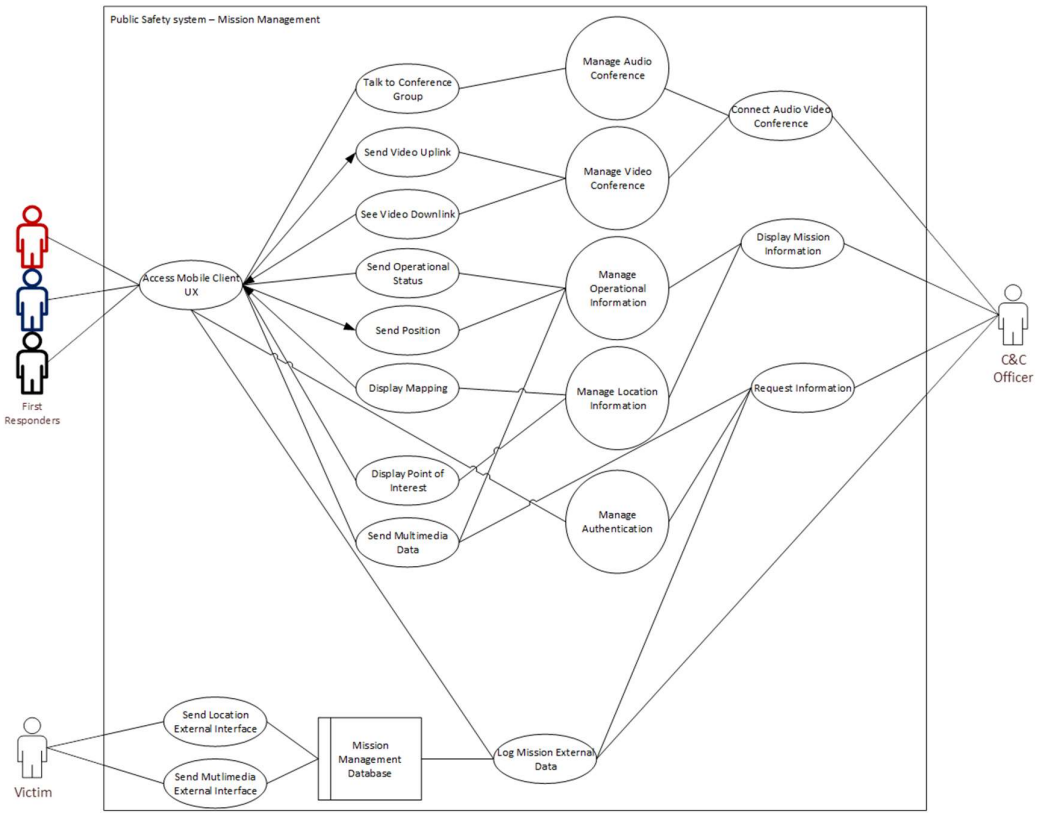


Figure 18: UC3 "Public Safety" – Mission management service delivery by DEDICAT 6G

4.2.2.4 UC4 – Smart Highway

Smart Highway (V2X application)

The Smart Highway use-case works with future *Internet of Vehicles* (IoV) applications such as the *Local Dynamic Map* (LDM) application. The LDM objective is to identify obstacles and users present along the course of a vehicle. These obstacles and users can be identified in two ways: by sensors or by informing their GPS coordinates. Therefore, in this use-case, we have two main actors: The users and the sensors. These two groups of actors will interact with the LDM app by feeding the necessary data, so the application keeps the LDM updated and support road users to be aware of road status (see Figure 19 below).

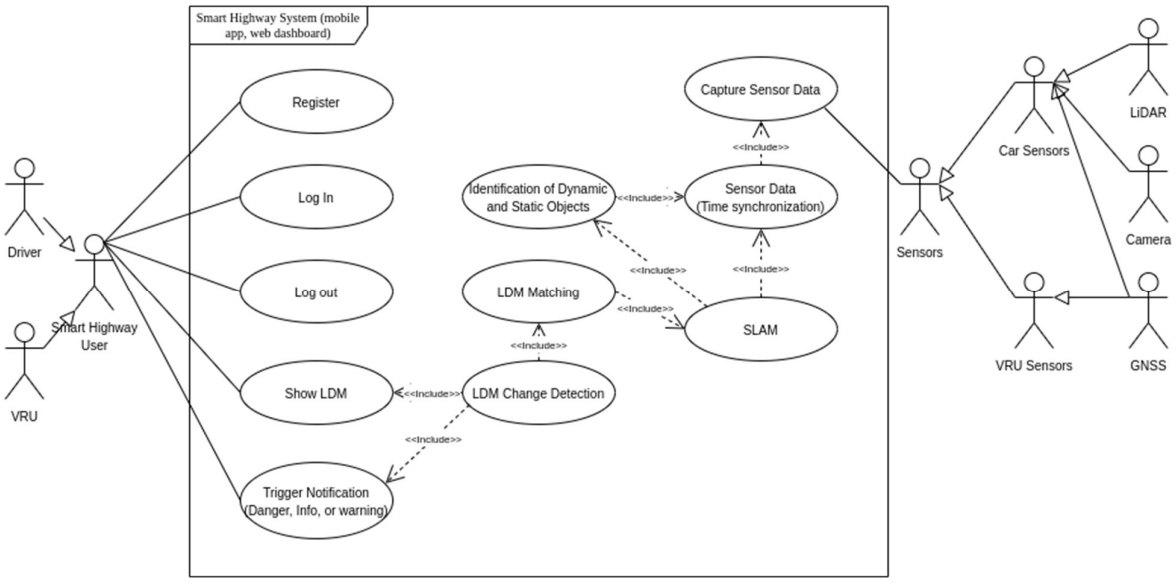


Figure 19: UC4 "Smart Highway" - V2X application

A Smart Highway User is anyone registered and logged in to the LDM app server. We identified two main actors that are users of this application: the Driver and the *Vulnerable Road User* (VRU). The Driver is the actor driving a car that can be a smart car or a conventional car. The VRU is any other user, e.g., pedestrian or cyclist, near a road and would like to collaborate or receive information about road status. Furthermore, the Car Sensors is an actor group that will provide raw data information to process and identify obstacles and road information. This type of actor can be a LiDAR, a Camera, or a *Global Navigation Satellite System* (GNSS). The LiDAR and the Camera operates with the primary objective to identify the car's nearby environment while the GNSS will provide the car's self-positioning to the Smart Highway application.

A Smart Highway User can avail of the features of the LDM app by Registering to the application. Moreover, the user will need to Log In to the system, having the possibility to Log Out from the app afterwards. Having the user logged in to the system, any of the Smart Highway Users will watch in real-time the LDM and check the road status. If the application detects any danger or essential information to send to the user, it can trigger a notification with the necessary message. The detection of Danger or Warning situations is done after collecting information from the Car Sensors. As aforementioned, there are three types of sensors: LiDAR, Camera, and GNSS. The LiDAR and the Camera are present in the Smart Cars, while the GNSS are present in both Smart Cars and the VRUs. The raw data from these sensors are sent to the LDM app server, where the time of the data is synchronized. The raw data from the LiDAR and the Camera are processed to identify obstacles and other users. These identified objects are used for *Simultaneous Location and Mapping* (SLAM), which will provide an updated version of the LDM. This version of the LDM will be compared to the previous status of the LDM, and if any change is identified, the LDM app updates the LDM for the Users, and, if necessary, a notification is triggered.

Smart Highway (distributed intelligence network)

The DEDICAT 6G system supports the Smart Highway by providing Vehicular Edge Node and Mobile Edge Computing servers to support task offloading for vehicular processing-intensive applications such as LDM data gathering and processing (Figure 20 below).

For this use-case, we identified three groups of system actors: Application Owner, Hosted Application, and Edge Node. In addition, the Edge Node can be specialized into Vehicular Node or Stationary Node, distinguishing behaviours when the Edge Node is a vehicle.

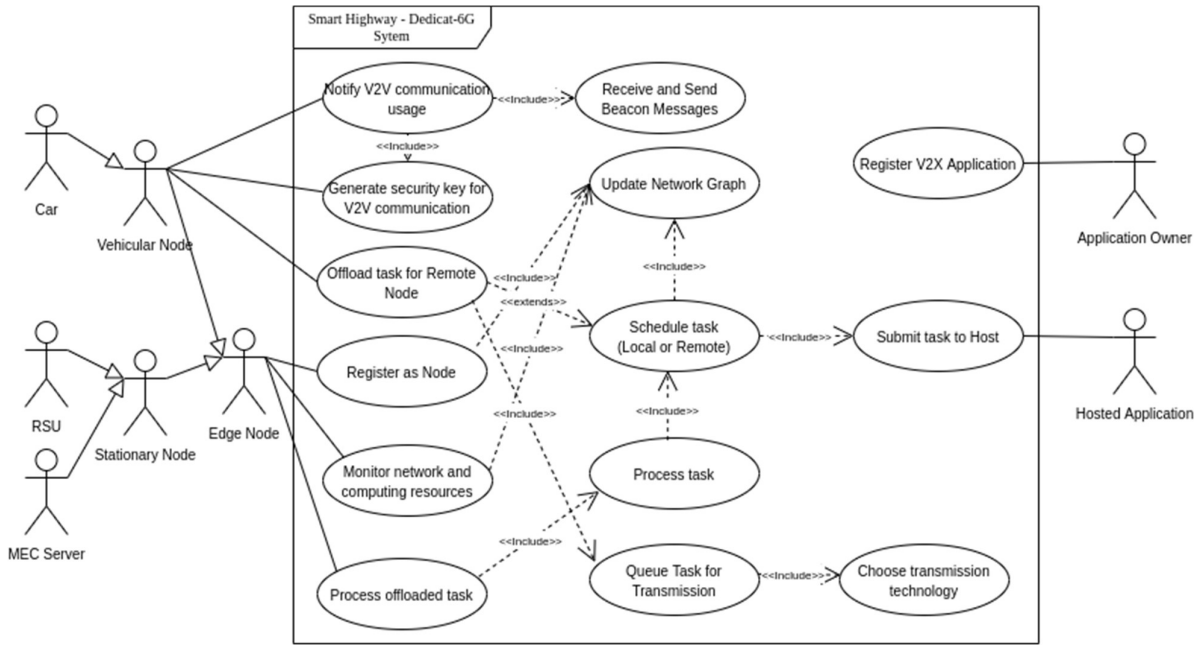


Figure 20: UC4 "Smart Highway" - Distributed Intelligence Network

When the infrastructure is turned on, the *Edge Nodes* (EN) register to the DEDICAT 6G system and make their resources available for usage. With a newly registered node, the system updates the network graph for the network orchestrator. From this point on, the Edge Nodes start monitoring the available computing and network resources. With the received information about network and computing resources from the Edge Nodes, the DEDICAT 6G system can update the network graph with the status of each EN's network links and processing capabilities. In a *Vehicular Node* (VN), the system also generates a security key to enable secure V2V communication. With the security key received, the VN can enable the V2V communication and notify the server that this feature is enabled. After enabling the V2V communication, the VN starts sending and receiving beacons from nearby vehicles. The beacons transport information about the computing and network capabilities of the VN for the nearby vehicles.

With the EN set up in the network, the Application Owner can register a V2X Application used by Vehicles and Vehicular Nodes. The application client runs on the Vehicles of the Smart Highway. The application can submit tasks for the host to process. With the task details uploaded together with the task, the VN can decide if the task is going to be processed locally or it is going to be offloaded to another VN or Stationary Node (SN). After deciding where the task will be processed, the VN schedule the task to be executed. If the task will be processed remotely, the VN must communicate to the remote host and reserve processing capabilities. However, the VN may have multiple radio network technologies available. Therefore, before making the reservation, the VN is required to choose the network technology to be used for communication with the remote node. Then, the VN offloads the task for the remote node, which returns the result of the task afterwards. If the VN is the remote node, it receives the request for processing a task, schedules the processing of the task, receives the task, and processes it. By the end of this sequence flow, the VN returns the result to the processing request source.

4.3 Functional View

In this Section we shed the light on the main functional pillars of the DEDICAT 6G architecture as outlined within the DoA. We also give a preliminary list of Functional Components that are necessary to achieve the technical objectives and realize the vision of the DEDICAT 6G project. Those components were identified through analyzing the FREQs on the one hand and from resolving the perspectives on the other hand (via NFREQs analysis and Design Choices).

The first section introduces and describes shortly those pillars (Functional Group), before delving into each one of them, elucidating the Functional Components they are made of.

Most importantly, we conclude this section with a set of System Use-Cases that gives a glimpse at some of the main system scenarios that will take place during DEDICAT 6G platform operation. In particular we elucidate the interactions that take place between DEDICAT 6G FCs and the supporting 5G legacy network that DEDICAT 6G is expending with novel functionalities (e.g., Dynamic Intelligence Distribution and Dynamic Coverage Extension).

4.3.1 Introducing the DEDICAT 6G Functional Model

This section sets the foundation of the functional decomposition by identifying the essential FGs the DEDICAT 6G (cloud and edge) platform will be built upon. It also sets the different abstraction layers, one or several FGs may belong to (see Figure 21 below).

During the requirement mapping activity taking place at the end of the requirement process, we identify which FG a given requirements fits in and start identifying relating FCs. The result of this process is the Functional Decomposition.

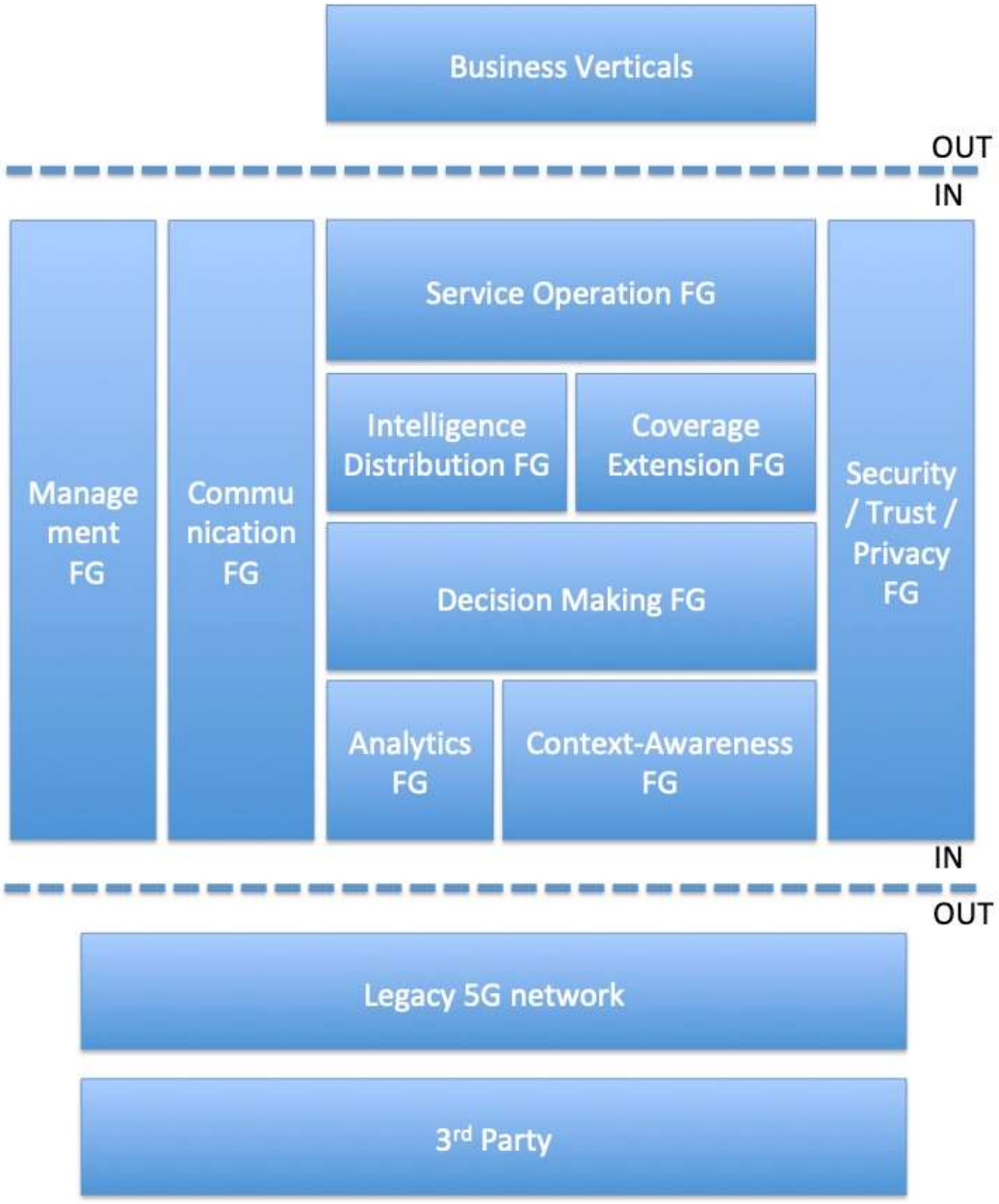


Figure 21: DEDICAT 6G Functional Model

We now explain each of the Functional Groups inside the perimeter of DEDICAT 6G and the nature of the FCs they are hosting:

