



“5G for Drone-based Vertical Applications”

D1.5 – Description of the 5G trial facilities and use-case mapping

Document ID:	D1.5
Deliverable Title:	Description of the 5G trial facilities and use-case mapping
Responsible Beneficiary:	UO
Topic:	H2020-ICT-2018-2020/H2020-ICT-2018-3
Project Title:	Unmanned Aerial Vehicle Vertical Applications' Trials Leveraging Advanced 5G Facilities
Project Number:	857031
Project Acronym:	5G!Drones
Project Start Date:	June 1 st , 2019
Project Duration:	36 Months
Contractual Delivery Date:	M12
Actual Delivery Date:	May 29 th , 2020
Dissemination Level:	Public (PU)
Contributing Beneficiaries:	UO, THA, ALE, INV, HEP, NCSRD, AU, COS, UMS, INF, NOK, EUR, DRR, CAF



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 857031.

Document ID: D1.5

Version: V2

Version Date: May 29th, 2020

Authors: Abdelquodouss Laghrissi, Antti Tikanmäki, Idris Badmus, Juha Röning, Jussi Haapola, Vesa Halonen (UO), Adlen Ksentini, Maha Bouaziz (EUR), Johannes Jyrkkä, Janne Väättäri, Ilkka Finning, Mika Järvenpää, Ilkka Käsälä (NOK), Vaio Koumaras, Christos Sakkas, Aggeliki Papaioannou (INF), Viljar Vooremäe, Siim Heering (HEP), Tanel Järvet (CAF), Abderrahmane Abada, Damoon Shahbaztabar, Oussama Bekkouche, Tarik Taleb, Hamed Hellaoui (AU), Tomas Gareau, Nemish Mehta (UMS), Grégoire Guerout, François Despaux (ALE), Harilaos Koumaras, Stavros Kolometsos, Anastasios Gogos (NCSRD), Fofy Setaki (COS), Paweł Montowtt, Mélanie Guittet (INV), Paweł Korzec (DRR)

Security: Public

Approvals

	Name	Organization	Date
Coordinator	Jussi Haapola	UO	May 29 th , 2020
Technical Committee	Pascal Bisson	THA	May 22 nd , 2020
Management Committee	Project Management Team, NCSRD (reviewer)	UO, THA, AU, AIR, UMS, FRQ, NCSRD	May 22 nd , 2020

Document History

Version	Contribution	Authors	Date
V0.1	Table of Contents	UO	January 28 th , 2020
V1	First complete version	UO, EUR, NCSRD, COS, AU, NOK, CAF, INV, DRR, HEP, UMS, ALE, INF	May 6 th , 2020
V2	Final version	UO, THA, EUR, NCSRD, COS, AU, NOK, CAF, INV, DRR, HEP, UMS, ALE, INF	May 29 th , 2020

Executive Summary

This Deliverable aims at extensively describing different partners' 5G facilities required to carry out trial experiments in the 5G!Drones project, with a focus on the upgrades and new features offered, as well as the security mechanisms in place. The deliverable is an extension of the description of the 5G trial facilities in D1.2, as it details the radio and core network capabilities of each facility, the edge computing technologies supported, and the interactions with the trial controller. It also provides a more advanced mapping of use-case scenarios and facilities, initially introduced in D1.2. This mapping is expressed through a set of functional components that will permit the deployment of a given scenario. These components are first mapped within an architecture proper to each scenario deployment, and then categorized into UAV components, UAV operator components, UTM components, and 5G components.

Table of Contents

EXECUTIVE SUMMARY	3
TABLE OF CONTENTS.....	4
TABLE OF FIGURES.....	6
TABLE OF TABLES.....	7
LIST OF ABBREVIATIONS	8
1. INTRODUCTION.....	11
1.1. OBJECTIVE OF THE DOCUMENT	11
1.2. STRUCTURE OF THE DOCUMENT	11
1.3. TARGET AUDIENCE.....	11
2. 5GENESIS	12
2.1. HIGHLIGHTS OF 5G COMPONENTS/ ENABLERS WITHIN THE FACILITY FOR USE CASE DEPLOYMENT	12
2.1.1. Architecture.....	12
2.1.2. Network Infrastructure	16
2.1.3. Computing infrastructure.....	18
2.1.4. Orchestration and management.....	18
2.1.5. Coordination Layer	21
2.1.6. Security features in 5GENESIS.....	21
2.2. FACILITY INTERACTION WITH THE TRIAL CONTROLLER FOR USE CASE DEPLOYMENT.....	22
2.2.1. Deployment of a Trial	22
2.3. DETAILED MAPPING TO THE FACILITY OF UC4 SCENARIO 1 - CONNECTIVITY EXTENSION & OFFLOADING DURING CROWDED EVENTS.....	24
3. 5GEVE.....	32
3.1. HIGHLIGHTS OF 5G COMPONENTS/ENABLERS WITHIN THE FACILITY FOR USE CASE DEPLOYMENT	32
3.1.1. Architecture.....	32
3.1.2. Network Infrastructure	33
3.1.3. Computing infrastructure.....	34
3.1.4. Orchestration and management.....	35
3.1.5. Security features in 5GEVE.....	38
3.2. FACILITY INTERACTION WITH THE TRIAL CONTROLLER FOR USE CASE DEPLOYMENT.....	38
3.2.1. Deployment of a Trial	38
3.3. DETAILED MAPPING OF USE CASE SCENARIO COMPONENTS TO THE 5G FACILITY.....	39
3.3.1. UC1 scenario 1 - UTM Control and command application	39
3.3.2. UC2 Scenario1 - Monitoring a wildfire	42
3.3.3. UC2 Scenario 2 - Disaster recovery.....	44
4. X-NETWORK.....	47
4.1. HIGHLIGHTS OF 5G COMPONENTS/ ENABLERS WITHIN THE FACILITY FOR USE CASE DEPLOYMENT	47
4.1.1. Architecture.....	47
4.1.2. Network Infrastructure	47
4.1.3. Computing infrastructure.....	49
4.1.4. Orchestration and management.....	49
4.1.5. Security features in X-Network.....	51
4.2. FACILITY INTERACTION WITH THE TRIAL CONTROLLER FOR USE CASE DEPLOYMENT.....	51

4.2.1.	Deployment of a Trial	51
4.3.	DETAILED MAPPING OF USE CASE SCENARIO COMPONENTS TO THE 5G FACILITY.....	52
4.3.1.	UC3 scenario 2 - UAV-based IoT data collection	52
4.3.2.	UC1 scenario 3 - Drone logistics.....	53
5.	5GTN.....	56
5.1.	HIGHLIGHTS OF 5G COMPONENTS/ ENABLERS WITHIN THE FACILITY FOR USE CASE DEPLOYMENT	56
5.1.1.	Architecture.....	56
5.1.2.	Network Infrastructure	56
5.1.3.	Computing infrastructure	58
5.1.4.	Orchestration and management.....	61
5.1.5.	Security features in 5GTN	64
5.2.	FACILITY INTERACTION WITH THE TRIAL CONTROLLER FOR USE CASE DEPLOYMENT.....	67
5.2.1.	Deployment of a Trial	67
5.2.2.	KPI Metrics	68
5.3.	DETAILED MAPPING OF USE CASE SCENARIO COMPONENTS TO THE 5G FACILITY.....	71
5.3.1.	UC1 scenario 2 - 3D mapping and supporting visualization/analysis software for UTM	71
5.3.2.	UC2 scenario 3 - Police and counter-UAS	75
5.3.3.	UC3 scenario 1 Sub-Scenario 1 -3D Mapping of 5G QoS	77
5.3.4.	UC3 scenario 1 Sub-Scenario 2 -Long range power line inspection	80
5.3.5.	UC3 scenario 1 Sub-Scenario 3 - Inspection and search & recovery operations in large body of water	81
5.3.6.	UC3 scenario 3 - Location of UE in non-GPS environments	83
	CONCLUSIONS	86
	REFERENCES	87