- **Service Operation FG:** This FG deals with FCs that are responsible for implementing the decisions carried out by the Decision Making FCs. This includes in particular Network Services and micro-service (µService or µS) orchestration, load balancing of FCs and resource management;

- **Coverage Extension FG:** this FG contains FCs that are supporting the dynamic coverage extension like MAP dynamic ad-hoc routing, autonomy management, placement management, etc.
- **Intelligence Distribution FG:** this FG contains all UCs that are supporting the Intelligence Distribution like registries and repositories for the MEC and associated look-up /discovery functions plus *Service Level Agreements* (SLA) and migration policies storage; those FCs are used by both the Context-Awareness FCs and Decision Making FCs;
- **Decision Making FG:** this FG hosts FCs dealing with all aspects of using available information and knowledge provided by Context-Awareness layer in order to take decision (applying various IA algorithms) about e.g., migrating FC due to (envisioned) poor network performance or network failure, deploying drones (via the Management FG), acting on the legacy network to increase capacity of functioning base stations;
- **Context-Awareness FG:** this functional group contains FCs that are used to build up "contexts" that FCs from the Decision Making FG can base their decisions on. More precisely a context is a collection of pieces of information that gives the needed level of detail and characterization of a system state (or space). It is usually initially based on raw data, which is enriched using various methods (like correlation, analytics, machine learning) in order to reach the level of "knowledge" (following the well-known Data-Information-Knowledge-Wisdom classification [10]). The FCs can then use this knowledge in order to take proper decisions concerning various sorts of problems (e.g., Coverage Extension or Intelligence Distribution). In DEDICAT 6G we maintain various sorts of context that focus on specific matter. The accuracy of a context is paramount in order to ensure that a related decision is taken while the context is still valid and relevant. In order to optimize this accuracy, we have to ensure that the refreshing time (raw data sampling rate) is appropriately chosen and implemented at the awareness agents sides;
- **Analytics FG:** this FG contains FCs dealing with data analysis for various purposes e.g., for providing better QoE/QoS to user, or decreasing the UE processing by shifting the computation to edge nodes. The Analytics FG contains FCs such as network optimization and analytics toolbox aligned with in particular performance monitoring and decision making needs.

In addition, we have three transversal FGs in which the FCs are expected to potentially interact with all FCs from the six previous FGs:

- **Management FG**: this functional group includes all aspects of DEDICAT 6G management (see FCAPS classification) e.g., monitoring of deployment, of network performances, or system failure, dashboards, User-to-System web interface, and all aspects of PST management (e.g., account, key management and ACL management) etc.;
- **Communication FG:** this FG contains FCs that can be used to ensure inter-FC communication like for instance message bus and HTTP/RESTful-based communication;
- **Privacy/Security/Trust FG**: This FG contains all FCs that are needed to fulfill the requirements in term of Security, Privacy and Trust. This includes blockchain-related FCs, identity management, authentication/authorization, trust management, non-repudiation/accountability, audit and more;

4.3.2 Description of DEDICAT 6G FGs and FCs

4.3.2.1 Service Operation FG

The FCs in that FG are aiming at implementing the decisions taken by the IDDM.

- **Orchestration FC:** This FC executes the outcomes of the Decision Making FG, that is from Network Operation and Intelligence Distribution Decision Making FCs to

physically deploy other DEDICAT 6G and vertical FCs and 5G network components towards the selected Edge Nodes. It is also devoted to providing the configuration needed for the correct operation phase in the components, including day-2 operations, if the DM components request it;

- **Load balancing FC:** This FC provides support for inter- and intra-node load balancing between the FCs. This feature is applied to service and networking components due needed for the distributed nature of the micro services to be onboarded. The policies for load balancing the FCs need to be described in the Policy factory FC and processed by the Decision Making FCs (e.g., NODM and IDDM) to request the Load Balancing FC to create the required functionalities.

4.3.2.2 Intelligence Distribution FG

This functional group stores the registry and the metadata of both the vertical applications that are uploaded to the platform, as well as of all the edge nodes that are going to be used. It serves as the backend endpoint for the users in the DEDICAT6G platform, since the service to be rolled-out with all the associated policies and SLAs, and also the edge nodes and their capabilities are inserted in the inner functional components of this group.

The data formats associated with Edge Computing polices, SLAs and Edge nodes are elucidated in the Information View and will be available in deliverable D2.4.

- **EC Policy Factory FC:** This FC collects the information about the fine-grained policies that are applied to each vertical application in order to deliver an optimal deployment and configuration (in particular fulfilling the QoS/QoE described in the SLA factory FC). Such an EC policy can be set-up by a business vertical application that wants to use the Intelligence Distribution capabilities of the DEDICAT 6G platform in order to deploy either its own components or DEDICAT 6G native FCs towards the edge (i.e., either towards 5G legacy equipment or towards its own deployed IT EC-ready equipment). In order to facilitate the decision-making process, a policy issued by a vertical must provide the "logic" of deployment and execution especially when that logic is depending and based on characteristics (which belong to the service semantic itself) that are not covered natively by the various awareness and status agents. Making those characteristics explicit in the policy allows the Decision Making to know which elements of context have to be tracked in order to have a business-dependent Decision Making process. In addition, any such vertical FC MUST instrument the awareness FCs and status agents FCs with the proper information about those "semantic" characteristics. The implementation of such a component must "encode" this knowledge using either a dedicated language (rule-based e.g.) or through a dedicated data model (for the static cases);
- **SLA Factory FC:** is used to negotiate a QoS/QoE contract between the DEDICAT 6G and the vertical application that wants to rely on the DEDICAT 6G to help running its business applications. When the contract is agreed upon, the DEDICAT 6G platform may engage into deploying components and scaling up network resources or certain services of the vertical components according to EC policies and required QoS/QoE (note that QoE is probably translated into QoS indicators eventually);
- **Edge Node Registry FC:** This FC stores information about any Edge Node capabilities, this includes in particular (the complete information model will be detailed in further deliverables including D2.4 Information View):
    - CPU computational power (OPS/FLOPS);
    - Number and type of processor cores;
    - Availability and properties of SIMD units (per core/per processor);
    - Availability and properties of video computing/transcoding accelerators;

  - L1/L2/L3 cache, RAM and Storage space;
  - Memory system throughput (L1/L2/L3 caches, main memory);
  - GPU computational power and RAM;
  - SSD or HD enabled;
  - Maximum SSD/HD read/write speed;
  - Power consumption of execution and I/O units as the function of performance (DVFS, #active cores, power saving modes);
  - Maximum available network I/O bandwidth (comm. Wise);
  - Available virtualization interfaces (Openstack/Kubernetes/Docker, etc.);
  - Available Radio interfaces;
  - Type (Drone / Connected Car / Robots);
  - Autonomy;
  - Administrative Domain/Region;
- **Edge node discovery and lookup FC:** This FC maintains the list of Edge Nodes exposing its capabilities for supporting matching search criteria. This component returns an Edge Node handler or endpoint for exploiting it;
- **µService Registry FC:** gives a list of operating requirements such as:
  - Needed computing power and RAM;
  - Needed GPU computing power and RAM;
  - Needed video computing/transcoding capability;
  - Needed communication bandwidth;
  - Needed storage space or performance;

  Defining such requirements will therefore allow selecting candidate hosting Edge Nodes according to the best of their capabilities. To get a working result, the current status of the Edge Node is also to be taken into account. In order to accommodate a large number of different Edge Nodes having their own characteristics, we may have several implementations of the same components with scaled-down requirements (for its the light-weight versions). This will allow, when considering a given functionality, to deploy the version of the code that fits best the targeted Edge Node or – in general- available Edge Nodes according to their current status or capabilities. This strategy increases the global availability and guarantees an optimal performance of a given functionality throughout the whole network with the cost of extra hardware and more complex management;
- **µService Repository FC:** provides the basic functionality for uploading a µService/agent and registration (meaning providing a service description that can be used for deployment and discovery). All the metadata and images related to the service are hosted in the µService Repository FC;
- **µService Discovery and Lookup FC:** This FC maintains the list of criteria matching services. It returns a service handler or endpoint for exploiting it.

4.3.2.3 Coverage Extension FG

- **Swarm Operation FC:** This component is deployed at the different nodes involved in Coverage Extension with the purpose of MAP (such as UAV and AGV) self-management based on high-level instructions initially released by the Decision Making (i.e., CEDM). It means that the Decision Making is not responsible for the "basic implementation tasks" of a deployment decision. Therefore, this FC allows a swarm of MAPs to perform their routine tasks autonomously with the distribution of master & slaves roles among the mobile entities. The tasks performed by the Self-organizing FC covers:
  - Self-organizing as an ad-hoc network;

- Optimization of MAPs placement in order to fulfill the CEDM coverage area constraints;
- Optimization of MAP operation according to the overall requirements from the CEDM, assuming that the MAP drones/robots do not necessarily have the exact same characteristics (e.g., supported radio carrier and interfaces, autonomy, freedom of movement, etc.);
- Self-management of resources including autonomy (e.g., how frequently and where does a MAP have to get back to its docking station);

As mentioned above the overall operation planning will result from "negotiations" between an individual (the "Master") and the rest of the MAP swarm (the "slaves").
The swarm of MAPs may be contacted anytime by the CEDM for the sake of changing essential mission parameters or simply to stop/resume/end-up the mission (which result into terminating communication and performing a global return to assigned docking stations);

- **Connected cars Operation FC:** this component supports similar features than AGV for the deployment of Mission Critical Services on the Edge with needed specific power supply for connectivity resiliency. Regarding the size and the autonomy needed, AGV features have to be delivered by car for Public Safety use-case. Operationally, Connected Cars could be part of Mobile C&C truck or specific cars deployed on strategic places in order to extend the coverage. These strategic places are supported by the analysis conducted by drones.

4.3.2.4 Decision Making FG

There are different purposes to Decision Making in the DEDICAT 6G projects and radically different technologies can be used. Examples are Fault Recovery, explicit coverage Extension (on-demand CEaaS), Congestion Handling, etc.

- **Network Operation DM (NODM) FC:** this component generates the decisions about the network provisioning and maintenance, keeping the optimal operation of the network based on data it receives from the various Context-Awareness FCs and from optimization recommendations issues by the optimizers FC (see Analytics FG). Besides, it is responsible for handling network degradation resulting from faulty equipment or network saturation. It may trigger actions from the Coverage Extension DM FC in case network extension is needed to palliate the defect of network equipment's or to expand the capabilities of the network in a certain area.

  The NODM process the recommendations and create the concrete actions to perform in the network infrastructure to fulfill the vertical application topology, requirements and declared SLAs. These actions describe the network elements that are involved in the operation and the configuration that needs to be applied on them. Finally, they are forwarded to the Service Operation FG for applying the operations in the infrastructure. The NODM FC relies on recommendations and performance indicators from the Analytics and Context-Awareness FGs;

- **Coverage Extension DM (CEDM) FC:** The key aim of this component is to produce the optimal configuration of the radio network of the *Mobile Access Points* (MAP) entities and the paths (trajectories) that need to be followed by the MAP entities, in order to offer adequate QoS levels, in terms of service availability, performance and reliability. This optimization also includes the most appropriate allocation of nodes to MAPs as well as selection of nearby docking/charging stations for drone and robot MAPs to ensure connectivity of the appropriate QoS to mobile nodes. This component may also be utilized for 1) complementing the actions of Network Operation DM FC and 2)

implementing necessary network extension actions needed to fulfill a *Coverage Extension as a Service* (CEaaS) request from a vertical for instance. This component may rely on the IDDM below as part of dynamic migration of intelligence related task, if needed.

- **Intelligence Distribution DM (IDDM) FC:**
  This component is responsible for deciding the optimal placement of intelligence in terms of data and computation as micro-services. The optimal placement of computation and storage at the right place, at the right time considers user and edge node mobility as well as mobility of data sources (data may be collected by devices that move). The aim is to proactively move intelligence along the edge, according to the required and available resources across the DEDICAT 6G system. Relevant aspects include:
    - the placement of micro-services taking into account associated devices and their geographic density, as well as service configuration and maintenance - e.g., scaling or healing based on real-time needs and resources (network, compute) availability;
    - computation migration (among available devices, edge and cloud resources) for adequately supporting mobility of data producers and/or consumers in the scope of diverse applications.

  More specifically, considering 1) a set of micro-services is assumed, defined as the minimal components to which functionality (as part of a broader service) can be fractionated and 2) a set of Physical Systems (e.g., edge nodes, core nodes, robotic units, end-user devices, etc.) then, a specific computational load corresponds to the execution of each micro-service.

  For micro-services exchanging data there is also a corresponding communication cost (depending also on the data transferred, the position of micro-services and physical systems and the type of communication channel).

  Moreover, each physical system is characterized by some capabilities. These are:

    - the maximum computational load;
    - the battery level;
    - the trust level;
    - the type and number of micro-services that can be supported;
    - the number of available CPU cores;
    - the available RAM and mass storage.

  The objective for the Intelligence Distribution Decision Making is to find **the best possible allocation of micro-services to physical systems**, that satisfies a set of capacity and performance constraints, as well as the distribution of network traffic to corresponding *Distributed Units* (DU).

  The factors that need to be considered include:

    - the number of PSs that will need to be activated, assuming the cost (related mostly to energy consumption) associated with the activation of a PS;
    - the computational cost of running a particular micro-service on a particular physical system which is related to the computational load of the micro-service and the maximum computational load of the PS;
    - the cost (latency) imposed by the communication among PSs, which may be related to the available functionality capabilities of the PSs or the availability of the PS to conduct the job (i.e., standby mode);
    - the power consumption cost of running the particular micro-service on the PS;

- the travel distance (in the case of mobile physical entities) of a particular PS to execute the micro-service;
- the waiting time (delay) related to load per device, communication between elements;
- The longevity of the installation (e.g., if batteries are there), related to the battery level.

The following constraints need to be considered as well:

- All micro-services need being assigned to the available PSs;
- All PS capabilities need being respected;
- The capacity constraint of each communicational link should be respected. It is assumed that that the communication cost between two micro-services executed on the same PS, is negligible.

4.3.2.5 Analytics FG

This FG contains the FCs that are monitored and analysed by the DEDICAT 6G platform. This FG is closely related to Decision Making and Context-Awareness FGs where the monitored analytics can be used for directing the system performance towards the predetermined criteria e.g., for decreasing the network load, optimizing network KPIs, or altering the device specific characteristics, such as power consumption. The functional entities can provide the results for evaluating the system performance against the baseline criteria as well selecting optimized network parameters dynamically depending on its state.

- **Network Optimization FC:** Ensuring the desired network coverage and selection of suitable computation server for a set of user applications have interrelated optimization targets. An important common factor is to meet the end-to-end delay targets with minimal cost that may involve various parameters such as number of required stations and their energy consumption. While optimization may involve only either network-related parameters, such bandwidth allocation and user association, the most sophisticated approach is to also include computation-related parameters, such as the CPU rate, of target servers in the network. The optimization framework must be aware of conditions of heterogeneous users that may have different QoS targets and different location-dependent channel characteristics.

  A promising way to maximize the coverage is to dynamically optimize network topology while ensuring adequate frequency resources and interference mitigation. The DEDICAT 6G platform enables sophisticated means for configuring the network topology according to the optimization goals set in the DM FG. A suitable optimization cycle must be carefully selected, especially if the coverage optimization is done iteratively which means that the optimal configuration is achieved after a certain period of time and iterations may consume additional resources. The key asset in dynamic network configuration is the MAP, which can be a ground or aerial based component, as described in Section 4.3.4. Moreover, the limitations (e.g., feasible trajectories, computing capability, and operation times without recharging) of specific MAPs must be considered before reacting to the optimization process. The selected centralization degree of the whole optimization process inherently affects the required interaction between the different involved FCs.
- **Network Prediction FC:** those components are deployed through the network and aim at analyzing the network traffic (using ML/statistical techniques) in order to isolate patterns that can in turn be used to make predictions about future conditions, using AI

predictive algorithms. The predictions themselves can be used by the network optimization FCs or directly used by the Decision Making in order to take actions. Another research direction is to analyse various external sources of information that can help forecasting needed additional Intelligence Distribution and Coverage Extension actions before they are actually needed, in order to maintain optimal QoS objectives. Such possible sources of information - when searching for unusual potential increase in radio coverage need - include e.g., social media, news channels, RSS etc.

- **Platform Performance analytics FC:** This component is responsible for assessing the way the DEDICAT 6G platform performs based on pre-defined KPIs which are assessed regularly relying in particular on the analytics FCs.

  the following KPIs are identified that can be used for network performance optimization, prediction aligned with decision making, edge computing and context-awareness:

  - Overall performance;
  - System utilization rate;
  - CPU utilization;
  - Programmability, flexibility, scalability, availability and usability;
  - Power consumption;
  - Quality of service including latency and throughput;
  - Security level;
  - Cost;
  - Number of users.
- **Analytics toolbox FC:** provides a collection of general purpose Machine Learning algorithms that can be used by other FCs from this FG or also other components from the other FGs like for instance Decision Making-related FCs or Security FCs like Auditing.

4.3.2.6 Context-Awareness FG

The FCs in that group are responsible for building various kinds of context depending on the specific needs of the FCs from the Decision Making FG. It mainly relies on information it can collect from the communication layer and/or knowledge it can gain from using the analytics FCs. Such contexts are part of the main inputs for decision making FCs and includes information and knowledge such as:

1) Computation tasks that need to be handled including corresponding storage and caching requirements;
2) Power consumption requirements;
3) A set of mobile nodes that need coverage;
4) Mobility and traffic profiles of the different nodes;
5) Radio quality experienced by client nodes;
6) Options for connecting to wide area networks;
7) The locations of docking and charging stations for drone and robot MAPs;
8) The current locations of the terminals, client node and MAPs elements;
9) A (potentially large) set of candidate final positions to which the MAP entities can move;
10) The characteristics of potential trajectories that the MAP entities can follow in order to reach the candidate final positions.

MAPs can assume position characterized by latitude, longitude and altitude, i.e., of the form (x, y, z).

In the following list of FCs, we often refer to Status Agents FCs and Awareness FCs for a given purpose (e.g., µService, Edge Nodes, etc.). There is a difference about what data they do report: status agents are collecting raw data and provide information about the collected raw data (information being a data structure with data and meta-data) while Awareness FCs are aggregating and transforming incoming information into knowledge that can be used to take decision. As a matter of fact, information and knowledge can be very different in nature as they are used in different abstraction layers.

The FCs in this group include the following:

- **µService status agent FC:** provides information about the status of a µS (lifecycle, resource consumption etc.);
- **µService Awareness FC:** provides compiled information about a cluster or group of clusters to the µService orchestrator and Edge Load Balancing FC;
- ***Edge Node* (EN) status agents FC:** those components are deployed through the network hierarchically (structured in regions/sub-regions) and reports regularly their status to the local/upper **Edge Awareness FC** (if any) and/or the local Decision Making FC (if any) and or the closest upper **Edge Node Status agents FC** instance until it reaches eventually an **Edge Node Awareness FC**: such status includes CPU/GPU available computation time (expressed in %), available memory/storage, bandwidth, etc. The sampling rate can be changed by upper FC instances; the way status is reported is part of the agent configuration at deployment time, but can also be updated dynamically;
- **Edge Node Awareness FC:** compiles an overall Edge Node context for Decision-making FCs to use (mainly IDDM). To be discussed if that FC is responsible for the deployment of EN status agents whenever a new node appears within its administrative scope, or if the agent deployment is somehow triggered from the top (like the IDDM is notified the new EN creation by the Management plane);
- **Network status agent FC:** those components are deployed through the network hierarchically (structured in regions/domains) and reports regularly the status of the communication network in the region to the local/upper **Network Awareness FC** (if any) and/or local Decision Making FC (if any) and/or to the closest upper **Network Status agent FC** instance, until it reaches eventually a **Network Awareness FC**; The sampling rate can be changed by upper FC instances; the way status is reported is part of the agent configuration at deployment time, but can also be updated dynamically;
- **Network Awareness FC:** compiles an overall Edge Node context to Decision-making FCs (especially the CEDM);
- **Deployment status agent FC:** those components maintains a status about which FCs have been deployed in a given domain, and which Edge Nodes are hosting them
- **Deployment Awareness FC:** compiles an overall Deployment status to relevant decision making FCs.

4.3.2.7 Management FG

- **Dashboard FC:** this Front-End component provides graphical display of analytics or row information, like for instance performance indicators about how the DEDICAT 6G does perform. It also provides access (GUI) to all the configuration and monitoring functions that allow the proper operation of the platform, including FCs from the back-end below, but also configuration functions which are introduced in other FGs:
    - Management of Edge Nodes: declaring capabilities of an Edge Node;
    - Declaring and uploading µServices;
    - Setting-up policies (e.g., deployment policies);

- Negotiating SLA etc.

- **Management FC**: this **back-end** component is the home of all management functions (Fault / Configuration / Accounting / Performance / Security) such as:
  - **Accounting FC:** this sub-FC keeps track of the usage of resources by verticals in order to feed ticketing FC with the proper information for the sake of billing;
  - **Ticketing FC:** this counterpart of the accounting sub-FC, is responsible for billing a vertical application based on its resource consumption and associated service fees;
  - **PST Management FC**: this FC relates to the management and configuration of the FCs belonging to the PST Functional Group (whose main focus is enforcement). It can alternatively act as a front-end to the PST management functions hold at the PST FG side (depending on the case).

4.3.2.8 Communication FG

This FG provides support for inter FC communication - including secured communication - either the FCs are located in the DEDICAT 6G cloud platform, at the edge side of DEDICAT 6G or part of an external physical system legacy FCs (therefore outside the perimeter of DEDICAT 6G). Two different paradigms (and therefore communication channels) are envisioned as follows:

1. **Publish/subscribe:** this paradigm allows a source party to reach various potential sinks by publishing messages on a queue that several sources can subscribe to. Such sources are typically, the awareness and status related agents and other DEDICAT 6G FCs, but also 5G legacy components, which raise alarms/fault/performance related events. Several sinks can then consume that information based on subscription and filtering capabilities (e.g., according to a particular topic, scope, etc.);
2. **Asynchronous one-to-one:** one single source communicates asynchronously with one single sink (e.g., a DEDICAT 6G FC with a 5G Legacy component with the use of REST API).

We therefore propose as a first approach the following FCs:

- **Message Queue Client FC:** The client part of the message queue allows to access the queue for the sake of publishing messages and consuming messages according to the client role;
- **Message Queue Server FC:** the server part of the queue is responsible for managing topic subscriptions, sustaining the flow and distribution of messages issued by Publisher clients to the Subscriber (and therefore message consumer) clients. It is also responsible for connecting with the Logging FC for the purpose of event logging.
- **REST Client FC:** this component stands at the side of a FC that is willing to send a unicast POST/GET/PUT/DELETE message to another FC (in opposition to the Message Queue which is multi-cast);
- **REST Server FC:** Likewise, this component stands at the side of a component which is willing to answer a POST/GET/PUT/DELETE message sent by another FC, as the sole recipient of that message.

4.3.2.9 Privacy, Security & Trust FG

- **AuthN FC:** Authentication functionality applied to end-users. Roles defined on the level of the project and for each UC;
- **AuthZ FC**: Authorization functionality with role and attribute based authorization and access control. Applied on users and devices;

- **IdM FC:** Identity Management functionality used for assigning identity and roles to systems, devices and users;
- **Threat Analysis FC**: this FC performs threat detection, identification and classification and is executed either in centralized or in edge processing nodes. Threat analysis is based on ML models trained and updated on collected system logs. The ML models are performed in federated learning mode with global model running in DEDICAT 6G cloud and local models running on edge computing nodes. Federated learning approach allows for globally defined ML models to be distributed closer to the data sources, perform updates/re-training on the collected data and report tuned parameters to the global model for further performance improvements. All threats will be categorized based on severity/impact and decision making systems will include threat category in their processes;
- **Trust Metrics FC:** FC to be installed at all edge nodes as well as on the central/cloud resources. Trustworthiness metrics are calculated for edge nodes, processes, users and data streams. Trust metric value indicates if a node can join a local network, if process output can be further used, if a user can execute specific rule. Trust metrics are implemented as ML models whose outputs are written on private permissioned blockchain through dedicated smart contracts. This way all stakeholders in DEDICAT 6G instance have access to immutable record of trust metrics calculated for all actors, resources and processes. Decision making processes of the DEDICAT 6G system must consult calculated trust metrics before proceeding with decision implementation or execution. The following trust metrics are envisioned for the DEDICAT 6G system:
    - Device-based metrics - capturing a device's state and feature set;
    - Connection-based metrics - define the connection types which are established in DEDICAT 6G systems;
    - Behaviour-based metrics - capturing the user's and device's behaviour within the observed network;
    - Context-based metrics - expected operations of a node in a known context. e.g., in case of failures;
    - Composite metrics computed based on the weighted calculation of different security, reliability, safety and privacy metrics at the device, connection, behaviour, and application levels.
- **Distributed Ledger FC:** this FC is a basis for trusted data transactions between different stakeholders and their services/devices/actors. It is based on private permissioned blockchain (Hyperledger Fabric) and a set of smart contracts for facilitating read/write/report operations and implementing relationships between actors and processes. Trust metrics are calculated based on information stored in distributed ledger and calculation results are stored in the ledger. Multiple Hyperledger Fabric channels can be implemented to facilitate deployment requirements and integration rules dictated by the DEDICAT 6G system and its use-cases.
- **Data marketplace FC:** Data marketplace FC is a distributed platform for data sharing, which can be used to stream data from any source, IoT devices, physical assets, autonomous cars, drones, and many more.

  The Data marketplace FC enables:
    - Secure data exchange through blockchain;
    - Federated AI/ML for orchestration and processing at the edge;
    - Usage of smart contracts to control access and implement business logic on top of the data.

  Data marketplace FC has several functions:

- System-wide proxy that ensures trust and security of all transmitted data and possibly stores all transactions, audits and reports using blockchain technology, so that it could later be used for AI/ML models training, forensic and other purposes;
- Storage of trusted logs of all transactions between components and sub-components of DEDICAT 6G, audits of sessions and reports;
- Instrumentation of automated training of AI models (for different purposes across the DEDICAT 6G project).

- **Logging FC**: This FC enables collection and secure storage of all types of logs across the DEDICAT 6G system (with main focus on security) and implements blockchain technology to ensure logs consistency and trustworthiness.
  Its main functions are:
  - Collection of logs (transactions, audit of sessions, reports);
  - Storage of trusted logs in a secure manner;
  - Providing access to logs for authorized clients;
- **Audit FC**: This FC provides surveys and reports based on algorithms exploiting the data logs collected and stored by the Logging FC, e.g., security threats like intrusion detection resulting from complex correlations and deductions exploiting the data logs and that cannot be achieved in real time.

4.3.3 Description of OTHER layers (outside DEDICAT 6G perimeter)

After getting into the detail of the FCs that populates the different Functional Groups of the DEDICAT 6G architecture, we elucidate the FCs, which seat outside the perimeter of DEDICAT 6G.

4.3.3.1 Legacy 5G Network FG

We give here a catalogue of 5G components, which interact directly with the DEDICAT 6G FCs and we also explain the nature of the intended interactions (e.g., deployed, providing information or receiving information).

CORE components

In this section are introduced some relevant highlights and components of the 5G system [12] [13], and how the DEDICAT 6G platform is interfacing with the *5G Core* (5GC) components.
In Figure 22 below are depicted the main components of the 5G system [14]. It is worth noting that:

- Control and User Plane are separated in order to allow Control and User Plane systems to scale up independently. In Figure 22 below, the components devoted to the user plane are showed in red and the ones placed in the control plane are in blue;
- In order to fully support scalability and resilience of the *Network Functions* (NF), there is a separation between computation and storage;
- The NF capabilities are exposed through well-defined RESTful APIS, following a service-based architecture;
- Support for non-3GPP and fixed network access, providing mobile network convergence;
- Network slicing to provide end-to-end logical network separation for automate the offering of different levels of QoS virtual set-up.

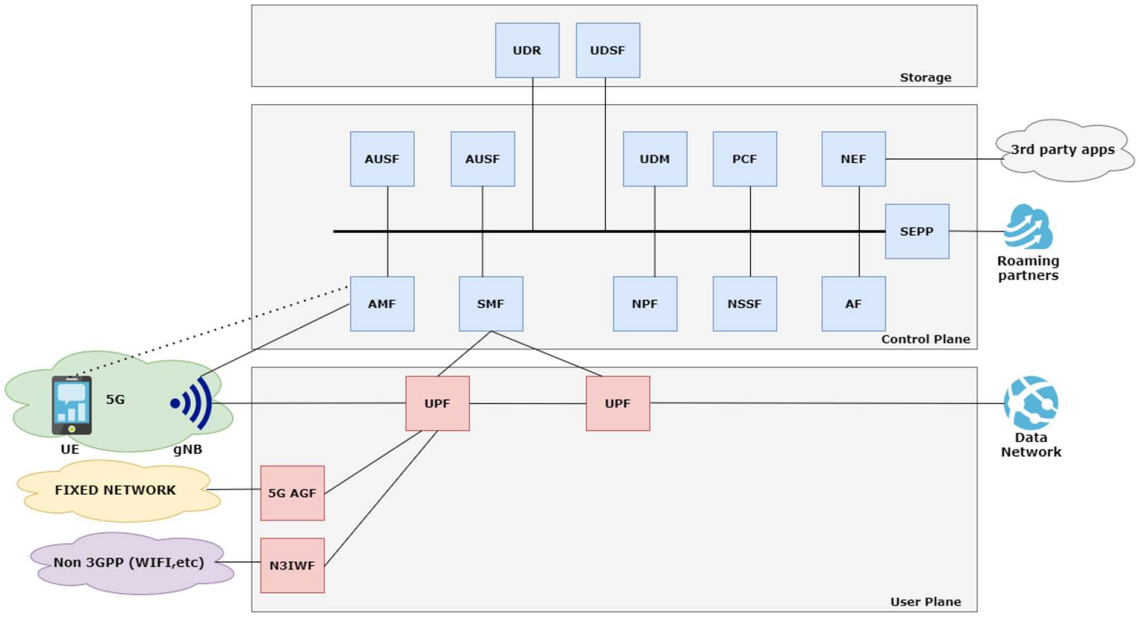


Figure 22: 5G Core components

The most relevant components for the DEDICAT 6G architecture are:

- ***Access Mobility Function* (AMF):**
  - Control which *User Equipment* (UE) can access the 5GC network and to exchange traffic with DNs;
  - Manages the mobility of UEs when they roam from one *gNodeB* (gNB) to another for session continuity;
- ***Session Management Function* (SMF):**
  - Keeps the trace of related PDU sessions and QoS flows;
  - Receives from PCF rules and enforce them in UPF, gNB and UE for QoS flows management;
- ***Network Slice Selection Function* (NSSF)**:
  - Support with the selection of the Network Slice instances that will serve a particular UE. Besides, the NSSF will dispose the Allowed *Network Slice Selection Assistance Information* (NSSAI) that is assigned to the device;
  - Reallocation of AMF in case it is not able to support all network slice instances for a given UE;
- ***Policy Control Function* (PCF):**
  - Hosts network policies to create PCC rules to be forwarded to the SMF;
- ***User Plane Function* (UPF):**
  - Forwards traffic between the RAN and DNs;
  - Enforces QoS of UEs based on the SMF templates through the N4 *Packet Forwarding Control Packet* (PFCP) interface;
- ***Network Exposure Function* (NEF):** Supports external exposure of capabilities of network functions. External exposure can be categorized as:
  - Monitoring capability;
  - Provisioning capability;
  - Policy/Charging capability;
  - Network status;
  - Reporting capability;

- Analytics reporting capability.