Table of Figures

FIGURE 1 - 5G!DRONES ARCHITECTURE	13
FIGURE 2 - 5GENESIS ARCHITECTURE.....	13
FIGURE 3 - 5G!DRONES ENHANCED 5GENESIS ARCHITECTURE.....	14
FIGURE 4 - 5GENESIS 5G NSA.....	17
FIGURE 5 - 5GENESIS WEB PORTAL	23
FIGURE 6 - USE CASE 4 - SCENARIO 1 COMPONENTS.....	25
FIGURE 7 - UC4 SCENARIO 1- FUNCTIONAL COMPONENTS AND THEIR MAPPING TO THE FACILITY	26
FIGURE 8 - UAV CONNECTION TO UL-CCP	27
FIGURE 9 - 5GEVE-SA ARCHITECTURE.....	33
FIGURE 10 - NETWORK CONNECTIVITY - 5G NSA.....	34
FIGURE 11 - INTEGRATION OF APPD INTO AN NSD	36
FIGURE 12 - EXAMPLE OF 5GEVE-SA NST	37
FIGURE 13 - 5GEVE-SA WEB PORTAL ARCHITECTURE	38
FIGURE 14 - UC1SC1- FUNCTIONAL COMPONENTS AND THEIR MAPPING TO THE FACILITY.....	40
FIGURE 15 - UC2 SCENARIO 1- FUNCTIONAL COMPONENTS AND THEIR MAPPING TO THE FACILITY.....	43
FIGURE 16 - UC 2 SCENARIO 2 - FUNCTIONAL COMPONENTS AND THEIR MAPPING TO THE FACILITY.....	45
FIGURE 17 - OVERVIEW OF THE NETWORK DEPLOYMENT IN AALTO UNIVERSITY	47
FIGURE 18 - OVERVIEW OF THE EPC/5GC ARCHITECTURE.....	48
FIGURE 19 - OVERVIEW OF THE CURRENT/PLANNED ORCHESTRATION SOLUTION AT X-NETWORK.....	49
FIGURE 20 - AN EXAMPLE OF A NST USED IN X-NETWORK.....	50
FIGURE 21 - SCREENSHOT OF THE WEB PORTAL USED AT AALTO UNIVERSITY	51
FIGURE 22 - UC3 SCENARIO 2 - FUNCTIONAL COMPONENTS AND THEIR MAPPING TO THE FACILITY	52
FIGURE 23-UC1 SCENARIO 3 - FUNCTIONAL COMPONENTS AND THEIR MAPPING TO THE FACILITY.....	54
FIGURE 24 - 5GTN UO NETWORK ARCHITECTURE	56
FIGURE 25 - 5GTN NETWORK INFRASTRUCTURE.....	57
FIGURE 26 - OVERALL DESCRIPTION OF NOKIA vMEC USED IN THE 5GTN	58
FIGURE 27 - NCIR ARCHITECTURAL DISPLAY	59
FIGURE 28 - HIGH-LEVEL FLOW OF ALCM OPERATIONS	60
FIGURE 29 - VNFD EXAMPLE USED IN 5GTN.....	61
FIGURE 30 - OSM HIERARCHICAL APPROACH FOR NETWORK SLICING USED IN 5GTN.....	62
FIGURE 31 - NST EXAMPLE USED IN 5GTN	63
FIGURE 32 - OVERVIEW OF 5GTN SECURITY	64
FIGURE 33 – vMEC IPSEC CONNECTIVITY	65
FIGURE 34 - USE CASE DEPLOYMENT ARCHITECTURE IN 5GTN.....	67
FIGURE 35 - SEQUENCE DIAGRAM FOR TRIAL DEPLOYMENT IN 5GTN	68
FIGURE 36 - UC1 SCENARIO 2- FUNCTIONAL COMPONENTS AND THEIR MAPPING TO THE FACILITY IN THE FIRST DEPLOYMENT OPTION	72
FIGURE 37 - UC1 SCENARIO 2- FUNCTIONAL COMPONENTS AND THEIR MAPPING TO THE FACILITY IN THE SECOND DEPLOYMENT OPTION	73
FIGURE 38-UC2 SCENARIO 3 - FUNCTIONAL COMPONENTS AND THEIR MAPPING TO THE FACILITY.....	76
FIGURE 39 - UC3 SCENARIO 1 SUB-SCENARIO 1 - FUNCTIONAL COMPONENTS AND THEIR MAPPING TO THE FACILITY	78
FIGURE 40 - UC3 SCENARIO 1 SUB-SCENARIO 2 - FUNCTIONAL COMPONENTS AND THEIR MAPPING TO THE FACILITY	80
FIGURE 41 - UC3 SCENARIO 1 SUB-SCENARIO 3- FUNCTIONAL COMPONENTS AND THEIR MAPPING TO THE FACILITY	82
FIGURE 42 - UC3 SCENARIO 3- FUNCTIONAL COMPONENTS AND THEIR MAPPING TO THE FACILITY.....	84

Table of Tables

TABLE 1: 5GENESIS REVISED GAP ANALYSIS	15
TABLE 2: RAN COMPONENTS OF 5GENESIS ATHENS PLATFORM	16
TABLE 3: 5GENESIS ATHENS PLATFORM MANO COMPONENTS.....	19
TABLE 4: 5GENESIS ATHENS SUPPORTED KPIS.....	20
TABLE 5: 5GENESIS COORDINATION LAYER COMPONENTS.....	21
TABLE 6: 5GENESIS OPEN APIS.....	23
TABLE 7: UC4 SCENARIO 1 PARTNER/COMPONENTS	30
TABLE 8: UC4 SCENARIO 1 UAV COMPONENTS	30
TABLE 9: UC4 SCENARIO 1 UAV OPERATOR COMPONENTS	30
TABLE 10: UC4 SCENARIO 1 UTM COMPONENTS	31
TABLE 11: UC4 SCENARIO 1 5G COMPONENTS.....	31
TABLE 12: UC4 SCENARIO 1 OTHER COMPONENTS.....	31
TABLE 13: RAN COMPONENTS OF 5GEVE-SA	33
TABLE 14: ETSI MEC COMPONENTS AVAILABLE AT 5GEVE-SA	35
TABLE 15: SUPPORTED KPIS IN 5GEVE-SA.....	37
TABLE 16: NBI OF THE SO OF 5GEVE-SA.....	39
TABLE 17: UC1SC1 PARTNER/COMPONENTS.....	41
TABLE 18: UC1SC1 UAV COMPONENTS.....	41
TABLE 19: UC1SC1 UAV OPERATOR COMPONENTS	41
TABLE 20: UC1SC1 UTM COMPONENTS.....	41
TABLE 21: UC1SC1 5G COMPONENTS	42
TABLE 22: UC1SC1 OTHER COMPONENTS	42
TABLE 23: UC2 SCENARIO1 PARTNER/COMPONENTS	43
TABLE 24: UC2 SCENARIO1 UAV COMPONENTS.....	44
TABLE 25: UC2 SCENARIO1 UAV OPERATOR COMPONENTS.....	44
TABLE 26: UC2 SCENARIO1 UTM COMPONENTS	44
TABLE 27: UC2 SCENARIO1 5G COMPONENTS	44
TABLE 28: UC2 SCENARIO 2 UAV COMPONENTS	46
TABLE 29: UC2 SCENARIO 2 UAV OPERATOR COMPONENTS	46
TABLE 30: UC2 SCENARIO 2 UTM COMPONENTS.....	46
TABLE 31: UC2 SCENARIO 2 5G COMPONENTS	46
TABLE 32: UC2 SCENARIO 2 OTHER COMPONENTS	46
TABLE 33: RAN COMPONENTS OF X-NETWORK	48
TABLE 34: LIST OF KPIS THAT CAN BE MEASURED AT X-NETWORK	50
TABLE 35: NBI OF THE SO OF X-NETWORK.....	52
TABLE 36: UC3 SCENARIO 2 PARTNER/COMPONENTS	52
TABLE 37: UC3 SCENARIO 2 UAV COMPONENTS	53
TABLE 38: UC3 SCENARIO 2 UAV OPERATOR COMPONENTS	53
TABLE 39: UC3 SCENARIO 2 UTM COMPONENTS.....	53
TABLE 40: UC1 SCENARIO 3 PARTNER/COMPONENTS	54
TABLE 41: UC1 SCENARIO 3 UAV COMPONENTS	54
TABLE 42: UC1 SCENARIO 3 UAV OPERATOR COMPONENTS	54
TABLE 43: UC1 SCENARIO 3 UTM COMPONENTS.....	55
TABLE 44: UC1 SCENARIO 3 5G COMPONENTS	55
TABLE 45: UC1 SCENARIO 3 OTHER COMPONENTS	55
TABLE 46: RAN COMPONENTS OF 5GTN OULU PLATFORM	57
TABLE 47: IKEV2 PROFILES FOR LTE SSH	65
TABLE 48: IKEV2 PROFILES FOR LTE IPSEC.....	66
TABLE 49: KPIS AVAILABLE FOR MEASUREMENT IN 5GTN	69
TABLE 50: NBI OF THE SO IN 5GTN	71
TABLE 51: UC1 SCENARIO 2 UAV COMPONENTS	74
TABLE 52: UC1 SCENARIO 2 UAV OPERATOR COMPONENTS	74
TABLE 53: UC1 SCENARIO 2 UTM COMPONENTS.....	75
TABLE 54: UC1 SCENARIO 2 OTHER COMPONENTS	75
TABLE 55: UC2 SCENARIO 3 UAV COMPONENTS	76
TABLE 56: UC2 SCENARIO 3 UAV OPERATOR COMPONENTS	76

TABLE 57: UC2 SCENARIO 3 UTM COMPONENTS.....	77
TABLE 58: UC2 SCENARIO 3 5G COMPONENTS	77
TABLE 59: UC2 SCENARIO 3 OTHER COMPONENTS	77
TABLE 60: UC3 SCENARIO 1 SUB-SCENARIO 1 UAV COMPONENTS.....	78
TABLE 61: UC3 SCENARIO 1 SUB-SCENARIO 1 UAV OPERATOR COMPONENTS.....	78
TABLE 62: UC3 SCENARIO 1 SUB-SCENARIO 1 UTM COMPONENTS	79
TABLE 63: UC3 SCENARIO 1 SUB-SCENARIO 1 5G COMPONENTS	79
TABLE 64: UC3 SCENARIO 1 SUB-SCENARIO 1 OTHER COMPONENTS.....	79
TABLE 65: UC3 SCENARIO 1 SUB-SCENARIO 2 UAV COMPONENTS.....	80
TABLE 66: UC3 SCENARIO 1 SUB-SCENARIO 2 UAV OPERATOR COMPONENTS.....	81
TABLE 67: UC3 SCENARIO 1 SUB-SCENARIO 2 UTM COMPONENTS	81
TABLE 68: UC3 SCENARIO 1 SUB-SCENARIO 2 5G COMPONENTS	81
TABLE 69: UC3 SCENARIO 1 SUB-SCENARIO 2 OTHER COMPONENTS.....	81
TABLE 70: UC3 SCENARIO 1 SUB-SCENARIO 3 UAV COMPONENTS.....	82
TABLE 71: UC3 SCENARIO 1 SUB-SCENARIO 3 PARTNER/COMPONENTS	83
TABLE 72: UC3 SCENARIO 1 SUB-SCENARIO 3 PARTNER/COMPONENTS	83
TABLE 73: UC3 SCENARIO 1 SUB-SCENARIO 3 5G COMPONENTS	83
TABLE 74: UC3 SCENARIO 1 SUB-SCENARIO 3 OTHER COMPONENTS.....	83
TABLE 75: UC3 SCENARIO 3 UAV COMPONENTS	84
TABLE 76: UC3 SCENARIO 3 UAV OPERATOR COMPONENTS	85
TABLE 77: UC3 SCENARIO 3 5G COMPONENTS.....	85
TABLE 78: UC3 SCENARIO 3 OTHER COMPONENTS.....	85