DEDICAT 6G Network Awareness FC subscribes to certain events thus detects them in the platform. The events and metrics are available in the 3GPP 23.502 [15], some examples of the events tracked by the Network Awareness FC are:

- Loss of Connectivity (AMF- Network detects that the UE is no longer reachable for either signalling or user plane communication);
- UE reachability (UDM- Detected when the UE transitions to CM-CONNECTED state or when the UE will become reachable for paging);
- Communication failure (AMF-RAN or NAS level failure is detected based on connection release and it identifies RAN/NAS release code);
- PDU Session Status (SMF-PDU session established or released);
- Number of UEs present in a geographical area (AMF- It indicates the number of UEs that are in the geographic area described by the AF);

- ***Network Data Analytics Function* (NWDAF):** It performs data analysis, collecting data from NEF, NFs, *Operations, Administration and Maintenance* (OAM) or the *Unified Data Repository* (UDR) and provides the analytical result to the AF, the 5GC NFs and the OAM [16] [17]. NWDAF and NFs cooperate to build and supply consistent and efficient policies, analytics output results, and finally decision-making in the *Public Land Mobile Network* (PLMN). In can be delivered in distributed architectures providing analytics at different points of presence: at the edge in real-time and a central function for analytics, which need central aggregation (e.g., service experience), etc. NWDAF collects data from different sources of the 5GC and delivers analytics services using a request or subscription model. DEDICAT 6G network optimizer and network prediction leverages this component to place analytics at 5GC level;
- ***Application Function* (AF):** It is a logic representation of a broad set of capabilities intended to support the 5G Core system. The AF can interact with the 5GC in the following ways:
  - Assisting in traffic routing;
  - Accessing the NEF;
  - Interacting in policy management;
  - Enabling *IP Multimedia Subsystem* (IMS) interaction with the 5GC.

  Moreover, depending on the operator's deployment, AFs can be considered as trusted or untrusted. Only in case they act as trusted, AFs can interact directly with the relevant NFs. Otherwise, their scope is limited to the NEF, acting as a gateway for the rest of the NFs. In addition, the entity of the AF is used in the 5GC to be the entry point for other standardised subsystems, such as the ETSI MEC [18]. Thus, the DEDICAT 6G platform, or part of it, will be recognized as AF in the 5GC system.

Radio Access Network

The different *Radio Access Network* (RAN) functions and architectures are discussed in [19],[20] and [21]. The RAN functions between the radio antenna site and central locations are shown in Figure 23(a) below.

The RAN components which are the most relevant to the DEDICAT 6G architecture are:

- The *Radio Frequency* (**RF**) signal processing is responsible for the D/A conversion and the RF front End;
- The physical (**PHY**) layer is responsible for coding and modulation;

- *The Medium Access Control* (**MAC**) layer is responsible for buffering, multiplexing and de-multiplexing segments, including real time scheduling decisions about which segments are transmitted and when;
- The *Radio Link Control* (**RLC**) layer is responsible for segmentation and reassembly, including reliably transmitting/receiving segments by implementing an automatic repeat request;
- The *Packet Data Convergence Protocol* (**PDCP**) layer is responsible for (de)compressing IP headers, ciphering and integrity protection and making a forwarding decision (i.e., whether to send the packet down to UE or forward it to another base station for handover or link aggregation;
- *Radio Resource Control* (**RRC**) layer is responsible for configuring the coarse grain and policy related aspect. The RRC runs in the control plane and does not process packets on the user plane.

In [20], the *Third Generation Partnership Project* (3GPP) defined a *Next Generation RAN* (NG-RAN) architecture where 5G NR base station (a.k.a. gNB) functionality is split between two logical units:

- The *Central Unit* (**CU**) is responsible for non-real time, higher L2 and L3. The CU runs the RRC and PDCP layers. The split architecture enables a 5G network to utilize different distribution of protocol stacks between CU and DUs depending on midhaul availability and network design. It is a logical node that includes the gNB functions like transfer of user data, mobility control, RAN sharing, positioning, session management etc., with the exception of functions that are allocated exclusively to the DU. The CU controls the operation of several DUs over the midhaul interface. In the 3GPP model, the CU is connected to the 5G core (5GC) via the NG interface and the CU is connected to the DU via the F1 interface, as shown below in Figure 23(b);
- The *Distributed Unit* (**DU**) is responsible for real time L1 and L2 scheduling functions. DU sits close to the *Radio Unit* (RU) and runs the RLC, MAC, and parts of the PHY layer. This logical node includes a subset of the eNB/gNB functions, depending on the functional split option. Its operation is controlled by the CU.

The 3GPP studied several different functional splits between the CU and DU in [20]. Functions that need real-time processing are grouped within the DU, while those not requiring real-time are grouped within the CU.

In a separate study [21], the ITU Telecommunication Standardization Sector (ITU-T) adopted a slightly different transport network architecture for 5G that is comprised of three logical elements: CU, DU and RU, as shown in Figure 23(c). In this model, the mid and lower layer functions are divided between the DU and RU.

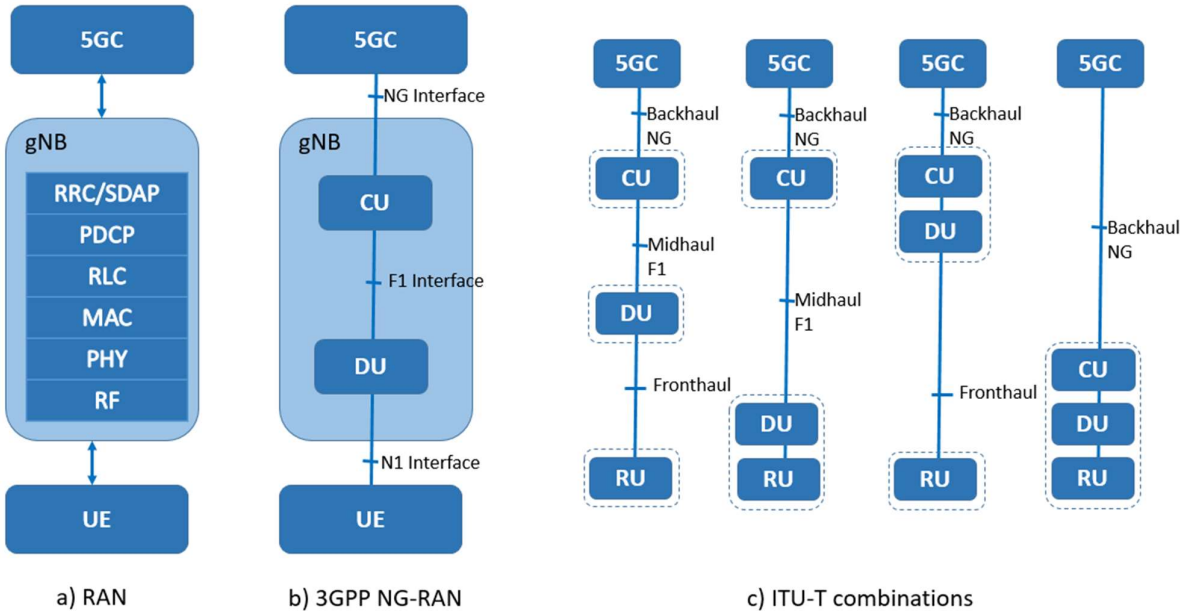


Figure 23: Radio access network functions (a), 3GPP NG-RAN Architecture (b), possible CU, DU, RU combinations (c)

The architecture of *Integrated Access and Backhaul* (IAB) networks [22] represents a fundamental evolution in 5G networks. Two types of links are supported in IAB networks:

- An access link is a link between an access UE and an IAB node or IAB donor;
- A backhaul link is a link between an IAB parent node and IAB child node:
  - The IAB parent node is responsible for scheduling the downlink/uplink traffic for both access and backhaul links;
  - The IAB child node at the end of the transmission chain is responsible for scheduling the downlink/uplink traffic between itself and the UEs.

In order to avoid the expensive installation of fiber for the backhaul, DEDICAT 6G can provide with IAB a better alternative for connectivity extension and cell densification by connecting new MAPs wirelessly to backbone networks (see Figure 24 below) and sharing the spectrum for access and backhaul links. If temporary coverage or capacity needs to be added in a particular area, IAB nodes can be opportunistically deployed/activated to deliver services.

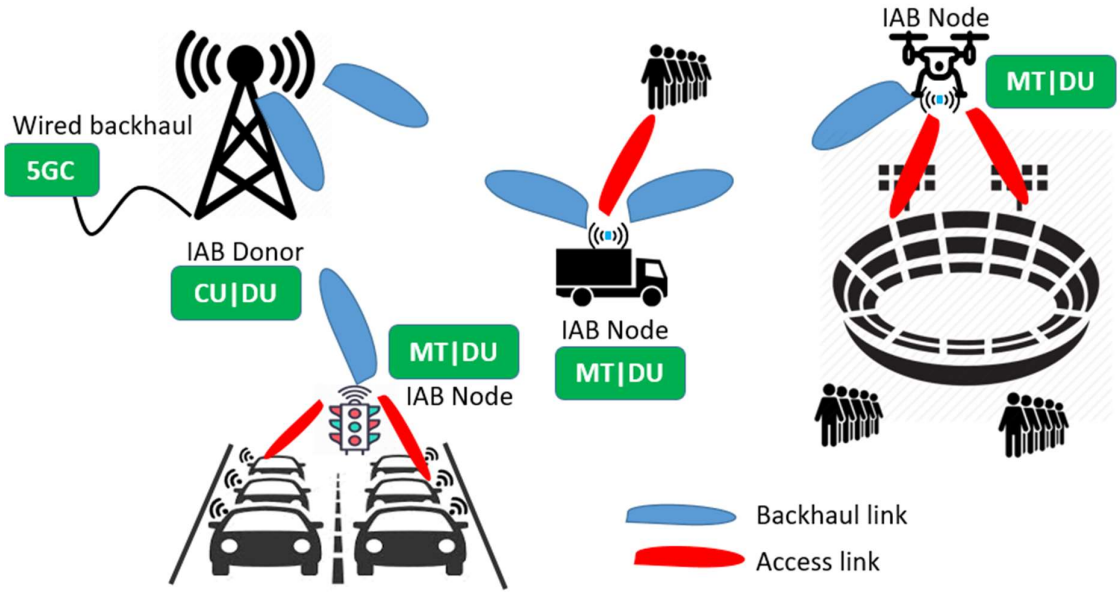


Figure 24: Usage of IAB in connection with MAPs

4.3.3.2 Business Verticals FG

This FG hosts the business applications that are using the services offered by DEDICAT 6G. They are not described here but will be visible in the Network Deployment View of D2.4 (next iteration of this deliverable) where we will elucidate the deployment of each of the four DEDICAT 6G UCs

4.3.3.3 3rd Party FG

This FG hosts all 3rd party products that are supporting the applications ran by the verticals when using the DEDICAT 6G services (like ECaaS and IDaaS). We do not give here any detail about those 3rd party software components as those FCs are not part of the DEDICAT 6G architecture, but Table 16 gives a good overview of the FCs identified so far and pertaining to the four DEDICAT 6G scenarios. Those FCs will be emphasized when dealing with the Network Deployment of the four scenarios (in the second iteration of the DEDICAT 6G System Architecture).

4.3.4 System Use-Cases

System use-cases are meant to describe interactions taking place between the (logical) FCs and will act as a **guidance** for the implementation activities taking place in WP3, 4, 5 and 6. (likewise for data flow diagrams in the Information View in the next iteration of this deliverable).

It will be the responsibility of each WP to ensure consistency between System Use-cases and actual implementation.

In this first version of the System Use-Case we describe textually only what are the steps involved and intended interactions taking place between the FCs partaking into that Use-Case steps.

In the next iterations of this document, we will elucidate more precisely those steps using precise UML Message Sequence Charts (a.k.a. Interaction Diagrams).

4.3.4.1 Initial deployment at T_0

This first UC elucidates the sequence of actions that take place at t_0. It covers the discovery of the network topology and the decisions taken by the DEDICAT 6G platform to undergo the initial FC deployment (likely to be mostly awareness-related agents and aggregators). Since there is theoretically no Edge Node yet, the main target for the initial deployment is the 5G network. The objective is then to start building up the deployment that provides continuous flow of information that can trigger decision-making to the different decision making FCs (i.e., IDDM, CEDM and NODM). This means of course that all FCs meant to be running in the Cloud need to be started as well (e.g., the Decision Making FCs, Service Operation, cloud-based context-awareness components, etc.)

Again, at that stage it is assumed that no edge node has been already deployed.

However, Edge Nodes such as Connected Cars, Drones and Robots can be pre-declared and pre-configured (see Edge Node Registry and Edge Node Repository FCs) so that if it happens coverage extension is required based on analysis of context-awareness data and selection criteria, the needed Edge Nodes can be selected and deployed straightaway, without losing time going into the configuration phase first.

In the same way, those Edge Nodes have to be deployment–ready, meaning that a certain number of FCs can also be pre-deployed inside the Edge Nodes in order to save time. Those pre-deployed FCs comprise e.g.:

- 5G legacy components needed for handling the Coverage Extension Scenarios (See Sections 4.3.4.3, 4.3.4.4 and 4.3.4.5);
- Execution environment;
- Awareness FCs and agents that monitor those 5G components at run-time;
- Edge Node Status and related-Agents that give information about the Edge Node at run-time.

This pre-configuration is performed by a network operator using the Front-End GUI from the Management FG.

We give below an example of initial deployment for one of the DEDICAT 6G scenario namely the UC2 scenario "Enhanced Experience".

The main focus in this second UC is performing live video streaming from the event site relying only on the underlying mobile network. The initial deployment at T0 will be introduced with 5G network followed with the baseline measurements for enabling easier comparison against DEDICAT 6G solution(s). The objective is to start building up the deployment where different Edge Nodes can improve the network performance according to the certain level (i.e., energy, latency, throughput, load distribution) with the help of triggered analytics, context-awareness and decision making policies. In later iterations dynamic intelligence with coverage extension will be added for enhancing the network flexibility and adaptation. The majority of the processing is planned to be executed in the Edge Nodes following the FCs with the context introduced earlier with the UC2:

- 5G legacy network components enriched with DEDICAT 6G optimizations;
- Application environment;
- Network analytics for providing necessary real-time status information to Edge Nodes.

4.3.4.2 Managing Edge Nodes

When a new node is created it brings computing capability (and eventually additional radio coverage depending on the exact nature of the node) to the DEDICAT 6G platform. The exact characteristics of the new ENs are to be stored in the EN Registry so that it can be discovered by the Decision Making and used whenever they do fit the requested criteria. Some detail about the type of information stored in the EC registry can be found in the Section 4.3.2.2

After being properly registered, the edge node needs being installed a certain number of FCs - mainly awareness FCs- which are needed by the platform in order to be able to take proper decisions at run time (after the Edge node has been actually activated). Such examples are described already in the Section 4.3.4.1 above.

4.3.4.3 Coverage Extension – Reacting to a radio network failure

The first coverage extension scenario is triggered by the 5G legacy network as follows.

Awareness agents (network status agents) are deployed in order to collect raw information from the 5G legacy network (e.g., NEF notifications if the NEF is available or any 5G components providing status/performance indicators, or alarms sent by the Network Prediction FC) concerning various performance indicators or H/W fault alarms, report to the DEDICAT 6G Network Awareness FC such issues in the form of enhanced messages, which are then published onto the message bus FC (part of the communication FG).

Such sort of information is subscribed by default by the Network Operation DM that in turn decides whether solving the problem must involve Intelligence Distribution, Coverage Extension or eventually both. It also provisions Network-related information that can be useful to support the IDDM and CEDM (like information concerning the initial network/radio capacity of a faulty piece of H/W equipment, geographical origin of the fault if any, recipient (meaning human operator) of any further MAP physical deployment requests, etc.)

From now on, we only consider the case where CEDM must take the lead.

During the next step the CEDM will -- depending on the nature of the received message and its parameter -- plan and initiate the deployment of Mobile Access Points with 5G capability, based on the pool of available MAPs and their characteristics. Additional MAPs might be needed in case the existing ones cannot fulfill the constraints of that particular case (e.g., no drone has been already physically deployed in the targeted area).

The rest of this System Use-Case is similar to the CEaaS case below (Section 4.3.4.5), branching to step 3) or 4).

4.3.4.4 Coverage Extension – Reacting to an optimization recommendation

This second scenario is relatively similar to the first case above. However, it does not rely on direct notification from the 5G legacy network, but on the result of the optimization task performed by the Network Optimization / Network Prediction FC and related agents. In the same way than above, the network recommendations issued by those FCs are made available to the NODM which is ultimately responsible for operating the network in an optimal way. Depending on NODM's decision regarding operation, the IDDM (resp. CEDM) may be triggered whenever Intelligence Distribution (resp. Coverage Extension) is needed, branching then to step 3) or 4) of the CEaaS scenario below.

4.3.4.5 CEaaS (Coverage Extension as a Service)

The DEDICAT 6G system provides coverage extension as a service to vertical business applications, meaning that a third-party application would require an explicit extension of (temporary) radio coverage with specific QoS requirements in order to be able to run the application while fulfilling its QoS constraints.

CEDM is triggered first, relying then on both IDDM (for supporting intelligence distribution) and NODM (for provisioning the networking part). This scenario does not cover the case where the Vertical also requests the deployment and execution of its own FCs as that case is already covered in Section 4.3.4.6 below). The various steps involved are described hereafter (see also Figure 25 below for a graphical illustration of the steps involved):

1. A vertical application (e.g., a public concert organizer) requests a temporary coverage extension for the duration of its event in order to allow video sharing, and online video coverage). The request comes with a set of technical constraints e.g., number of targeted attendees and expected UEs, event location, traffic goal per UE, expected kind of traffic etc.;
2. A SLA negotiation takes place between both parties, leading to a set of technical objectives to be met by the DEDICAT 6G platform. Those objectives are the main input to the CEDM;
3. Then the CEDM instruments the NODM with QoS targets, which in turn will configure the network in order to fulfill the QoS objective (e.g., involving network slicing);
4. The CEDM also decides about the nature of MAP involved and their deployment (planning, number of MAPs etc.). Edge Node Awareness (and related agents) and Edge Node Registry FC are involved in building up a context used for the IDDM decision process;
5. The CEDM also instruments the IDDM in case intelligence distribution is required too either to support the deployment and execution of vertical-specific FCs or to support the pure telecommunication aspects. The Edge Node Awareness FC and related agents are involved in building up a context used for the IDDM decision process;
6. Then the physical deployment and operation of MAPs and (eventually) MEC is shortly described in the next scenario below (Section 4.3.4.7).

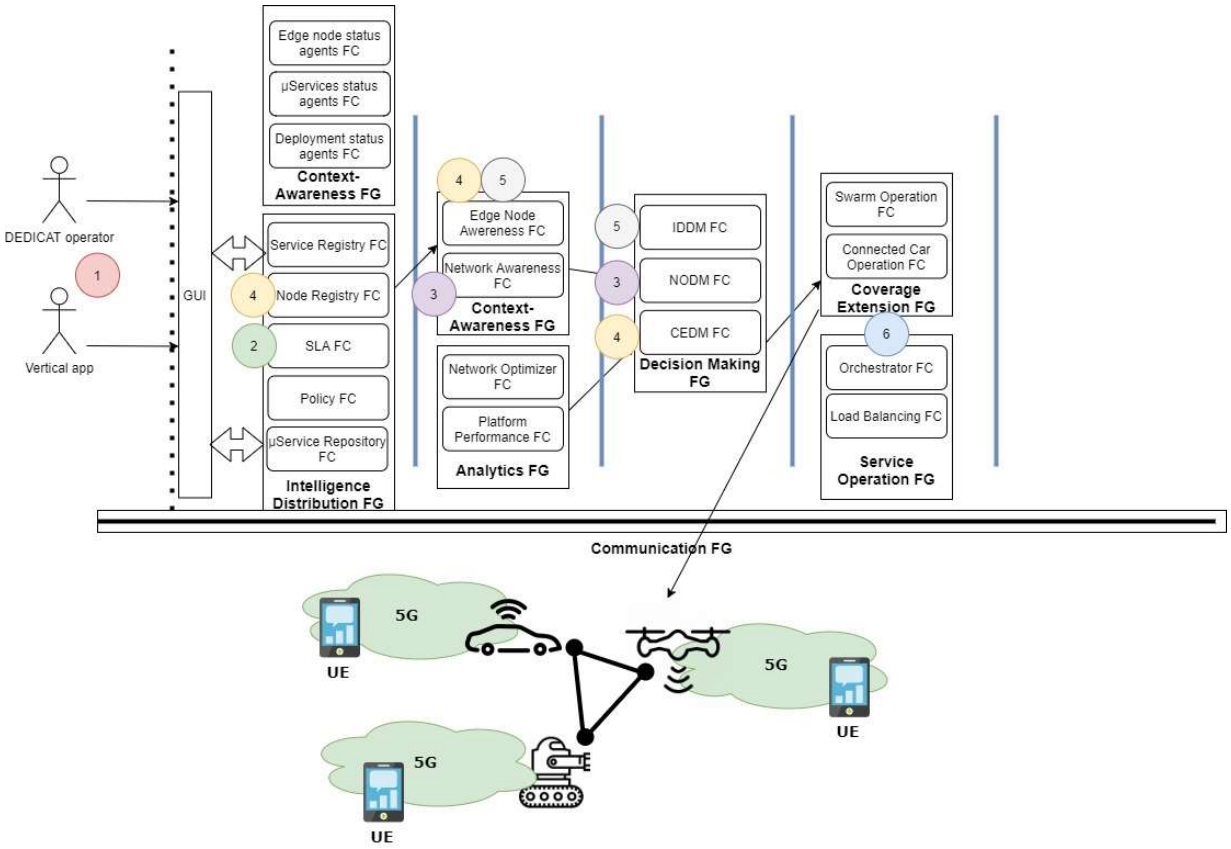


Figure 25: Steps involved in CEaaS System Use-Case

4.3.4.6 IDaaS (Intelligence Distribution as a Service)

Intelligence Distribution as a Service is offered to verticals as a support to their business operation. Verticals have the ability 1) to register and upload their own FCs, 2) to register edge nodes (EN) and their capabilities to the DEDICAT 6G platform and 3) to set-up deployment policies, negotiate SLA and set-up QoS requirements (which eventually involves slicing). This System use-case elucidates such a scenario end-to-end (see also Figure 26 below for a graphical illustration of the steps involved):

1. It usually starts with the description and registration of EN (see System UC Section 4.3.4.5 above);
2. Deployment/Start the EN (incl. Status and related agents) and start FC (the generic ones);
3. Awareness-related FCs build-up a Customer-related Context. For example, part of the context is the pool of ENs which are eligible for Vertical FC (re)-deployment based on 1) the policy issued by the Vertical and 2) some awareness information such as the EN status, overall capabilities and ownership;
4. Decision making, based on the Policy and updated Context decides about the (re-) deployment of Vertical FCs; Please note that if the SLA cannot be fulfilled according to the current EN deployment, the IDDM may instruct the verticals to deploy more ENs;
5. Service Operation implements the Decision making instructions;
6. Steps 3 and 4 are repeated in order to ensure an optimal deployment and operation according to the Context and Policy.

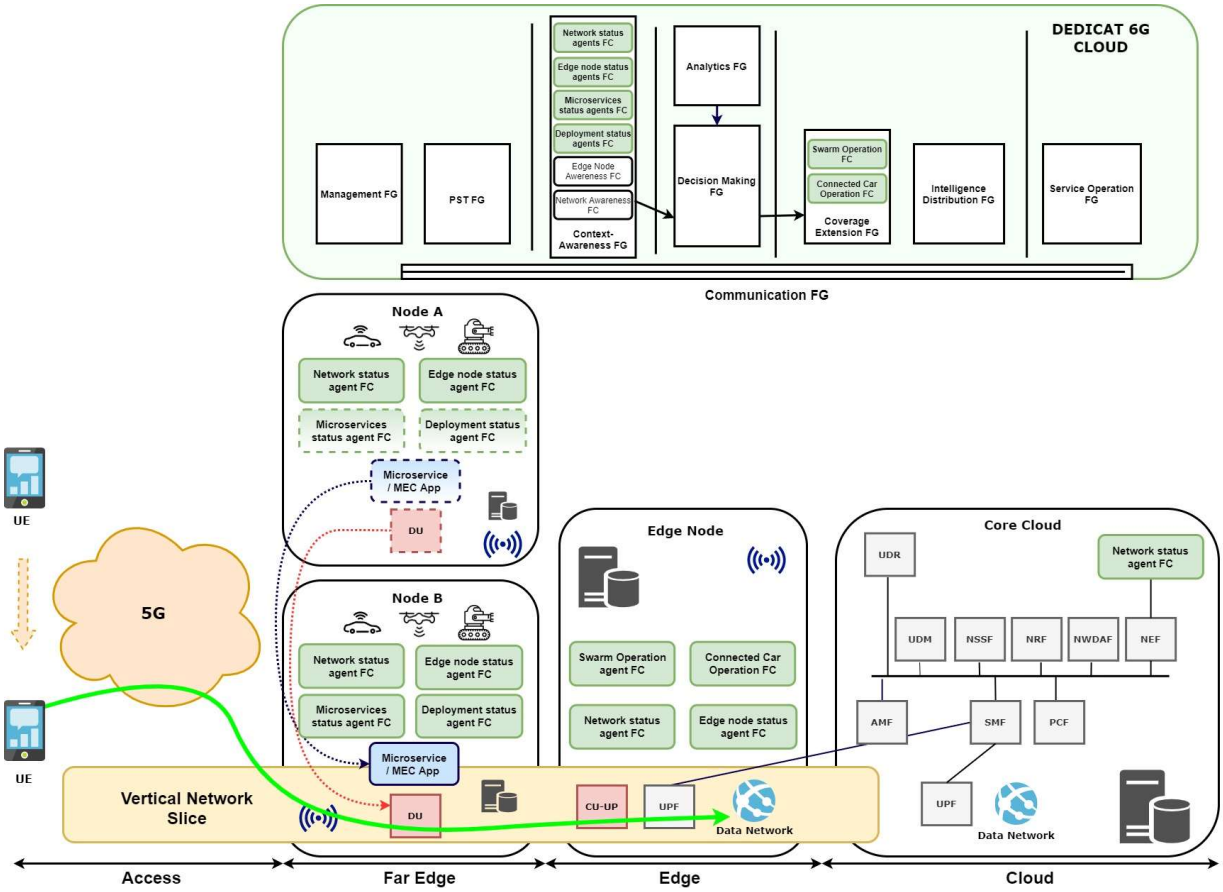


Figure 26: Steps involved in IDaaS System Use-Case

Please note that this scenario does not involve Coverage Extension

4.3.4.7 MAP/MEC physical deployment and operation

In DEDICAT 6G we consider four classes of MAPs/MECs as part of our baseline architecture:

- **UAV:** they are Unmanned Aerial Vehicles. While the project is focusing on the use of drones as far as aerial vehicles are concerned, the use of airships could be considered as a very interesting alternative (deployment would be probably longer but they would enjoy eventually much greater energy autonomy and tolerate much heavier payloads);
- **AGV:** They are Autonomous Guided Vehicles (at large) and DEDICAT 6G includes the use of Robots as the baseline solution (smart vehicles are also introduced in UC4);
- **Manned Connected Vehicles** (MCV), a.k.a. Connected cars/vans: They can be easily deployed on demand and enjoy a long autonomy;
- **Small servers:** they are reasonably small in size and weight and can be easily deployed in order to support scenarios relying on Intelligence Distribution, like for instance Critical Mission management in the context of natural disaster (e.g., UC3 Scenario).

UAV, AGV and MCV are used for the purpose of coverage extension and Intelligence distribution, while small servers are used to support Intelligence Distribution only.

The use of MAP results from either 5G network malfunctions (bad performance, faulty devices, lack of capacity vs. demand) or service request for enhanced coverage or intelligence distribution (a.k.a. respectively ECaaS and IDaaS).

Therefore, the deployment of MAPs cannot be planned in advance and performed without involving human operators such as: physically moving the MAP to the suitable location and making sure they are ready for communicating with the Cloud components. Also drones (and robots as well to a lesser extend though) cannot fulfill entirely their allocated missions without docking regularly (every 20~25mn for drones depending on their payload weight) in order to recharge/change batteries. These steps need human intervention as well.

After being deployed on suitable location near the operation field, the unmanned MAPs are self-organizing (as a swarm) and physically deploy in order to cover optimally a geographic area instructed by the Decision Making.

In a nutshell, the system use-case for MAP deployment relies on the following steps, assuming the Decision Making FCs have already decided about a deployment plan. Please refer to System UCs Sections 4.3.4.3, 4.3.4.5 and 4.3.4.6 for more detail about what actually happens before a MAP/MEC deployment):

1 Notifying a human operator about what needs to be deployed (nature of the MAP/MEC and number) and where;
2 When on site, make sure the MAP/MEC are ready for communication with the cloud (meaning e.g., their embedded gNB can talk with the closest IAB-donor) and double-check needed FCs and interfaces are available;
3 Depending on the outcome of step 2, possibly engage into MEC management in order to create entries into Edge Node registry etc. (See Managing Edge Node System Use-case above), Some –by default- or needed FCs are then automatically uploaded;
4 Possibly some additional FCs are uploaded to the MAP/MEC (in addition to FCs which are deployed in the MAP/MEC by default;
5 At this stage, the MAPs – instructed by the cloud or by the Self Organize FC- initiate physical deployment (to designated place or to perimeter to be covered);
6 When a MAP battery is shy of being fully depleted, the MAP returns automatically to its assigned docking station, then its battery is replaced for a fully charged one by a human operator (notification through the GUI may be used beforehand) and is then re-deploying to its initial position.

4.4 Network Deployment View

The Network Deployment View leverages the Functional View providing a great focus on static and dynamic aspects of Intelligence Distribution and Coverage Extension. While the FV gives a high level logical description of the FCs and their interactions in various contexts, the NDV will elucidate the physical implications and related mechanisms of dynamic component migration in liaison with the Edge Computing FG and Decision Making FG. This includes (to be confirmed) (pre-) installation of execution Environment (e.g., VM), micro-services/container migrations etc. Since DEDICAT 6G leverages the existing 5G legacy network, the NDV naturally also includes the 5G network architecture for the following reasons:

1. Many interactions (sometimes bi-directional) have to take place between the DEDICAT 6G and the supporting legacy 5G;
2. Some of the 5G Core or RAN components do have to be deployed towards the far edge inside DEDICAT 6G-specific Mobile Access Points and/or Mobile edge Computing nodes, depending on the considered scenario;
3. DEDICAT 6G extends the capabilities of the existing 5G network therefore it seems natural to show both of them in a single view, complementing then a rather IT-flavoured Functional View where the deployment issues and 5G intrinsic architecture were left aside.