List of Abbreviations

4G	Fourth Generation Cellular Telecommunications Network
5G	Fifth Generation Cellular Telecommunications Network
5GC	5G Core
5G NR	5G New Radio
API	Application Program Interface
CIS	Common Information System
CMP	Certificate Management Protocol
COTS	Commercial-of-the-shelf
DC	Data Centre
Dx.y	Deliverable No y of WPx
EASA	European Aviation Safety Agency
EMBB	Enhanced Mobile Broadband
EMS	Element Management System
eNB	Evolved Node B
EPC	Evolved Packet Core
FFD	Frequency Division Duplex
FLARM	Traffic awareness & collision avoidance system for General Aviation, aircrafts, and UAVs

FTTH	Fiber To The Home
GCS	Ground Control System
gNB	Next generation Node B
KIVU	The name of independent drone tracker from INVOLI
KPI	Key Performance Indicator
LoS	Line of Sight
LTE	Long Term Evolution
MANO	Management and Network Orchestration
MCT	Micro Control Tower (INVOLI's product)
MEC	Multi-access Edge Computing
MMTC	Machine-to-Machine Type Communication
NBI	North Bound Interface
NFV	Network Function Virtualization
NFVI	Network Function Virtualization Infrastructure
NFVO	Network Function Virtualization Orchestrator
NMS	Network Management System
NR	New Radio
NSA	Non-Standalone
NSI	Network Slice Instance
NST	Network Slice Template
OAI	Open Air Interface
OAM	Operation, Administration, and Maintenance
ODL	Open Day Light
OSM	Open Source MANO
PNF	Physical Network Functions
PoP	Point to Point
RAT	Radio Access Technology
RRU	Remote Radio Unit
SA	Standalone
SBI	South Bound Interface
SCTP	Stream Control Transmission Protocol

SDN	Software Defined Network
SO	Slice Orchestration
SUT	System Under Test
TDD	Time Division Duplex
UAS	Unmanned Aerial System
UAV	Unmanned Aerial Vehicle
UPF	User Plane Function
URLLC	Ultra-Reliable Low Latency Communication
USSP	U-Space Service Provider
VDU	Virtual Deployment Unit
VIM	Virtual Infrastructure Manager
VLAN	Virtual Local Area Network
VNF	Virtual Network Function
VNF-FG	VNF Forwarding Graph
WAN	Wireless Area Network
WIM	WAN Infrastructure Manager
WPx	Work Package x

1. INTRODUCTION

1.1. Objective of the document

The main objective of D1.5 is to further elaborate the supported features and prerequisites of the 5G test sites to trial 5G!Drones use cases. This deliverable extends the initial description of the 5G trial facilities in D1.2, to provide the complete description of the 5G trial facilities and their mapping to each respective use-case scenario. The 5G facilities of different partners contributing towards this project are the 5GENESIS Athens 5G site, the 5G-EVE Sophia Antipolis 5G site, Aalto university X-network, and the University of Oulu 5G Test Network (5GTN).

The 5G!Drones vertical use case features, defined and presented in deliverable D1.1, will be mapped to the respective facility 5G components. Along this line, each facility further elaborates and clearly declares its architecture, components, capacity and capabilities regarding the respective technical features at the radio, core network, edge computing, and security, with further mapping and reporting 5G specifics at Unmanned Aerial Vehicle (UAV) service component level, proper to each scenario.

Specifically, this deliverable reports the details and highlights on the related 5G components and enablers within each 5G facility focusing on all the prerequisites for a successful use case deployment and execution. Emphasis is given on the facility interaction with the corresponding trial controller for each related use case deployment while a detailed mapping of corresponding use case scenario components to each 5G test facility is presented.

In addition, the D1.5 further elaborates the UAV and 5G requirements of each use case, expressing a clear mapping among the facilities and the 5G!Drones use cases and their scenarios.

1.2. Structure of the document

This Deliverable is structured in eight chapters:

Chapter 1 presents an introduction of the Deliverable focusing on its objectives, structure and target audience.

Chapter 2 analyses the 5GENESIS facility, its 5G components and enablers, its interaction with the corresponding trial controller for each related use case deployment and how each related use case and scenario is mapped to the 5G trial facility.

Chapter 3 analyses the 5GEVE facility, its 5G components and enablers, its interaction with the corresponding trial controller for each related use case deployment and how each related use case and scenario is mapped to the 5G trial facility.

Chapter 4 analyses the X-NETWORK facility, its 5G components and enablers, its interaction with the corresponding trial controller for each related use case deployment and how each related use case and scenario is mapped to the 5G trial facility.

Chapter 5 analyses the 5GTN facility, its 5G components and enablers, its interaction with the corresponding trial controller for each related use case deployment and how each related use case and scenario is mapped to the 5G trial facility.

The conclusion, references and appendix are presented in Chapters 6, 7 and 8 respectively.

1.3. Target Audience

This project consortium deliverable is open to the general public, and targets the scientific/research community, as well as industry stockholders working on UAV and 5G. It aims to offer a better understanding of the framework and scope of the 5G!Drones project. It shows how different 5G trial facilities are aligned with the use case scenarios that were defined within the project. Furthermore, this

deliverable is also targeting the two communities in scope of the project namely 5G (5G PPP and beyond) & UAV.

2. 5GENESIS

2.1. Highlights of 5G components/ enablers within the facility for use case deployment

5GENESIS stands for “5th Generation End-to-end Network, Experimentation, System Integration, and Showcasing” and its main goal is validating 5G KPIs for various 5G use cases in both controlled setups and large-scale events¹. The project brings together results from a considerable number of EU projects as well as the partners’ internal R&D activities in order to realize an integrated End-to-end 5G Facility.

2.1.1. Architecture

5G!Drones has already defined in D1.3 [4] the high-level architecture that must be supported by 5G platforms so that to efficiently support large-scale UAV trials. This architecture, graphically depicted in Figure 1, can be deployed over pre-existing or new 5G testbeds, each of which needs to address the adaptations necessary in order to support it and become effectively a 5G!Drones platform. At the same time, 5GENESIS Athens platform is a mature all-encompassing 5G experimentation platform that has been validated as part of 5G-PPP Phase2 for execution of targeted 5G trials. As presented in D1.2 [3] 5GENESIS already implements an experimentation framework, as seen in Figure 2 that is specified in detail in 5GENESIS Deliverable 2.3 “Initial overall facility design and specifications” [5].

The primary observation is that the 5GENESIS architecture specifies exhaustively and in a top down manner all the components expected to exist in a testbed in three distinct layers, the (i) Coordination Layer, implementing the Experimentation Framework and interactions with the Experimenters, the (ii) Management & Orchestration (MANO) Layer that is in charge of the 5G Platform Orchestration & Monitoring and the (iii) Infrastructure Layer, containing the actual equipment (5G Core, Access, Transport Network and Data Centres & Cloud nodes). At the same time, the 5G!Drones architecture primarily focuses on the functions of -in 5GENESIS terms- Coordination layer and specifically the UAV experimentation, and considers some capabilities of the MANO Layer as necessary to collect and maintain key monitoring & measuring metrics for the subsequent KPIs validation. The internals of the Infrastructure Layer are left open and are not tightly coupled allowing for the flexibility of various 5G platforms to be interconnected through the proper adaptation.

¹ <https://5genesis.eu/>

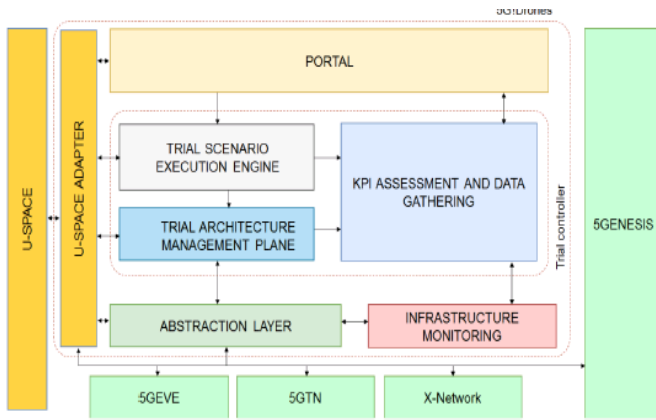


Figure 1 - 5G!Drones Architecture

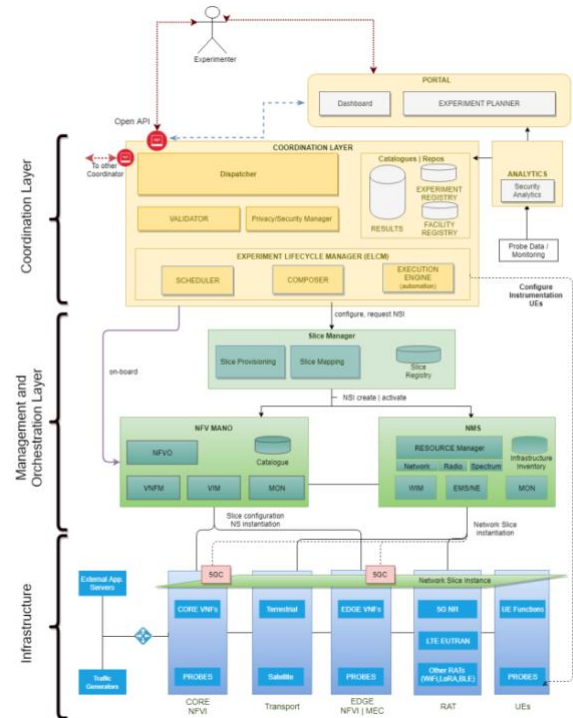


Figure 2 - 5GENESIS Architecture

For the realization of the 5G!Drones platform on top of 5GENESIS, a key challenge thus becomes to properly project both concepts in a common and revised 5G!DRONES-Enhanced 5GENESIS architecture, optimized for 5G-assisted UAV experiments that encapsulates and reuses the existing capabilities. An initial gap analysis has identified components that are similar in both architectures and the work has now evolved to a concrete architecture that is depicted below in Figure 3. The main updates will happen at the 5GENESIS Coordination Layer, whereas the MANO and Infrastructure Layer shall follow the platform's evolution plan. It is noteworthy that the vertical applications for UAV management (UAS systems) to be installed on the platform as well as the necessary interactions to involved 3rd parties (UTM systems) are considered in 5GENESIS terms as a part of the infrastructure layer and the proper placeholders to host and manage them at the edge are analysed in the relevant sections.