In the first iteration of the Network Deployment View, we consider the baseline DEDICAT 6G operation excluding any scenario involving verticals (e.g., IDaaS and CEaaS cases as described in the System Use-Case Section 4.3.4) and therefore focusing on dynamic coverage and/or Intelligence migration extension resulting from the sole operation of the legacy 5G (e.g., cases where those are triggered by H/W failure, poor performances, etc. in order to help bringing back the 5G network operation to normal).

Consequently, all base-line MAPs/MECs are grouped under one single umbrella, as while being different in nature, their deployments are rather identical (with very minor differences).

In the next iterations of this architecture document, we will revisit network deployment in a more specific way, adding to the current generic view, four more views corresponding to the network deployment of each one of the four WP6 scenarios, as described in D2.1 [3].

4.4.1 Generic Network Deployment View

In this first iteration of the NDV (see Figure 27 below), we put the light on providing a generic overview of a potential network deployment highlighting the interactions between the DEDICAT 6G platform and a legacy 5G network infrastructure when applying the DEDICAT 6G solution, specially focused on dynamic coverage extension and/or intelligence distribution/migration operations.

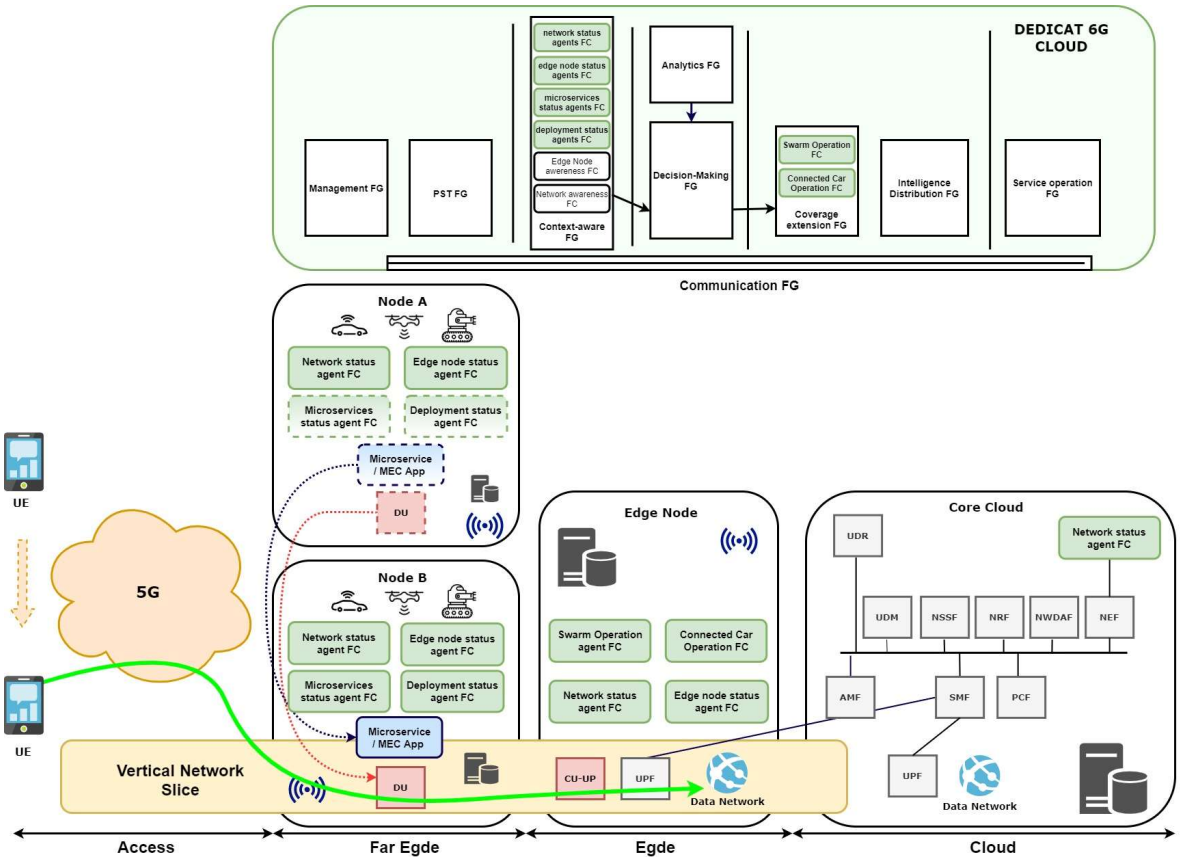


Figure 27 – Generic simplified DEDICAT 6G network deployment schema

Figure 27 above shows a diagram of the simplified and baseline deployment where the DEDICAT 6G platform supports a 5G/B5G ecosystem in accommodating a vertical service. Just for the sake of simplicity and in order to provide a clear picture of the environment, we assume a hierarchical network scenario organized in four main domains:

- **Access:** the closest part to the final users (UEs) of the network where network access is provided. In Figure 27 above this domain is represented by the 5G orange cloud icon on the left. It encompasses all the typical pre-deployed technologies of the 5G legacy infrastructure to enable the access of user's traffic (e.g., fixed wireline/wireless or mobile RAN);
- **Far Edge:** ordered by proximity to the user, the next network domain is the *Far Edge*, where nodes are close enough to guarantee minimum latency. Nodes belonging to this domain have very limited computational resources, but still enough to host tiny or small virtual pieces of software aimed at providing high performance with the lowest latency. In our scenario, the far edge nodes will have mobility capabilities, e.g., robots and drones, with embedded equipment meant to transmit data and be part of or interact with the RAN system. In addition, nodes can be used as MEC hosts to deploy vertical µServices (MEC apps) in small VMs or containers. Finally, their computational resources can be utilized by the DEDICAT 6G platform for deploying some agents that could perform specific tasks of some key FCs;
- **Edge:** the *Edge* domain is composed of a set of nodes and links still close to the end-users but with larger resources compared to the far edge entities. From a hierarchical

point of view, it is the link between the far edge domains and the core cloud. Moreover, from our deployment view, edge nodes can host, not only the same functionalities and agents as far edge nodes - if required, but also other FCs agents or instances needed to manage and control some of the functionalities available in the far edge nodes, e.g., swarm operation or connected car operation FCs. In addition, depending on the vertical requirements (embodies in SLAs) and the nature of its implementation, in this domain we can find the first potential entry point to the data network or private network facilities, i.e., using 3GPP terminology, *5G Non-Public Networks* (5G-NPN). If so, the 5GC system architecture will require instantiating the UPF to enable *End-to-End* (E2E) 5G connectivity;

- **Core Cloud:** the last domain in this network hierarchy is the *Core Cloud*, a set of remote servers, mainly devoted, in this context, to first, accommodate the control plane functions of the 5GC (e.g., NEF, AMF, SMF, PCF or UDR, among others). Typically, the core cloud comprises the connection to the core/backbone networks, that can provide access to the data network or the Internet. In those cases, the 5GC system demands to place here the UPF.

It is noteworthy that the DEDICAT 6G platform will be remotely located in the cloud, and able to reach out to all nodes and UEs within its deployment. This position is essential to provide a global picture of the scenario from above to support the whole system. At all nodes involved in the establishment of the vertical service from the far edge to the cloud core, the DEDICAT 6G platform will instantiate specific agents to monitor the network status and retrieve the necessary metrics required by its corresponding FCs.

As complementary assumptions of the NDV we consider that all the nodes from the far edge to the core cloud will be part of the Network Function Virtualization Infrastructure (NFVI), thus facilitating the establishment of network slices and network services instantiation. Regarding the ETSI NFV [23] architecture, the NFVI is orchestrated by the NFV Orchestrator (NFV-O), which is placed at the control plane part of the network. It is responsible to perform NFV *Management and Network Orchestration* (MANO) functions, basic in a 5G-based scenario. The DEDICAT 6G platform will assist the NFV-O on the instantiation of network services and network slices, according to the outcomes coming from the NODM FC and executed by the Orchestration FC.

In order to complement the description of the NDV, here we expose an exemplary generic use-case where a vertical requests the deployment of its service. To simplify the use-case and maximize the understanding, we will assume that the vertical requirements can be satisfied by establishing only one network slice.

As depicted in Figure 27, we assume in this example that a UE has moved from a coverage-covered area to another one. This change is monitored by the system and notified to the DEDICAT 6G platform. At this point, just for the sake of simplicity, we could assume two procedures or a mix of them that can be triggered to handle it: to extend or move the current coverage or migrate the needed intelligence:

- **Coverage extension**: the new UE location and other relevant information, extracted by the Context-Awareness FG, is used as input by the Coverage Extension DM FC that produces the correct configuration and path of the far edge mobile node (drone, AGV or robot). Next, the corresponding FC of the Coverage Extension FG (Swarm Operation FC or Connected Car Operation FC) will react according to the output of the CEDM FC. Finally, the far edge node moves to the new coordinates, changing the coverage area and re-enabling the UE connectivity. If proceeding, the network slice must be updated and reconfigured accordingly.

- **Migrate Intelligence**: when coverage extension is not possible to be used as a solution or the UE enters the coverage area of another node, migrating intelligence may be a feasible option to reconnect UE connectivity. If so, the FCs in the Context-Awareness FG (thanks to the agents deployed at the nodes and other information sources as NEF) will provide the necessary information to the Intelligence Distribution DM FC to calculate the optimal location of the intelligence. As can be seen in Figure 27, the migration of DEDICAT 6G and vertical μServices (MEC apps) from the original node to a new one. This also has some impact on traffic steering and, in turn, on the establishment of the network slice. Then, with the help of the Orchestration FC and the Network Optimization FC, a new path is established in the network that traverses and the new DU, CU and UPF, if applicable, to enable E2E connectivity in the network slice, always fulfilling the SLA and vertical requirements.

Please note that the description and level of detail of the NDV can be much more extensive, however, for the purpose of this document, it is out of its scope. Further information will be provided in later documents and, specially, in WP6 outcomes.

5 DEDICAT 6G Architecture Perspectives

5.1 Privacy Perspective

The project will implement mechanisms and tools for ensuring privacy in the scope of applications supported over B5G/6G networks. Such mechanisms and tools will include functionality for controlling data flow in terms of privacy and confidentiality.

Threat detection mechanisms will be based on federated learning boosting privacy protection by moving ML model training process to the source of data instead of transferring data to a centralized entity. Implement comprehensive policies, procedures and protocols for handling personal data. The following Table 17 summarizes how the privacy perspective is dealt with.

Table 17: Privacy perspective survey

Targeted System Quality	Full (100%) protection of obtained personal data information Private data cannot be used in malicious manner
Requirement(s)	• Event logging and auditing • Data anonymisation; • Usability; • Privacy by design. FREQ-3, FREQ-6 to FREQ-11, NFREQ-1 to NFREQ-3, NFREQ-51 to NFREQ-59
Activities	• Setup logging procedure; • Generate logs; • Check log completeness; • Check personal data at source; • Check data when stored in database; • Hide system information from the user; • Perform Audit.
Tactics	• Logging functionality: the logs will allow investigating a system malfunction. It will be possible to know which data/functionality has been abused. Controlling the quality of log data by analyzing and adding missing information to the logs; • Audit functionality: This functionality is responsible for analysing the logs in an offline manner in order to create security and management surveys and reports (which could include threats like intrusion detection attempts or platform malfunction); • Implementing algorithm for creating and storing permanent records of events that can be reviewed and checked Plan and carry out thorough testing of the integration algorithms, analyzing their performance and the results produced; • Implement comprehensive policies, procedures and protocols for handling personal data.

Applying the tactics above, results in the following list of Design Choices (**Table 18** below)

Table 18: Design choices for the Privacy perspective

Design Choice ID	View	FG/FC	Technical description
PRIV-01	Functional	Security FG / {Logging FC, Audit FC}	Introducing system logging functionality
PRIV-02	Functional	Security FG / {Logging FC, Audit FC}	Implementing algorithm for checking log completeness
PRIV-03	Functional	Security FG / Data marketplace FC	Implementing system algorithm for comparison data

PRIV-04	Functional	Security FG / AuthZ FC	Adopting policies and protocols for personal data

More detail about this privacy perspective will be given in the next iteration of this deliverables (D2.4) based on results obtained from WP5 work (and D5.1 in particular).

5.2 Security Perspective

Security is composed of confidentiality, integrity or absence of unauthorized system alterations, and availability for authorized actions only and protecting against eavesdropping and replay attacks.

The following Table 19 summarizes how the security perspective is deal with.

Table 19: Security perspective survey

Targeted System Quality	All data inside the system or its part will be protected against cyber attacks. Full (100%) protection of unauthorized internal and external accesses.
Requirement(s)	• Data encryption; • Auditing; • Data protection; • Minimal performance and scalability; • Compliance; • Zero trust security framework. FREQ-1 to FREQ-20, FREQ-22, NFREQ-71 to 74
Activities	• Protection of intelligence distribution and local resources; • Verification activity; • Confirming system compliance with security standards and policies; • Un-trust all devices, networks, and users.
Tactics	• Introducing security requirements; • Implementing decision-making security algorithms; • Introducing intelligent auditing mechanism; • Adopt mechanism required to authorize and authenticate system components and users; • Implement algorithm for data confidentiality; • Zero trust mandates that information security pros treat all network traffic as untrusted. This way, network is more efficient, more compliant and more cost effective; • Event logging and perform audit

Project will implement security and data protection framework based on existing industry standards and will specify and implement federated learning mechanisms for training ML models capable of detecting and classifying security threats and data protection risks

Applying the tactics above, results in the following list of Design Choices (**Table 20** below)

Table 20: Design choices for the Security perspective

Design Choice ID	View	FG/FC	Technical description
SEC-01	Functional	Security FG / Edge Node Awareness FC	Implementing decision-making security algorithms
SEC-02	Functional	Security FG / AuthN, AuthZ FC	Authorize and authenticate system components and users

SEC-03	Functional	Security FG/ Threat Analysis FC	Implement algorithm for data confidentiality
SEC-04	Functional	Security FG/ AuthN FC	Enable Zero trust security approach
SEC-05	Functional	Security FG/{Logging FC, Audit FC}	Event logging and offline audit

5.3 Trust Perspective

Trust management platform for DEDICAT 6G dynamic networking and computational distributed systems would be responsible to ensure the integrity of highly dynamic and distributed communication and computation systems.

Platform will be based on private permissioned blockchain like Hyperledger Fabric. The trust management platform will facilitate identity management for users, devices and services.

Trust architecture as a security framework in 5G/6G networks is a solution to address security requirements in a network with untrusted infrastructure, devices and personals. Every access request is individually authorized and monitored during the access period for compliance with security policy rules.

The following Table 21 gives summarizes how the Trust perspective is dealt with.

Table 21: Trust perspective survey

Targeted System Quality	Full (100%) trusted communication between parties, devices and sub-systems
Requirement(s)	• Trust assurance; • Trusted relation distribution; • Identify trust goals; • Trust requirements validation. FREQ-3, FREQ-9 to FREQ-11, FREQ-21 to FREQ-26, NFREQ-81
Activities	• Calculate trust metrics; • Private permissioned blockchain; • Trustworthiness policies.
Tactics	• Utilizing private permissioned blockchain to specify and implement trust management platform based on blockchain technologies and to specify and implement trust metrics and levels of trustworthiness for DEDICAT 6G networks; • To implement security and privacy protection compliance auditing and certification procedures – certificates written to private blockchain through smart contracts; • Validate security, data protection and implement trust KPIs throughout project pilots.

Applying the tactics above, results in the following list of Design Choices (**Table 22** below)

Table 22: Design choices for the Trust perspective

Design Choice ID	View	FG/FC	Technical description
TR-01	Functional	PST FG / Distributed Ledger FC	Implement trust management platform based on blockchain
TR-02	Functional	PST FG / Distributed Ledger FC	Implementing smart contracts
TR-03	Functional	PST FG/ Data marketplace FC	Continuously validate security controls with breach and attack simulation and checking readiness of data protection security protocols

6 Conclusions

This document provided a first iteration of the DEDICAT 6G architecture. It provides the level of detail known at the time of writing, considering especially that the WP3, 4 and 5 are still discussing the most technical aspects of those novel functionalities brought by DEDICAT 6G. Many design decisions are still to be made on that matter.

The main achievements are:

- Identification and description of Physical Entities and Systems, definition of the DEDICAT 6G perimeter (Physical Entity and Context Views);
- Threat Analysis;
- List of Unified functional and non-functional requirements;
- VOLERE template including the result of requirement mapping which can be used for consistency check;
- Extensive set of scenario use-cases as a complement to the textual descriptions in D2.1;
- Functional Model and first version of the functional decomposition (Functional View);
- Various system use-cases covering two of the three main project pillars;
- Base-line Network Deployment View;
- Privacy, Security and Trust Perspectives.

Looking back to the extensive methodology description available in Section 2 and especially Section 2.1.1, it is clear that a few views are still missing (i.e. Information and Instantiation Views, as explained in the Section 1).

However, the Functional View gives a pretty precise catalogue of the Functional Components we are introducing in our architecture, even though some updates and improvements are expected in the next document iterations based on the outputs of WP3, 4 and 5 in particular.

The second iteration of the architecture document will focus on the following aspects:

- Completing the list of views with the Information View: we will start describing data models and most-importantly the data flows occurring between the DEDICAT 6G FCs but also with the 5G legacy components;
- Revise and complement the UML scenario use-cases in the Context view, aligned with the WP6 outcomes;
- Updating the Functional Decomposition and revising and extending the list of System Use-cases, introducing in particular additional view points like Interaction Diagrams and also all aspects pertaining to Privacy, Security and Trust. We will also provide more detailed information concerning the FC interfaces. In particular interfacing with the 5G legacy components will be elucidated;
- Deployment View: Refine the "generic" Network Deployment view and add four more customized examples for the use-cases UC1, 2, 3 and 4;
- Addressing more perspectives and updating the Privacy, Security and Trust existing ones;
- Addressing the new requirements from D2.3 (if any);
- More generally: Improving the level of detail everywhere possible and aligning all sections content with the latest outcomes from WP3, 4, 5 and 6;
- Cross-checking the architecture with the VOLERE template in order to identify eventual gaps or inconsistencies;

All updates made to iteration 1 (this document) in iteration 2 will be documented in a "Delta section" at the beginning of Section 1 of D2.4.

References

[1] DEDICAT 6G consortium, "DEDICAT 6G Description of Action".

[2] N. Rozanski and E. Woods, Rozanski, Nick and Woods, Eoin. "Software Systems Architecture – Working with Stakeholders Using Viewpoints and Perspectives", Addison Wesley, 2011.

[3] DEDICAT 6G Deliverable D2.1 "Initial Scenario Description and Requirement Collection"

[4] Hernan, S.; Lambert, S.; Shostack, A.; & Ostwald, T. "Uncover Security Design Flaws Using the STRIDE Approach". MSDN Magazine. November 2006.

[5] DEDICAT 6G list of UNIfied requirements (as a VOLERE template) https://dedicat6g.eu/wp-content/uploads/2021/09/Dedicat6G_UNI_Requirements_v1.xlsx

[6] IEEE Architecture Working Group, "IEEE Std 1471-2000, Recommended practice for architectural description of software-intensive systems", 2000.

[7] Rozanski, Nick and Woods, Eoin, "Applying Viewpoints and Views to Software Architecture", http://www.viewpoints-and-perspectives.info/vpandp/wp-content/themes/secondedition/doc/VPandV_WhitePaper.pdf (Last accessed 28/09/21)

[8] Atlantic Systems Guild Ltd., "Volere Requirements Resources", http://www.volere.co.uk/ (Last accessed 28/09/21)

[9] DEDICAT 6G Deliverable D1.3 "Data Management Plan".

[10] DIKY Pyramid, Wikipedia page https://en.wikipedia.org/wiki/DIKW_pyramid (Last accessed 28/09/21)

[11] "IoT-A Deliverable D1.5 – Final Architectural Reference Model for the IoT v3.0", Carrez, F. editor https://www.dropbox.com/s/8u9yfbmxbwskw2w/D1.5%20%202013.07.15%20VERYFINAL.pdf?dl=0 (Last accessed 28/09/21)

[12] 3GPP TS 23.501 V1.0.0, "System Architecture for the 5G System; Stage 2 (Release 15)", June 2017.

[13] 3GPP TS 23.791 V1.0.0, "Study of enablers for Network Automation for 5G; (Release 16)", December 2018.

[14] https://derekcheung.medium.com/5g-core-pdu-session-and-qos-part-1-a12852e1b342 (Last accessed 28/09/21)

[15] 3GPP, Specification 23.502 "Procedures for the 5G System (5GS)", Release 15, 3GPP, 2017.

[16] 3GPP TS 23.791 V1.0.0, "Architecture enhancements for 5G System (5GS) to support network data analytics services; (Release 16)", June 2019.

[17] 3GPP TS 23.791 V1.0.0, " 5G System; Network Data Analytics Services; Stage 3 (Release 15)", June 2018.

[18] ETSI MEC, "Multi-access Edge Computing (MEC) 5G Integration, V2.1.1", ETSI, 2020

[19] Innovation in 5G backhaul technologies, June 2020, [online] Available: https://www.5gamericas.org/wp-content/uploads/2020/06/Innovations-in-5G-Backhaul-Technologies-WP-PDF.pdf (Last accessed 28/09/21)

[20] 3GPP, "TR 38.801, Technical Specifications Group Radio Access Network: Study on new radio access technology: Radio access architecture and interfaces," 3GPP, 2017.

[21] ITU-T, "Technical Report GSTR-TN5G - Transport network support of IMT-2020/5G," ITU-T, 2018.

[22] 3GPP, "Study on New Radio Access Technology: Radio Access Architectures and Interfaces. 3GPP Technical Specification," 3GPP, 2018.

[23] [ETSI-NFV] ETSI, "NFV Release 4 Definition", ETSI, 2021.

7 ANNEX A: List of Unified Scenario Requirements

As mentioned in the Requirement Engineering section, the unification process took place in two steps, in order to make it easier to deal with:

- Unification of the Scenario requirements (4 groups of 2 tables in D2.1) into 2 tables in this deliverable;
- Unification of the Unified Scenario requirements with the platform requirements with as a result the two Table 11 and Table 12 which are the absolute reference for DEDICAT 6G as far as requirements are concerned.

We present hereafter in Table 23 (resp. Table 24) the list of unified scenario functional (resp. non-functional and non-technical) requirements.

Note: The "Comment" column keeps track of the initial reference ID as stated in D2.1, providing then full traceability (x-y meaning: y^{th} requirement of scenario x). Since requirement analysis includes handling redundancies, one single requirement may track back to more than one initial scenario requirements.

7.1 Unified scenario functional requirements

Table 23: List of unified scenario functional requirements

ID	Category	Description	P	Rationale	Fit Criterion	Comment
SF-1	Security	It must be able to **identify** and **authenticate** devices/pieces of equipment and actors and **authorize** them to perform specific actions without requiring access to a centralized authentication/authorization entity	H	Edge computing system must be able to perform authentication and authorization autonomously in emergency situations where related cloud services are not available, ensuring therefore highest level of trust in un-conventional context	Check - Identity provided and verified with and without access to centralized identity provider	1-1; 3-8
SF-2	Security	The authorization system must provide the ability to define various level profiles that can therefore assigned to groups of people. (authorization by role vs. authorization by ID)	H	Accessible functionalities in smart warehousing setup should depend on predefined authorization levels: DEDICAT 6G admin, warehouse manager, warehouse personnel, test user	Configurable authorization levels implemented and tested.	1-5
SF-3	Trust	It must be possible to assess and assign a level of trust to	H	Devices and services must establish and confirm trust before	Trust metrics calculated and tested in experimental setups.	n/a

		each entity, node and actor participating to DEDICAT 6G operation. This trust level shall be based on a DEDICAT 6G dedicated metrics.		engaging in data exchange or any sort of interaction. Trustworthiness will be assessed with trust metrics (for devices, interfaces, users, processes, decisions, etc.) to be implemented within DEDICAT 6G trust management system.		
SF-4	Trustworthiness	During DEDICAT 6G operation (e.g., intelligence distribution, coverage extension, …) it must be possible to assess end-to-end trust based on individual level of trust of entities engaged in that operation.	H	Certain critical DEDICAT 6G operation requires checking overall trust levels of entities potentially involved into an operation prior to actually performing it (e.g., devices, actors, processes ,…)	Trust metrics calculated and tested in experimental setups.	1-7 & 1-8
SF-5	Security, privacy, trust	Communication between all nodes shall be realized in a secure and trusted manner (if required) and must follow best practices in communication channel encryption	H	The system operation and configuration should be restricted to DEDICAT staff only.	Check based on experimental setup. We need project level fit criterion for this requirement.	1-28, 2-15 & 3-20
SF-6	Security, privacy and trust	A device or node must not be used for dynamic coverage extension or intelligence distribution without the approval of the user/owner/operator of the device/node.	H	Node/resource owners must be able to make decision about their resources and devices being utilized in local ad-hoc networks with devices belonging to other users.	Approve two out of three nodes and trigger coverage extension or intelligence redistribution and observe which nodes are involved in ad-hoc networks.	1-17, 3-22
SF-7	Security	It must be possible in certain circumstances to perform actuation upon an IoT actuator (e.g., a door lock) without relying on global communication (like Internet)		Have an option to access and utilize cyber-physical security systems like control of locks and alarms without access to central command (accessed through internet connection)	System interacts with mobile devices (e.g., smartphones) and performs authorized actuation (onboard relay trigger)	3-7 related to 1
SF-8	Security, privacy and trust	DEDICAT 6G must provide ways to protect private data stored in nodes partaking to DEDICAT 6G operation (e.g., network extension, edge computing,…)	H	This needs to be enabled so that data obtained from a field node cannot be used in malicious manner.	Check that data in local storage is encrypted with selected method.	1-15, 3-21

SF-9	Management/Monitoring	Collecting performance logs from edge computing and communication nodes and systems in the backend. Local edge computing systems must be able to log performance of processes and resource utilization in every operational context.	H	Locally deployed computation and communication systems must be able to perform monitoring of established emergency processes and act on collected information in line with pre-defined set of rules. Collected data is sent to central platform for performance analysis and updates for local decision-making models. Exact performance metrics will be defined within project.	Access and completeness analysis of collected logs.	1-2, 3-9, NFREQ3-6, 2-10, & 4-14
SF-10	Management/Monitoring	DEDICAT 6G web dashboard for administration of the system instances and monitoring performance metrics of DEDICAT 6G resources and services (metrics to be specified within project)	H	Web dashboard to be provided for administrating the overall DEDICAT 6G system, performance monitoring and maintenance. It can be specialized for specific stakeholders of the project use-cases.	Web dashboard available on URL and tested in experimental setups.	1-4
SF-11	Management	DEDICAT6G could provide a way to access incident log on demand through a dedicated dashboard	L	As part of the F of FCAPS	Trigger reporting procedure, receive test report and check its content.	1-14
SF-12	Management	DEDICAT 6G smart warehousing procedures can send push notifications to managers and personnel	H	Push notifications provide information on daily tasks, alerts and status of the DEDICAT 6G resources.	Check that push notifications are delivered to DEDICAT 6G mobile application	1-20
SF-13	Management	Configurable safety zones and parameters	H	IoT system needs to support configurable safety zones through web dashboard interface where digitalized warehouse layout is provided. These zones need to be configured by warehouse manager in line with operating context (e.g., offloading of dangerous products).	DEDICAT 6G web dashboard provides interface for safety zone configuration. IoT system monitors location/movement of mobile assets and personnel and sends triggers when a mobile asset or personnel member enters safety zone.	1-21

SF-14	Management	AGVs can be shut down remotely	M	Warehouse managers need to be able to remotely shut down AGV in case it is faulty in any way or in case energy needs to be reserved.	Trigger AGV shutdown through web dashboard and observe AGV ceasing all operation.	1-29
SF-15	Management	It must be possible to configure existing node in such a way they can be become part (or leave) of the DEDICAT 6G eco-system		new devices or piece of equipment can be added as candidate for intelligence migration, edge networking or any other specific DEDICAT 6G operation	check GUI	NFREQ1-1
SF-16	Management	The system must be able to be remotely controlled and configured	H	To allow testing and evaluation, the systems will be configured and controlled remotely	Checked that the system can be accessed remotely.	4-7
SF-17	Management	Remote access to deployed DEDICAT 6G resources and equipment must be enabled	H	Warehouse managers must be able to manage deployed resources (AGVs, IoT system) remotely with minimal latency.	Warehouse manager sends command (e.g., make sound signal) to AGV through web dashboard accessed over Internet. Warehouse manager can trigger onboard relays of IoT controllers remotely – door opens.	NFREQ1-7
SF-18	Performance Analytics	DEDICAT 6G must provide ways to assess/measure the performance of the system components and operations	H	Measure, evaluate and analyse the developed components via performance indicators	Comparison to key performance indicators (KPIs)	NFREQ2-4
SF-19	Performance /Machine Learning	The dynamic changes of networks conditions and performance over time are collected and analysed in a central node.	H	Various network conditions (including the traffic load levels, traffic spatial distribution patterns, etc.) and the network performance achieved multiple APs can be analysed for coordination of multiple APs with machine learning.	Checked.	
SF-20	Edge processing	AGV performs edge processing for self navigation and interaction with personnel and warehouse systems	H	AGV will act as a mobile computing node capable of analyzing collected information and making decisions in context of smart warehouse operation	Software developed and deployed. Data analysis and decision-making algorithms implemented in code as part of AGV firmware/subsystem.	1-9

				and DEDICAT 6G system operation		
SF-21	Edge processing	DEDICAT 6G mobile app performs processing necessary for AR interface	M	DEDICAT 6G mobile app should be able to perform data analysis processes and decision making by using computing and data storage resources of mobile devices (smartphone or tablet) on which it is deployed. This way the AR features can be supported with and without access to centralized services.	Check in experimental setup. Mobile app installed on a mobile device and check that it is capable of performing implemented ML tasks required for AR functionality.	1-11 (???)
SF-22	Edge Computing	It shall be possible to identify the need for (re-)distribution of intelligence.	H	DEDICAT 6G system in context of smart warehousing needs to be capable of identifying (re)distributed intelligence needs and opportunities while relying on AGVs, mobile devices with DEDICAT 6G app and deployed IoT controllers.	Check that trigger is properly recognized. We need project level fit-criterion for identifying the need for redistribution of intelligence.	1-33, 3-13 (is normally already captured by context-aware decision making)
SF-23	Edge Computing	It must be possible to dynamically distribute computation between central and edge nodes	H	Intelligence can be distributed across central and edge nodes based on the needs of the operational context.	Check that process for data analysis can run on central and at least two edge nodes in a federated manner.	1-36, 3-16
SF-24	Edge Computing	Gait analysis for attendees must be operated at the attendee's UE side	H	Abnormal Crowd movement detection is based on individual gait analysis and must be handled at the edge to minimize both bandwidth consumption and computation utilization at the cloud side	Crowd movement detection performs as expected	3-1
SF-25	Edge Computing	DEDICAT 6G must provide Context-aware Decision making algorithms to support and enable the dynamic migration of intelligence towards the edge (when it is required) Those mechanisms must consider which nodes should be used, which functions should	H	DEDICAT 6G system must run algorithms for load balancing decision making in order to balance workload between the cloud and edges depending on context and policies	check in experimental set-up	1-27, 3-19

		be distributed to which nodes, etc.)				
SF-26	Edge Computing	IoT controllers perform edge processing and decision making for indoor positioning and monitoring of environmental parameters	H	Deployed IoT system should include edge IoT controllers capable of performing data analysis and decision making in context of smart warehouse operation and DEDICAT 6G system operation. Edge IoT controllers will allow smart warehousing operation to be performed with and without support or access to the server side processes.	Software developed and deployed. Data analysis and decision-making algorithms implemented in code as part of IoT controller's firmware/subsystem.	1-10 Specialization of the next one)
SF-27	Decision Making	DEDICAT 6G must provide context-aware decision making algorithm based on a variety of context data (networking, load, performance, QoS, loss of service, weather-related…)	H	DEDICAT 6G system needs to be able to provide decisions/alerts/ notifications based on results of analysis of collected data at various levels in the whole system	Emulate sensory data out of predefined range and observe decision making algorithms result in triggering event.	1-24
SF-28	Decision Making	DEDICAT 6G should provide algorithm that recalculate AGV route according to changes in warehouse layout	M	AGVs need to adapt to changes in warehouse layout as result of offloading and placement of products – dynamic obstacles. Precise indoor positioning will be used to feed the algorithm.	Set mobility route (point A to point B) for AGV, put obstacle on the rout and monitor AGV ability to reach destination without manual reconfiguration.	1-23
SF-29	Decision Making	Crowd Movement analysis must be provided in order to trigger emergency response	H	Natural disaster or terror attack generally results in hectic crowd movements	Such simulated crowd movements are detected	3-2
SF-30	Networking	IoT controllers should be able to reach servers/cloud system through auxiliary communication paths	M	If a direct communication channel (wired or wireless) between IoT controller and IoT system server/cloud is disabled or overloaded, the controller should be able to utilize local wireless communication network to reach a node with access to the Internet/cloud services.	Disconnect/ disable primary interface and observe that IoT controller is able to connect with the cloud system.	1-13