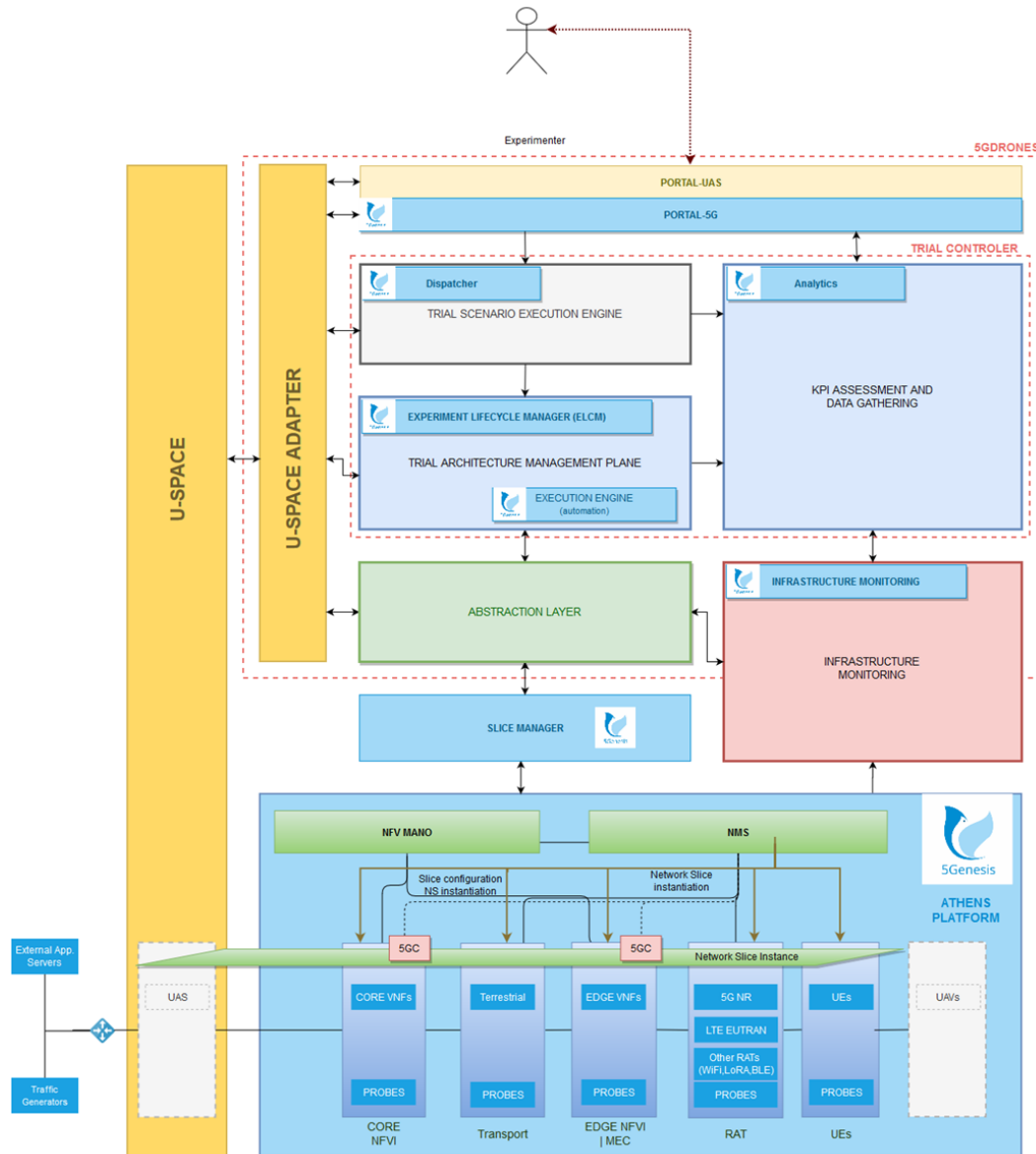


Figure 3 - 5G!Drones Enhanced 5GENESIS Architecture

This projection of the 5G!DRONES architecture to 5GENESIS has provided interesting insights on the initial gap analysis work in [4] that has been revised as depicted in Table 1 and will be considered in the implementation work packages (WP2, WP3) and the recommended action plan.

Table 1: 5GENESIS Revised Gap Analysis

5G!DRONES Component	5GENESIS Component	Evolution
Portal: UAS 5G	Portal-5G	The Portal-UAS is missing and needs to be incorporated The Portal-5G exists and will be reused and enhanced on the basis of WP2 work
U-Space Adapter	N/A	It shall be included as delivered by WP2 in 5GENESIS coordination layer as an optional component for UAV trials
Trial Scenario Execution Engine	Dispatcher	5GENESIS Dispatcher shall be enhanced to optionally interact with the U-Space Adapter for UAV trials
Trial Architecture Management Plane	ELCM (Experiment Life Cycle Manager)	5GENESIS ELCM, based on Keysight's Open TAP implementation ² , shall be enhanced with capabilities to execute through the U-Space Adapter experiments delegating executions to USPACE systems.
Abstraction Layer	Plugins	The 5GENESIS has the concept of Open TAP Plugins. Any UAV-specific extensions shall be developed following the same methodology
KPI Assessment & Data Gathering	Analytics, Influx DB, Grafana	The 5GENESIS components shall be extended as necessary to support new metric flows and statistical analysis methods.
Infrastructure Monitoring	Prometheus, Libre NMS, etc	5GENESIS MANO Layer has a plethora of monitoring tools, as necessary per case that shall be reused.
U-SPACE	N/A	Drones industry partners shall make sure that all appropriate systems (UAS/UTM) shall be made available and open for interaction with 5GENESIS ELCM component.

From the 5G Technology Architecture perspective, the Athens platform implements the 5G NSA (3GPP option 3) and has a roadmap of evolution towards SA as the technology matures. Also, as noted in [3] the 5GENESIS Athens platform is comprised of 3 main sites that are interconnected through high-speed transport networks (see 5.1.2.3):

- **The NCSR D campus:** It is considered the main data centre of the Athens platform, and hosts the Coordination Layer components –such as the portal towards the experimenters, the ELCM and Analytics modules. It also hosts the Mobile Core functions and especially the HSS (Home Subscriber Server) and MME (Mobility Management Entity) components for the proper users' authentication within the mobile network and mobility management. Also, within the NCSR D campus, edge computing capabilities through a private cloud infrastructure can serve over the mobile core network any application components on demand.
- **The COSMOTE campus:** It is a fully functional edge site that contains mobile network functions and in alignment with ETSI White Paper "MEC Deployments in 4G and Evolution Towards 5G" [6], implements LBO (Local break Out) and Distributed S/PGW (Serving/Packet Gateway)

² <https://about.keysight.com/en/newsroom/pr/2019/21may-nr19075.shtml?cc=GB&lc=eng>

functions. It also provides a private cloud infrastructure to appropriately host application components that need to be close to the mobile edge.

- **The Egaleo stadium:** It is the field of experimentation and provides the basic infrastructure for the deployment of the necessary equipment that are part of the use cases.

2.1.2. Network Infrastructure

2.1.2.1. Radio Access Network (RAN)

5GENESIS already contains a wide selection of 5G RAN equipment, including commercial solutions from Amarisoft - the 5G CallBox which supports both NSA and SA 5G Core and RAN deployment-, and from Nokia -the Airscale 5G Macro Cell- and beta releases provided by RunEL and Eurecom. The deployment already supports fully operational 4G LTE equipment. The RAN features are summarized in Table 2.

Table 2: RAN components of 5GENESIS Athens Platform

Component	Details
eNB (4G)	<ul style="list-style-type: none"> • 2 NOKIA “Flexi Zone Multiband Indoor Pico BTS” (FZ MBI) small cells (NCSR Site – IIT building) • 1 AmarisoftNB running on x86 server (SDR) (NCSR Site - administration building) • 1 AmarisoftNB (USRP B210) on x86 server (SDR) (NCSR Site – library building) • 1 AmarisoftNB (N210) for the Macro Cell at outdoor location (high mast) providing coverage to a large part of NCSR campus (NCSR Site) • Eurecom OAI in multiple instances & SDR HW (NCSR Site) • 8 NOKIA “Flexi Zone Multiband Indoor Pico BTS” (FZ MBI) small cells (Cosmote Site)
gNodeB (5G)	<ul style="list-style-type: none"> • 1 Amarisoft Callbox Classic 5G NSA (3.5 GHz, N78 Band) (NCSR Site) • 1 OAI gNB (USRP N310) and x86 server (prototype) – Laboratory / IIT building (NCSR Site) • NOKIA Airscale System and 5G Small Cell (RRH) (Cosmote Site)
UE	<ul style="list-style-type: none"> • Commercial 4G mobile phones compatible with OAI plus USB dongles • Commercial 5G mobile phones
Non-3GPP Access Networks	<ul style="list-style-type: none"> • WiFi 802.11ac

2.1.3. Computing infrastructure

2.1.3.1. Main Data Centre

The Main Data Centre (DC) of the Athens platform hosts all the Coordination Layer components, the Slice Manager and all the MANO Layer components. (i.e., NMS, EMS, NFVO, etc). Moreover, it is also hosting an NFV infrastructure (NFVI) that is orchestrated by the NFVO in order to instantiate network services and/or VNFs that relate to the test cases. For example, it is capable of hosting a 5GC instance or a proxy VNF.

Currently the Main DC comprises 3 compute nodes, operating with OpenStack release “Rocky” providing multiple tenants (OpenStack Projects) in order to respond to both roles of Virtual Infrastructure Manager (VIM) and for 5GENESIS software components deployment. Currently, it is deployed over three physical R630 DELL servers, with the plan to add more nodes if necessary, when resources are needed. The core OpenStack DC supports three provider flat layer-2 networks (i.e. no VLANs), which are directly connected to the rest of the platform.

In addition to the above infrastructure and in order to facilitate for Virtual Machines that have more stringent requirements (i.e. Windows based) two VMware ESXi nodes are provided also. These nodes are running Ixia IxChariot traffic generation instances and Prometheus infrastructure monitoring instances.