SF-31	Network-ing	A vehicle or device in the proximity of the MAP should be able to receive information transmitted by the MAP. Thus, these should be in the same network.	H	A vehicle in specific proximity of the roundabout should be able to receive information	It is tested that information can be received in a specific proximity from the MAP.	4-3, 4-13
SF-32	Network-ing, load balancing	The live streaming from the event to multiple simultaneous users relying on the ability to dynamically switch from unicast to multicast	H	The mobile multicast feature usage needs support from the operating network and requires guaranteed input throughput and latency. According to number of simultaneous users' handover from unicast to multicast is done for bandwidth savings.	BMSC server messages help to resolve possible interoperability issues. A decrease in mobile data traffic will be monitored and measured. S	2-5
SF-33	Network-ing, Load balancing	When UE devices support the multi-connectivity feature, UE association solution is required to fully utilized network resources.	H	Depending on a given condition (including the traffic congestion levels of networks, channel conditions, etc.), UE can be connected to networks via multiple links at the same time (e.g., a MAP and macro-BS).	Measured: The efficiency of load balancing will be derived from the measured network performance.	2-1
SF-34	Network Coverage Ext.	The (ad'hoc) Network Coverage Extension (creation/update/termination) will be triggered by Context-aware Decision making algorithms,	H	DEDICAT 6G system must run algorithms for coverage extension decision making in order to enable uninterrupted access to key resources and services by all participating nodes and with specific focus on mobile nodes like AGVs.	Move AGV in warehouse area without fixed wireless network (the main network used within warehouse) coverage and observe other communication nodes establish communication link towards the AGV. AGV maintains access to core services.	1-25, 1-26, 2-11, NFREQ3-7, 3-18 (***)
SF-35	Network Coverage Ext.	It shall be possible to identify the need for a dynamic coverage extension.	H	DEDICAT 6G system in context of smart warehousing needs to be capable of identifying coverage extension needs and opportunities while relying on AGVs and deployed IoT system.	Check that trigger is properly recognized. We need project level fit-criterion for identifying the need for coverage extension.	1-32, 3-12, 4-11 (induced by (***)

SF-36	Network Coverage Ext.	In some circumstances the coverage extension must be self-organised without help from cloud-based mechanisms	H	During crisis management there is no time and qualified tech for network configuration	Ad-hoc network performs as expected and bear the load	3-6
SF-37	Network Coverage Ext.	AGVs/Robots, Drones, cars and other devices should be able to communicate with each other and with the "central" network infrastructure (unless it is not available due to crisis situation).	H	This is required for setting up an ad-hoc network where an AGV/robot or drone may be playing the role of a mobile access point (MAP).	Check data propagation between end points (ping messages between points).	1-12, 1-30, 3-10, 4-2
SF-38	Network Coverage Ext.	Device and infrastructure capable to set-up connection	H	A device in an ad-hoc coverage extension network shall be able to set-up a connection with the central infrastructure. The infrastructure shall be able to trigger a device in an ad-hoc coverage extension network to set-up a connection.	Check that a device in an ad-hoc network can ping the central infrastructure. Check that the infrastructure can trigger the device to set up a connection with other devices.	1-34, 3-14 ???
SF-39	Network Coverage Ext.	Relaying should be supported by central nodes or by edge nodes.	M	This will allow forwarding of data and control signalling in the scope of dynamic coverage extension through an ad-hoc network.	Move AGV in area without fixed wireless network (the main network used within warehouse) coverage and observe other communication nodes establish communication link towards the AGV. AGV maintains access to core services.	1-31,3-11 sound linked to ad'hoc networking
SF-40	Network Coverage Ext.	More than one (ad'hoc) coverage extension networks must be supported at the same time.	H	Different ad-hoc networks established across shared nodes and in close vicinity must minimize mutual interference and share resources.	Setup two ad-hoc networks and monitor communication performance metrics (delay, packet drop rate, throughput).	1-35, 3-15
SF-41	Network Coverage Ext.	DEDICAT 6G could be able to determine the optimal geographical distribution of MAP when initiating network coverage extension, according to the current context	L	MAPs' positions will impact on various network performance (e.g., the num. of served UEs, sum data rate, spectral efficiency, energy efficiency, etc.)	Measured: When the locations of heavy data traffic generation vary over time, whether MAPs' position can be decided.	2-3

SF-42	Context-Awareness	DEDICAT 6G must provide mechanisms that collect and communicate element of context (sensor-based, probe-base etc…)	H	Context is needed in order to feed the Context-aware decision making or any other context-dependent functional component	Check implementaton	1-16, 1-19, 3-17
SF-43	Context-Awareness	DEDICAT 6G must provide high precision indoor positioning performed with edge computing and utilizing fixed, mobile nodes and BLE beacons	H	The indoor positioning will be used for tracking mobile assets and for triggering safety rules based on proximity of tracked assets and personnel.	DEDICAT 6G web dashboard displays precise location of tracked assets and personnel and their BLE beacons on the warehouse layout. Location precision is in radius of 1 meter.	1-22 (more specific on indoor loc)
SF-44	Context-Awareness	The car should be able to recognize the presence of a VRU via the LIDAR/camera.	H	Detection of VRU is essential for increasing the road safety.	VRU is detected within specified timing and range constraints.	4-1
SF-45	MMI	DEDICAT 6G mobile app for configuring and utilizing the deployed solution instance. Used by warehouse personnel and management.	H	Mobile app to be developed to support smart warehousing use-case. It will be the main interface through which end-users interact with the system.	Mobile app published and tested in experimental setups.	1-3
SF-46	MMI	AR interface for smart warehouse use-case for mobile apps	H	Smart warehouse use-case scenarios require AR interface for realization of the objectives. This interface will be part of DEDICAT 6G mobile application.	AR interface implemented as part of DEDICAT 6G mobile app and tested in experimental setups.	1-18
SF-47	MMI	The Smart Glasses must display vital and essential information to the bearer amid crisis management.	H	During crisis management visualizing essential information must be possible without hand manipulation of the smart phone	Vital and essential information, as described in the final users' requirements document, are displayed on the Smart Glasses.	3-4
SF-48	MMI	The Smart Glasses must be fully integrated with the overall system and interfaced with the smart phone	H	Indeed, a rescuer or first responder is connected with the DEDICAT 6G platform with the smart phone	The Smart Glasses device is connected to the user's Smartphone device. Information displayed on Smart Glasses is duplicated on Smartphone device.	3-5
SF-49	MMI	The car must be able to warn the driver about the presence of a VRU on an HMI	H	The driver must get a visual warning when VRU is present	Checked that the driver can get a warning about VRU presence.	4-4

SF-50	MMI	The system must be able to present information on the presence of a car to the VRU	H	The VRU must be warned when a car is on a colliding path.	Checked that the VRU is warned when a car is on a colliding path.	4-6

7.2 Unified scenario non-functional or non-technical requirements

Table 24: List of unified scenario non-functional or non-technical requirements

ID	Category	Description	P	Rationale	Fit Criterion	Comment
SNF-1	Privacy	Privacy sensitive information from personnel must be anonymized when stored and processed	H	Privacy protection must be ensured with best practice approaches for anonymization of the personally identifiable information when transferred and stored.	Check data collected at source (personal data) and check data when stored in database – confirm that data is anonymized.	1-15
SNF-2	Data protection	Depending on the context, it should be able to decide where and whether certain data can be stored depending on its very nature (private, sensitive, classified etc…)	M	Warehouse managers can select data that need to remain within warehouse logical perimeter and not transferred to 3rd parties. Event organizer may forbid the storage of live stream videos.	Check depending on context and associated policy	1-16, 2-7
SNF-3	Ethics	The system shall follow appropriate health and safety procedures conforming to relevant local/national/EU guidelines/legislation in order to protect the environment and people.	H	Health and safety procedures need to be translated into system automation and decision-making processes provided by DEDICAT 6G system.	Translate selected regulation into specific set of automation and decision-making rules. Confirm completeness.	1-9, 3-2
SNF-4	Ethics	The system shall include measures and tools to safeguard from misuse of data collected in alignment with the GDPR.	H			3-4
SNF-5	Ethics	The system should keep a log of places, moments and trajectories where personal data is compiled,	H	This is important for privacy and data protection audits that can be requested by regulatory bodies.	Setup logging procedure, generate logs and check their completeness in different experimental setups.	1-10, 3-3

		transferred, stored, deleted, anonymized (or pseudonymized) or processed in any other way.				
SNF-6	Privacy, ethnics	DEDICAT 6G must provide mechanism for handling selected privacy issues using Consent Forms (e.g., amid the various Android Apps used in the project) and Term & Condition	H	In certain circumstances it may be very difficult or even impossible to guaranty full privacy without asking for formal permission. In other cases, the use, transfer and storage of personal data may also require user's permission (this does not prevent the use of anonymisation and encryption)	Compliance to regulations	2-1, 3-1
SNF-7	Privacy, Ethics	DEDICAT 6G must provide mechanisms that enforces data usage policies (use of Term & Condition forms, non repudiation, accountability,..)	H	Data potentially captured or exchange may be subject to restriction or even may be forbidden by event organizers		2-5
SNF-8	Privacy, ethics	Position information of road users must be collected for locating the nodes in the map and must be handled in such a way the privacy of the user is maintained	H	App displayed on the HMI of the UEs must continuously gather location information of the users	Compliance to regulation	4-5
SNF-9	Privacy, Ethics	Video feed should be collected by cameras on the car and their treatment should comply to regulation	M	Camera on the car will continuously record the situation at the intersection	Compliance to regulation	4-6
SNF-10	Context-awareness	The system shall be context aware.	H	The system shall be able to obtain information on: • application, service and network goals and objectives to be achieved, as well as potential policies. • capabilities of network elements, MAPs and edge devices in terms of communication networking (e.g., radio access technologies	Check based on defined experiments. Check that the system is able to infer the current system context/situation.	1-37, FREQ1-16, FREQ3-17, 4-10

				(RATs) and spectrum, capacity, and coverage), physical movement, the type of the MAP, computation capabilities, storage capabilities and available power. The system should maintain information and knowledge on the context that has to be addressed in terms of • computation tasks, • power consumption requirements, • set of mobile nodes that need coverage, • mobility and traffic profiles of the different nodes, • radio quality experienced by client nodes, options for connecting to wide area networks, • the locations of docking and charging stations for drone and robot MAPs and • the current locations of the terminals and MAPs' elements, cars... Knowledge about floor plan, system layout		
SNF-11	Performance	The system should be able to balance load distributed on the edge nodes	M	To avoid too much load on specific devices, especially when computing power is limited.	Load distribution should happen within application-specific timing constraints.	FREQ2-12, FREQ4-8
SNF-12	Performance	The user perceived quality of service/quality of experience shall not be negatively affected by the dynamic coverage extension and intelligence distribution.	H	The coverage extensions and distributed intelligence must improve or maintain perceived QoE and QoS in order to justify creation of ad-hoc opportunistic systems.	We need project level fit criterion for user QoS and QoE assessment	FREQ1-38, NFREQ1-18, FREQ2-3-8

SNF-13	Performance	Critical communication shall not be decreased when DEDICAT 6G is deployed on the scene.	H	Based on legacy and 5G specifications, the average time to response has to be equal or less than existing specification in 3GPP Mission Critical (MCX) standards.	Measure the latency between UE during a MC-PTT call. The time shall not be decreased.	FREQ3-24
SNF-14	Performance	On multiple connection, the system has to support the QoS and shall not decrease during crisis management	M	When the worst happened, the Quality of Services shall keep similar value compared to 3GPP MCS standards in any cases.	Measure of QoS. QoS measured shall not be decreased regarding the 3GPP MCS standards.	FREQ3-26
SNF-15	Performance	Latency for Crowd movement analysis must be reasonably low (e.g., a few seconds max)	H	The slowest the detection is the largest the casualty count will be	Measured	3-5
SNF-16	Performance	DEDICAT 6G must provide reliable communication	H	Communication between all the devices in all circumstances should be high reliable (99.999%).	No loss of information should be occurred between actors and no delays in the communication due to instable situations	4-4 What is meant by "reliable"
SNF-17	Performance	DEDICAT 6G must provide overall performance metrics and implement mechanisms that can assess the platform performance against those metrics	H	How the DEDICAT 6G system or sub-system performs, what succeeded and what did not.	Pass/Fail criteria	2-3
SNF-18	Usability	End-users must not be involved in the processes for dynamic coverage extension, intelligence distribution and security, privacy and trust assurance.	H	The system complexity should be hidden from the user.	Check that coverage extension and intelligence redistribution is performed automatically without user intervention and that these processes are transparent to the user.	1-17, 2-13, FREQ3-23
SNF-19	Interoperability	DEDICAT 6G should be able to interface with selected systems already deployed in locations where use-cases are realized	M	Interfacing can be done through existing APIs, control points, databases etc. Interoperability with key services and resources already deployed in a warehouse is needed.	Integration completed and tested with message exchanges between end points.	1-13

SNF-20	Interoperability	The technology promoted by DEDICAT 6G to supporting dynamic edge computing, should ensure that it is deployable and interoperable with any Edge node.	M	To support the load balancing requirement, applications should be able to be run by any nodes	VRU Application components can be executed on RSUs and vehicles, independent of software and hardware architectures.	FREQ4-9 should be HIGH
SNF-21	Scalability	The specific solutions developed amid the different DEDICAT 6G scenarios must encourage minimum configuration time in order to maximize applicability/reuse in different contexts	H	It is important that solutions developed for e.g., one smart warehouse, one smart Highway configuration or a specific event can be deployed easily to a different smart warehouse, different highway or event, with minimum re-configurations.	TBD	FREQ1-6, 1-14
SNF-22	Scalability, Interoperability	DEDICAT 6G should be designed in such a way, interoperability with new IT system or equipment is possible and minimized in term of cost.	M	It should be able to elect new IT system or pieces of equipment as part of the cloud architecture or as part of the edge, e.g., new drones, robots from different providers.	Field trial based on interface documentation and architecture doc.	1-1, 1-8
SNF-23	Deployment, Performance	On loss of network infrastructure after a natural disaster, the DEDICAT 6G infrastructure should be deployed as fast as possible.	M	Depending on publication and reports on disaster response, the deployment of DEDICAT 6G shall be faster than legacy solution (divided by 2).	Evaluation of deployment time during recovery phase. Results should improve Response Times during the Recovery phase compared to legacy methods.	FREQ3-25 divided by 2, compared to wh