Finally, to support redundancy and allow for isolated execution a Main DC infrastructure is also deployed in COSMOTE for additional deployment of Coordination and MANO Layer components.

2.1.3.2. Edge Data Centre

The Athens Platform integrates edge computing infrastructure in various locations within its topology. The existing infrastructure can be later upgraded to a complete MEC infrastructure for deployment of edge applications and Network Service components. In order to achieve that, traffic that would normally reach the services sitting behind the 4G/5G core utilizing the backhaul connection can now be steered locally and either reach services instantiated at the edge or reach through the internet using local connections. There is a need to deploy a 5GC function locally at the edge. This function is named User Plane Function (UPF) and provides this kind of functionality. For 4G and 5G NSA deployments there are solutions that can achieve similar behaviour as seen in [6]. The capability of allowing edge computing and traffic routing locally greatly benefits latency sensitive services. In addition, it allows for better scaling of backhaul connections and cost reductions.

The sites of NCSR and COSMOTE stand primarily as permanent edge sites of the Athens Platform. In NCSR there are two types of edge computing infrastructures that are deployed: (i) an all-in-one installation of OpenStack small form factor (SFF) x86 PCs and (ii) K8s based Docker orchestration infrastructure.

In COSMOTE site the edge cloud is implemented using OpenStack Rocky installation over x86 workstation equipment. An edge cloud domain is also activated in the Egaleo campus, supported by an all-in-one OpenStack NUC based nodes. The edge nodes are installed in the permanent cabinets that are installed at the Egaleo stadium for this purpose. Three cabinets are available to host the gNB components as well as the edge computing infrastructure to support the 5GENESIS activities.

2.1.4. Orchestration and management

Table 3 provides an overview of the Management and Orchestration layer components and associated technologies deployed in the Athens platform.

Table 3: 5GENESIS Athens platform MANO components

Component	Product/Technology	Mode of Implementation
NFVO	Open Source MANO	Release 6 and 7
WIM	Custom open-source implementation, operate over SDN based WANs.	Python Dockerized application
SDN Controller	OpenDayLight	Fluorine release
NMS	LibreNMS	Rel. 1.59
Amarisoft EMS	Custom open-source implementation of Amarisoft eNB/gNB configuration and management	Ansible / python scripts used to set the configuration according to the slice
EPC/5GC EMS	Athonet EMS	SNMP based / Open API
Monitoring	Prometheus/Grafana/InfluxDB	Time series based monitoring, alerting and visualisation

Starting from the top, the NFV Orchestrator in the Athens platform is OSM release 6 and 7. OSM is one of the most popular open-source platforms for NFV orchestration, and, being developed under the ETSI umbrella, is also aligned with the ETSI NFV specifications.

In order to enable the creation of network slices, the 5GENESIS Slice Manager depends on the network management system (NMS) to provision resources, control the network and establish the appropriate paths within the WAN topology. The 5GENESIS NMS system comprises of the following components:

- WAN Infrastructure Manager (WIM), a component that has the overview of the Wide Area Network (WAN), the physical network that is used to provide connectivity to any physical and virtual component of the Platform. It keeps track on the way that all networking devices (SDN switches, routers), NFV Infrastructures and physical devices on the platform are connected, in the form of a network graph. The WAN implementation depends on the existence of an SDN capable WAN infrastructure. Current WIM version support ODL Fluorine API in order to manage the network infrastructure.
- Most Mobile Network elements deployed in the platform provide proprietary solutions that allow operations like configuration and monitoring for the respective devices. These systems are exploited to perform configuration management and retrieve status information per case. In the case of the Athens platform, EMS specifically build for use with OAI and Amarisoft solutions are developed and used. These EMS allow proper configuration and resource provisioning for the mobile network.
- The Platform has integrated network control based on OpenDayLight SDN Controller. The ODL controller is one of the most broadly used and integrates well with OpenStack environments. The version currently integrated in the Athens platform is “Fluorine” which enhances the support for network virtualization within cloud and edge computing environments. This includes improved IPv6 support, support for both stateful and stateless security groups, and SR-IOV hardware offload for OVS. Much of this work has been developed for OpenStack environments, and is now being leveraged to integrate ODL with the Container Orchestration Engine for Kubernetes environments.
- LibreNMS is used to measure state, health, configuration (Ports, VLANs, Neighbours, STP, Inventory and Logs) and performance (throughput, traffic, latency, loss) on networking devices

(Switches, Routers, etc.). It supports SNMP protocol and allows topology and infrastructure discovery for all network elements that support this protocol.

Prometheus servers deployed in hierarchical mode are collecting aggregated time series data from a larger number of subordinated servers and can be used to take measurements from any device on the platform by creating custom exporters that use the SNMP protocol. The visualization is taken care by Grafana which supports a scripted way of producing intuitive dashboard for presenting time series data and monitoring information

2.1.4.1. Network Slicing

The Slice Manager is the component that mediates between the Coordination layer components of the 5GENESIS architecture and the MANO layer. The 5GENESIS Slice Manager is responsible for the lifecycle of network slices, i.e. it manages the creation and provision of network slices over the infrastructure. The Slice Manager provides an API in order to communicate with the Coordination Layer and receive requests for network slices in the form of Generic Slice Template (GST). The GST is mapped to the Network Slice Template (NEST) by filling in the technical specification of the GST according to the slice requirements.

The 5GENESIS Slice Manager is a custom-made open source application named “Katana”³. It is based on a highly modular architecture, built as a mesh of micro-services, each of which is running on a Docker container. The NBI API module that creates the RESTful APIs is implemented with the use of Python and the Flask framework. Moreover, a swagger tool that visualizes the API Specification definitions in an interactive UI has been created for documentation purposes. Finally, an adaptation layer module provides a level of abstraction regarding the underlying layer technology, making it feasible for the Slice Manager to operate over any MANO layer component without any modifications to its core functionality, as long as the proper plugin has been loaded.

2.1.4.2. KPI

The list of KPIs supported by the 5GENESIS Athens platform are presented in Table 4. More KPIs might be added in the future releases of the 5GENESIS facility.

Table 4: 5GENESIS Athens Supported KPIs

KPI	Details	achieved values
Latency	The time it takes to transfer a given piece of information from a source to a destination, from the moment it is transmitted by the source to the moment it is received at the destination (in this link direction only) over the SUT.	15 ms*
Round-Trip-Time	Time it takes to transfer a given piece of data between two nodes, to process the piece of data at the receiving node, and to transfer an acknowledgement status back to the transmitting node, measured from the moment the piece of data is transmitted to the moment the acknowledgement status is received.	30 ms
Service Creation Time	The time required for the provision, deployment, configuration, and activation of a full E2Ecommunication service over a	60-70 sec**

³ https://github.com/5genesis/katana-slice_manager

	network slice, including all the physical and virtual components that are entailed in the Communication Service descriptors.	
Throughput	data (payload) successfully transferred within a given time period from a data source to a data sink	370 Mbps***

* The observed latency is mainly due to the NSA mode and that we only have eMBB support in the current implementation of 5GC. An estimated one-way latency value is about $RTT/2$ but certainly URLLC levels can't be reached at this stage without SA 5G deployment (where one-way measurement would make sense).

** Service Deployment time for 5GCore deployment at the edge + one NS comprising one VNF

*** Further advances are still ongoing in order to enhance the performance

2.1.5. Coordination Layer

The capabilities at the network, infrastructure and management level including the orchestration provided by the Slice manager are the building blocks for the dynamic provisioning of resources envisaged in the 5G era. On top of this, the 5GENESIS Athens platform addresses the capability to interact efficiently with the “verticals”; the clients of these services, through user-oriented coordination components that collect the end experimenter requirements and translate them to artefacts that can be effectively implemented through the Slice Manager through the underlying management systems on the available infrastructure components.

The fundamental components of the coordination capability of the Athens platform are summarized in Table 5.

Table 5: 5GENESIS Coordination Layer Components

Component	Details
5GENESIS Portal	Experimenter access portal, a graphical user interface to the experimenter, facilitating configuration and monitoring of experiments, as well as access to their results
Experiment Life Cycle Management	Lifecycle Management of the experiment exploiting Keysight's OpenTAP open-source testing automation tool, which interfaces southbound with the underlying element and network management components of the MANO layer as well as the Slice Manager.
Results Repository	InfluxDB is the open-source storage engine provided within the InfluxData framework and handles in particular time series data and is used to store all monitoring events and metrics that are necessary for the generation of the end-reports and KPIs validation.
Analytics	Custom Python scripts are developed to support the statistical analysis requirements for results presentation and KPI validation. The scripts are utilizing the native Influx DB capabilities to support Python.

2.1.6. Security features in 5GENESIS

5GENESIS is an infrastructure project focusing on providing a unified experimentation framework over End-to-end 5G facilities. As such, the project adopts security features addressing both the security of the deployed infrastructure, as well as the security and privacy of the experimenters accessing its facilities. Each platform shall provide the means for authentication and authorization of experimenters in the form of security functions for user authentication and access control.

In addition, 5GENESIS includes an Anomaly Detection Framework⁴, currently allowing the detection of anomalies, which may correspond to either malfunctions or security incidents. The framework uses the Data Analysis and Remediation Engine (DARE) developed in the SHIELD project⁵ and leverages Big Data technologies based on Apache Spot, Hadoop Distributed Filesystem (HDFS), Kafka and Spark. It consists of a main data analytics engine and distributed data collection components, implementing Data acquisition, transformation and storage, Data analysis, as well as visualization and export.

Finally, the Katana Slice Manager⁶ is under development in the context of 5GENESIS and is used for deploying services across multiple network domains (Edge, Core, RAN, etc.), while managing the resources reservations. During Phase 3 of the project, the Katana Slice Manager will be integrated with ERICSSON's APEX Policy Engine⁷ and will leverage the 5GENESIS "Analytics and Monitoring Framework"⁸, in order to apply security related mitigation policies across the infrastructure.

The APEX Adaptive Policy EXecution system is capable of defining, deploying and executing simple or even adaptive policies, based on the current network conditions and relevant business goals. The APEX Policy Engine is triggered by incoming events and generates response actions, according to the policy's defined logic. In APEX, the user can define the state information and data used by the policies, defined as the policy's Context. APEX provides many deployment options and can be included in applications as a Java library, as a micro service in Docker containers or as standalone service⁹.

2.2. Facility interaction with the trial controller for use case deployment

2.2.1. Deployment of a Trial

One of the major goals of 5GENESIS is to offer a common way for experimenters and 5G verticals to interface with the facility. The 5GENESIS open API is the interface offered by the coordination layer to experimenters for the definition and execution of the experiments. In addition to that, 5GENESIS also provides them with a Portal with a friendly Web Interface to facilitate their task even more. The Portal itself uses the 5GENESIS open API to communicate with the coordination layer component. Therefore, there are two ways in which the experimenters can interact with the 5GENESIS facility, (i) via the Portal and/or (ii) using the open API directly in the case of more advanced users of the Platform or experienced verticals.

Experimenters can define trials/experiments to generate KPIs and obtain results of the execution. For that purpose, they can configure several parameters of the trial, such as the test cases to perform, one or more Network Slices for the deployment of the trial and custom Network Services (previously uploaded) to deploy. Afterwards, all the logs captured during the different parts of the execution can be retrieved and reviewed.

2.2.1.1. Web Portal

In addition to the option of using the open API in a direct way, the 5GENESIS Portal provides a user-friendly web interface for experimenters to interact with the 5GENESIS facility. Users can define new experiments, examine the results and logs of previous executions or manage deployed VNFs among other features. Furthermore, experimenters can view information about their latest performed actions and access to system information. Figure 5 shows the home page of the 5GENESIS web portal.

⁴ https://5genesis.eu/wp-content/uploads/2019/10/5GENESIS_D3.13_v1.0.pdf

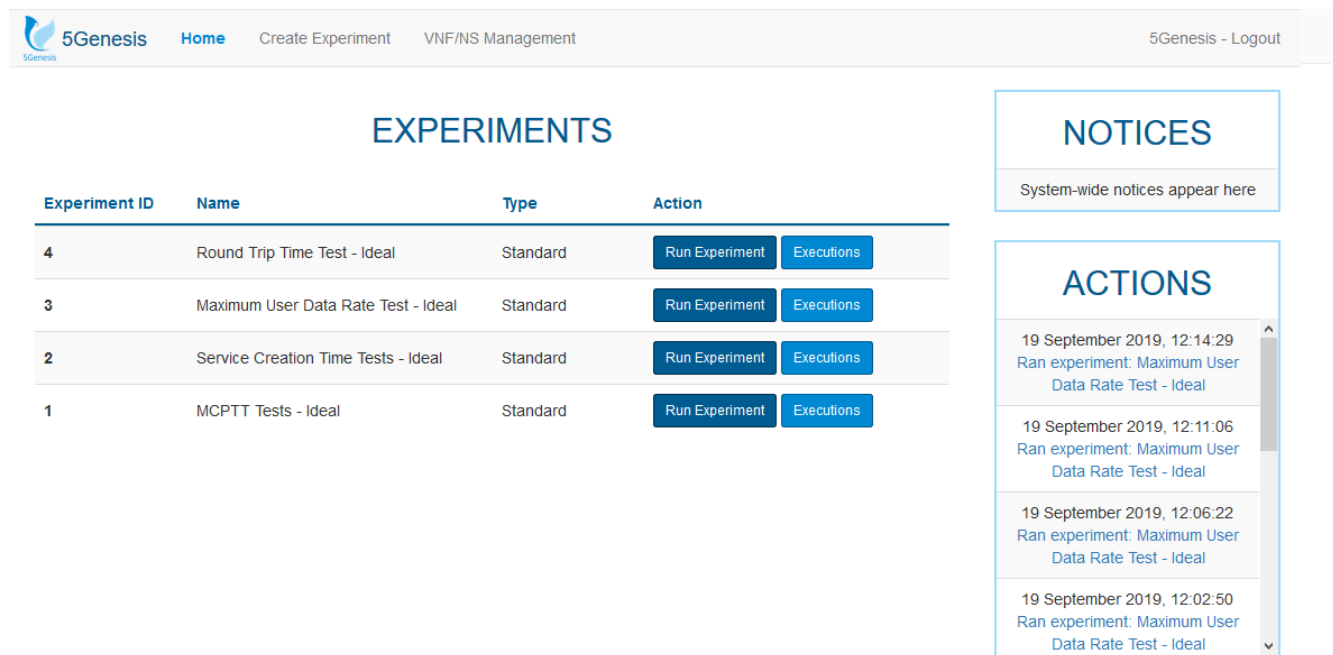
⁵ SHIELD project, <https://www.shield-h2020.eu/>

⁶ Katana Slice Manager, https://github.com/medianetlab/katana-slice_manager

⁷ APEX Policy Engine, <https://docs.onap.org/en/dublin/submodules/policy/apex-pdp.git/docs/APEX-Introduction.html>

⁸ 5GENESIS Monitoring and Analytics (Release A), Deliverable D3.5 https://5genesis.eu/wp-content/uploads/2019/10/5GENESIS_D3.5_v1.0.pdf

⁹ S. van der Meer, J. Keeney, L. Fallon and J. McNamara, "Demo: Adaptive policy execution (APEX)," *NOMS 2018 - 2018 IEEE/IFIP Network Operations and Management Symposium*, Taipei, 2018, pp. 1-2, doi: 10.1109/NOMS.2018.8406117.



The screenshot shows the 5Genesis web portal interface. At the top, there is a navigation bar with the 5Genesis logo, a 'Home' link, and links for 'Create Experiment' and 'VNF/NS Management'. The user is logged in as '5Genesis - Logout'. The main section is titled 'EXPERIMENTS' and contains a table with the following data:

Experiment ID	Name	Type	Action
4	Round Trip Time Test - Ideal	Standard	Run Experiment Executions
3	Maximum User Data Rate Test - Ideal	Standard	Run Experiment Executions
2	Service Creation Time Tests - Ideal	Standard	Run Experiment Executions
1	MCPTT Tests - Ideal	Standard	Run Experiment Executions

On the right side, there is a 'NOTICES' section with the text 'System-wide notices appear here'. Below it is an 'ACTIONS' section showing a list of recent actions:

- 19 September 2019, 12:14:29
Ran experiment: Maximum User Data Rate Test - Ideal
- 19 September 2019, 12:11:06
Ran experiment: Maximum User Data Rate Test - Ideal
- 19 September 2019, 12:06:22
Ran experiment: Maximum User Data Rate Test - Ideal
- 19 September 2019, 12:02:50
Ran experiment: Maximum User Data Rate Test - Ideal

Figure 5 - 5GENESIS web portal

2.2.1.2. Northbound API (NBI)

The main priority of the open API architecture is to define the interface that can be easily consumed and accessed by the experimenter's client. The result offers protocols and custom data format to facilitate the interaction with the 5GENESIS system. Table 6 shows the list of NBI allowing to manage the life cycle of a trial running on top of 5GENESIS.

Table 6: 5GENESIS open APIs

API	Methods	Details
/dispatcher/vnfd	POST	On boards a VNFD package in the NFVO VNFD catalogue
/dispatcher/image/{vim_type}	POST	Uploads an image file in the VIM
/dispatcher/vnfd	GET	Retrieve all VNFDs in the catalogue
/dispatcher/vnfd/{vnfd_id}	DELETE	Delete an existing VFND from the NFVO VNFD catalogue specified by its vnfd_id
/dispatcher/nsd	POST	On boards a NSD package in the NFVO NSD catalogue
/dispatcher/nsd	GET	Retrieve all NSDs in the catalogue
/dispatcher/nsd/{nsd_id}	GET	Retrieve a single full NSD from the NFVO NFV catalogue
/dispatcher/nsd/{nsd_id}	DELETE	Delete an existing NSD from the NFVO NFV catalogue specified by its nsd_id

/dispatcher/experiment	POST	Launch the execution of an experiment and run the tests included in the query
/dispatcher/executions	GET	Retrieve current experiment executions
/dispatcher/execution/{id}	GET	Retrieve the status of a specific experiment execution
/dispatcher/experiment/{id}	GET	Retrieve the experiment descriptor of an experiment
/dispatcher/execution/{id}	DELETE	Stop an experiment execution, keeping the data for the history
/dispatcher/execution/{id}/logs	GET	Retrieve the logs generated by a given experiment execution
/dispatcher/experiment/history	GET	Retrieve the list of experiment executions registered for a given experiment id
/dispatcher/analytics/{exp_id}	GET	Retrieve the list of KPIs generated by a given experiment execution
/dispatcher/report/{exp_id}	GET	Retrieves the generated PDF report of a given experiment execution

2.3. Detailed mapping to the facility of UC4 scenario 1 - Connectivity extension & offloading during crowded events

The purpose of this scenario is to demonstrate how UAVs through 5G network capabilities can improve connectivity services in a highly crowded environment e.g. during large events. The concept relies on providing end-to-end dedicated and reliable communication targeting specific user groups such as the event organizers to supervise and manage large events in an unhindered manner. At the same time, and with the proper dimensioning of the deployed solution in terms of capacity, the connectivity services can also be offered to the spectators.

In Figure 6, the Egaleo stadium is shown along with the deployed infrastructure and the necessary components that will be utilized in Use Case 4 – scenario 1 (UC4SC1). These components that will also be described in the next section, are comprised of the 5G system, the UAS deployed in the Edge cloud, the UTM deployed off-site, the Streaming server deployed in a private cloud and two drones, one for patrolling and one for infrastructure.

Note that the *Edge Cloud* refers to the data centre infrastructure at the stadium that also hosts the radio access network, and the *Core Network Cloud* refers to the Mobile Core and the main data centre of the 5GENESIS platform that is located at the NCSR/Demokritos premises. The *Private Cloud*, simulating the operational centre of the event planners, hosts the service components that relate central operations and the demo execution with some performance guarantees, and the role can be assumed from the COSMOTE's cloud site. Finally, the demo is supported by centralized UTM services offered over the public network.

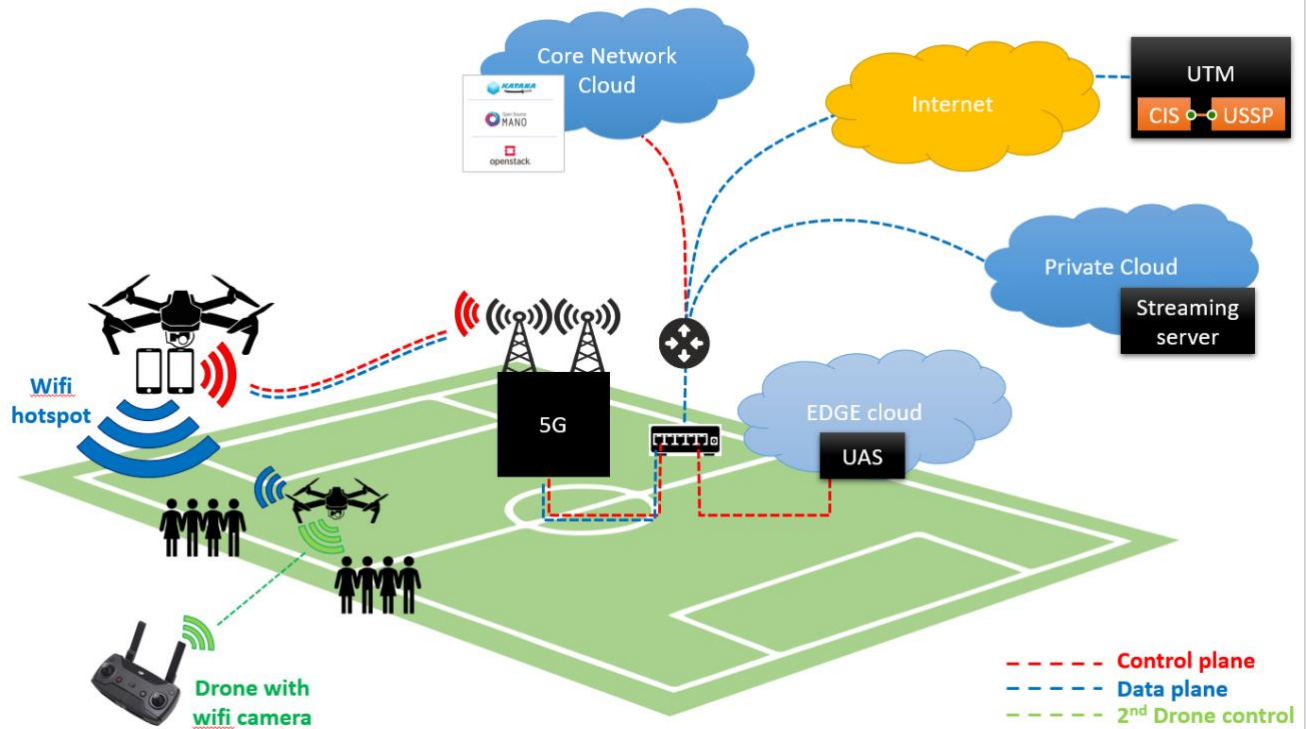


Figure 6 - Use Case 4 - Scenario 1 Components

2.3.1.1. Components

Figure 7 depicts the functional components and their mapping to the 5GENESIS facility focusing on the network connectivity. The Facility hard components enable 5G connectivity via the NSA mode and the UEs are connected through radio access. The rest of the components are deployed in different sites

and are connected via internet or dedicated links.

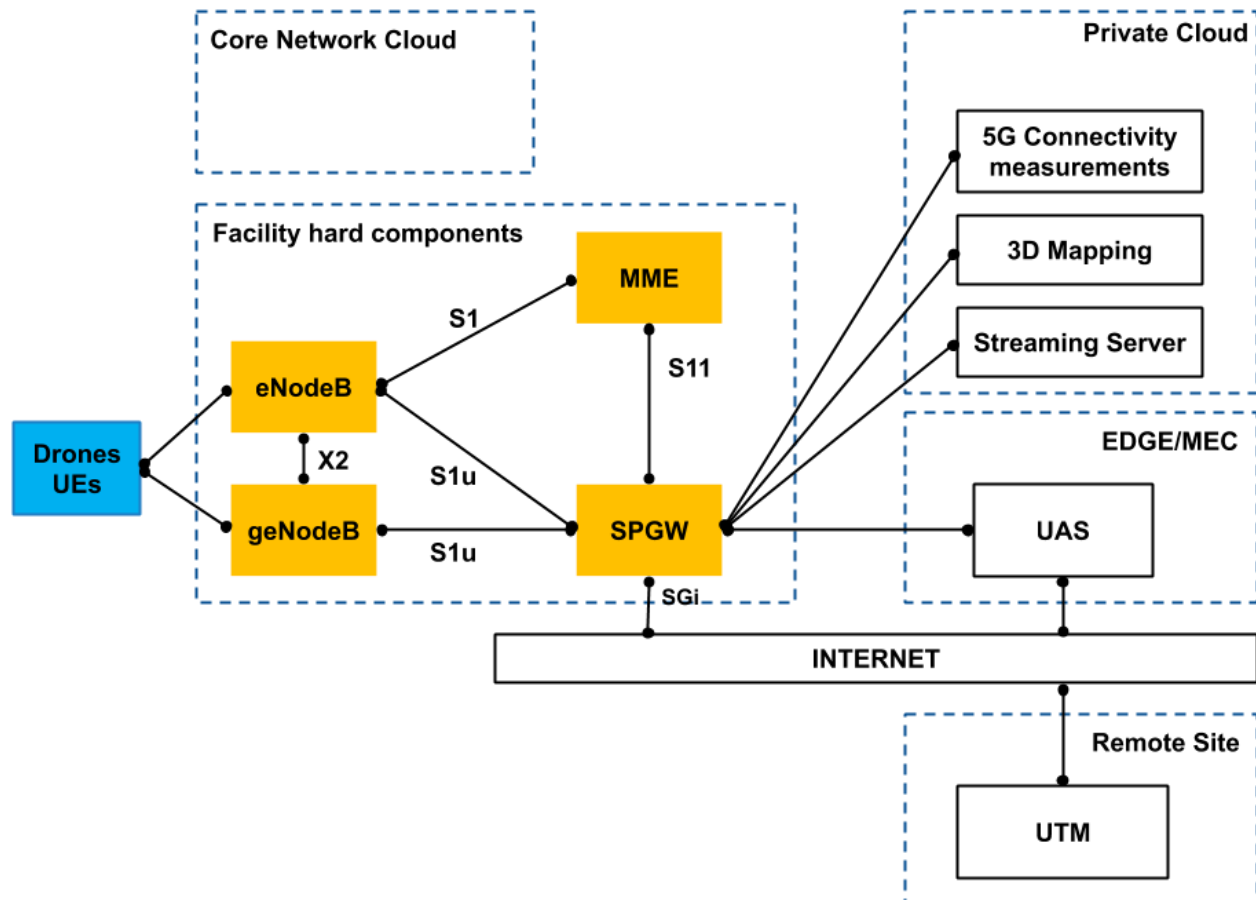


Figure 7 - UC4 scenario 1- Functional components and their mapping to the facility

2.3.1.1.1. Patrolling Drone

Before the event, a patrolling drone flies over the stadium, taking photos that are sent to a Private cloud, where 3D Mapping software processes a 3D map of them.

During the event, patrolling drone uses Android 5G device which runs 5G network QoS measurement application -CAFA Capture or Nemo Handy. CAFA Capture or Nemo Handy sends radio network quality data with x,y,z coordinates to MEC/Edge based CAFA 3D QoS Mapping software - CAFA Analyzer. Then results– in near real time network quality in 3D map will be shown, on CAFA Analyzer, to command centre - Connectivity Service Provider.

Same time patrolling drone same 5G device sends a video feed to CAFA VideoLyzer (video analytics software) and Video Streamer (streaming) software, which both applications run in the Private cloud. VideoAnalyzer detects automatically estimated number of people in the stadium, which allows to improve 5G connectivity. Both applications- VideoLyzer and VideoStreamer will be shown to command centre. The command centre can decide to change 5G base station directions or send one drone to provide additional 5G connectivity (Infrastructure drone).

2.3.1.1.2. Infrastructure Drone

This drone will be carrying two lightweight 5G UEs. The first one will be used for control plane and will be connected via 5G to the UAS. The second UE will provide connectivity to the users by creating a

Wi-Fi hotspot and will be used for data plane as it will utilize the 5G technologies as a backhaul between the Wi-Fi hotspot and the gNB.

2.3.1.1.3. 5G System

The 5G System refers to the Access Network and the Cells deployed at the stadium as well as the Core network side and data centre facilities that are hosted at Demokritos/NCSRD and offer the 5G network as well as the 5G!Drones trial execution components. Various deployments are scheduled as part of the use case trials as the 5G technology of the 5GENEIS platform evolves. In the first phase the 5G system is realized by the AmariCallboxClassic proprietary mobile network solution developed by Amarisoft. The NR implementation is based on 5G NSA option 3/3x/3a, following the 3GPP specification Release 15. Amarisoft RAN interacts with the Core Network through the standard S1 and S1-U interfaces, as shown in Figure 7. All Core and RAN functions are software defined, hosted inside an x86 node running Fedora 30 OS. The access network operates SDR boards connected through PCIe as RF front-end. The configuration enables two separate radio cells, one typical LTE (freq. band 1) and one 5G (freq. band n78). The LTE cell is utilized for signalling, authentication and control messages, whereas the actual user data traffic is transmitted through the NR cell. The NR cell operates on TDD transmission with supported bandwidth configurations that varies between 5 to 50 MHz and MIMO options for up to 4x4. Supported modulation schemes range up to 256QAM for Downlink transmission channel and 64 QAM for Uplink. Data subcarrier spacing can be modified between 15 kHz to 120 kHz. Currently, the UE solution utilized is the Samsung A90 mobile phone, compatible with n78 and n41 NR frequency bands.

2.3.1.1.4. UAS Systems

This scenario will make use of two UAS – the Unmanned Life Central Command Platform (UL-CCP) and the CAFA uGCS Platform (CUP) which will be deployed on the Edge.

Unmanned Life Central Command Platform (UL-CCP):

The UL-CCP will control and manage both the Matrice M600 and the Hepta's customized tethered drone (HTR-10) while the CUP will control and manage the DJI Mavic Pro.

As depicted in Figure 8, the UL-CCP, hosted at the edge, communicates with UAVs augmented by the Unmanned Life Autonomous Control Endpoint (UL-ACE). The UL-ACE is a single-board computer that will be mounted on the UAVs in order to provide network connectivity and integration with Unmanned Life platform. The UL-ACE is connected to the UAVs via a serial connection, and connected to the 5G network via any compatible adapter (in this scenario, via the USB Tethering functionality of a 5G-compatible smartphone).

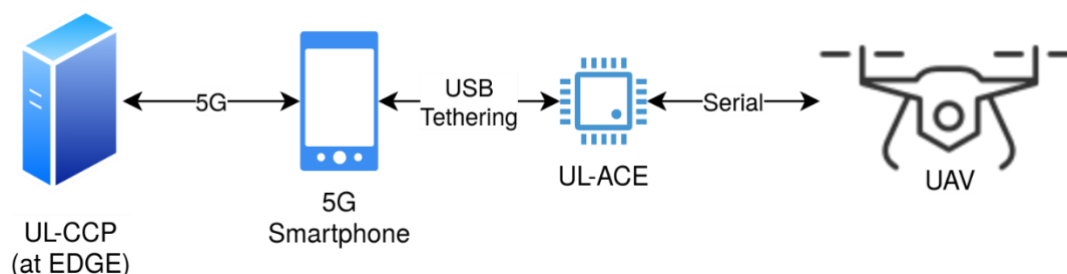


Figure 8 - UAV Connection to UL-CCP

CAFA UGCS based Platform (CUP):

CUP is a software for commanding and controlling UAV flights. CUP is hosted at the MEC/Edge and working process consists of the following steps:

1. Drone operator log in to CUP software and create drone flight mission. For example:
Mission 1: Capturing photos for 3D map;
Mission 2: Measuring 5G network QoS data and provide video-feed from site.
2. CUP sends flight mission details to 5G smartphone which is attached to remote controller.
3. Remote controller sends flight mission details to drone.
4. Drone starts mission and sends real time telemetry information to remote controller which send this data to 5G smartphone, which sends this data to 5G MEC/Edge. Operator monitor drone flights as he/she logged in CAFA CUP.
5. 5G smartphone which one is attached to Mavic drone runs different applications during the mission which depends on the goal:
When measuring 5G QoS the on-board 5G smartphone runs for example Nemo Handy app or CAFA positioning app Capture.

If during the flight is need to add some points of interests then operator uses Click and Go function in CAFA CUP.

2.3.1.1.5. 3D Mapping

3D Mapping software:

When a drone runs a mapping mission then the drone flight is planned by mapping software. Mapping mission includes:

- number of photos and overlapping;
- area to be mapped;
- Altitude for mapping etc.

For processing drone photos to 3D map Agisoft or other relevant software will be used. 3D Mapping software needs normally 512GB RAM for processing 100 photos to pointcloud in 20 minutes.

CAFA 3D map:

When pointcloud is processed then CAFA 3D map visualizes this pointcloud with georeferencing to map. CAFA 3D map works in Chrome browser and shows:

- 5G network QoS
- Drones on air
- Important activities which detected by CAFA VideoLyzer
- Video camera live-feed

The 3D Mapping software and CAFA 3D map will be deployed in the private cloud provided by Cosmote, which is capable of handling such workloads.

2.3.1.1.6. CAFA Capture and CAFA Analyzer

During the flight, 5G smartphone is attached to the patrolling drone. The Nemo Handy application or CAFA Capture logges radio network quality with x,y,z coordinates and sends these data to MEC/Edge based CAFA 3D QoS mapping software - CAFA Analyzer. CAFA Analyzer stores network measurement data to the database and visualizes the results in 3D map. CAFA Analyzer also provides situational

awareness regarding 5G QoS to command centre - Connectivity Service Provider. Together with the other software from CAFA Tech, this will also be installed in the private cloud.

2.3.1.1.7. Streaming Server

The following pieces of software are utilized for the video streaming service and will be installed in the Private cloud provided by Cosmote before the trials:

- 3D Mapping software for processing a 3D map of the drone photos,
- CAFA VideoLyzer (video analytics software) and
- CAFA Video Streamer (streaming) software

Private cloud has high bandwidth (minimum 300Mbps) connection both for incoming and out coming data.

CAFA Video Streamer software:

Patrolling drone carries on-board attached 5G smartphone which camera is directed to ground. In 5G smartphone runs video camera streaming application (Larix Broadcaster or other relevant application). This application sends video feed in RTSP or other format continuously to the Private Cloud. In Private Cloud is installed CAFA Video Streamer software which streams drone video for multiple users. Private Cloud based CAFA Video streamer is necessary because if end users directly have access to the 5G smartphone video then this smartphone cannot serve multiple viewers at once.

CAFA VideoLyzer video analytics software:

At same time when patrolling drone sends 5G video feed to CAFA Streamer, the Video Streamer stream video to CAFA VideoLyzer (video analytics software) which runs in the Private cloud.

CAFA VideoLyzer is software where are a lot of samples and rules and trained neural network for to identify matches with samples and rules and objects visible on the video.

CAFA VideoLyzer needs high performance computer and GPU (for example HPE Proliant server and Nvidia Tesla V100 GPU).

VideoLyzer detects automatically estimated number of people in the stadium and add estimated locations (coordinates) and sends this data to CAFA 3D map. Command centre users see detected activities on CAFA 3D map which allows to command centre to decide where is need to improve 5G connectivity.

2.3.1.1.8. UTM

The UTM system, which will be provided by DroneRadar will be installed in public cloud. System will be accessible via pre-defined end-points. It will be instance, which would simulate real USSP. It will be possible to define LAU in the system for the purpose of the use case covering the area of the experiment location. System will provide following services:

- Analysis and acceptance of the flight plan – it will issue flight approval based on the approval obtained “off-line” by drone’s operators
- Telemetry link to UTM with on-line, real time link

Frequentis will complement the UTM system providing a CIS integrated with DroneRadar’s system. Frequentis components will be hosted in FRQ cloud, and be accessible using public internet connection.

CIS will ensure information sharing amongst relevant aviation and mobile network stakeholders, including safety relevant data related to mobile networks (to the extend available). If necessary, Frequentis can provide USSP components as well.

Combined DroneRadar and Frequentis components will provide a system proving that validation results have been achieved in a full-scale U-space setup, in line with proposed regulation EASA.

2.3.1.1.9. Components Mapping

In the following section, a complete list of all the components that will be used are recorded in different types of tables. Table 7 has a short, general listing of the partners involved in UC4 scenario 1 and the components they contribute whereas the more detailed tables follow:

Table 7: UC4 scenario 1 partner/components

Component	Partner
5G connectivity and MEC	NCSR “Demokritos” & COSMOTE (5GENESIS)
Drone with 4G/5G connectivity	CAFA Tech, Hepta
C2 Link service	CAFA Tech, Unmanned Systems
UTM platform & interfaces	Frequentis & DroneRadar
Airboss service & Trial Script	Robot Experts

Table 8 lists the UAV hardware components. In particular, there will be 3 different types of Drones with different characteristics and capabilities, provided by Hepta and CAFA Tech.

Table 8: UC4 scenario 1 UAV components

UAV Components	Type (Hw/Sw)	Partner
DJI M600	Hw	HEP
Hepta tethering drone	Hw	HEP
DJI Mavic	Hw	CAF

Table 9 lists the UAV software components: two UAS systems for Command & Control of the drones and software for 3D mapping and network measuring.

Table 9: UC4 scenario 1 UAV Operator Components

UAV Operator Components	Type (Hw/Sw)	Partner
UAS system for Hepta drone	Sw	UMS
UAS system for DJI Mavic	Sw	CAF

Table 10 displays the two UTM systems that will be provided by Frequentis and DroneRadar.

Table 10: UC4 scenario 1 UTM Components

UTM Components	Type (Hw/Sw)	Partner
UTM Platform & interfaces	SW	FRQ
UTM Platform & interfaces	SW	DRR

Table 11 lists hardware and software that will be provided by the 5GENESIS partners.

Table 11: UC4 scenario 1 5G Components

5G Components	Type (Hw/Sw)	Partner
EDGE equipment (Intel NUC devices with OpenStack, Open Source MANO)	Hw & Sw	NCSRD
5G RAN (AMARISOFT)	Sw	NCSRD
Samsung A90	Hw	NCSRD and CAF
5G Nokia NSA NR	Sw	COS
Xiaomi mimix 5G phone	WH	COS

Table 12 lists some additional components that will be used during the execution of the scenario.

Table 12: UC4 scenario 1 other Components

Other Components	Short description	Type (Hw/Sw)	Partner
Airboss service, and Trial Script	Responsible for ground and air coordination, following the safety precautions, pre-flight checks, and regulatory measures.	Sw	REX
CAFA 3D Analyzer	3D Analyzer shows 5G QoS measurement results. Works in MEC/Edge	Sw	CAF
5G QoS measuring software	Android application which sends data from smartphone to MEC/Edge	Sw	CAF
Private cloud	HPE Proliant server, NVidia Tesla V100 32GB GPU, OpenStack, Ubuntu operating system	Hw & Sw	COS
3D mapping software	Works in Private cloud. Processing 3D map from drone photos	Sw	CAF

CAFA VideoLyzer	Works in Private cloud	Sw	CAF
CAFA VideoStreamer	Works in Private cloud- to stream video feeds to users	Sw	CAF
UTM	Impact of newly created service/infrastructure on the co-existing conditions of the current telecommunications network. Determining the conditions necessary to ensure an adequate level of services in the event of emergencies and the possibility of rapid reconfiguration for unmanned traffic.	SW	DRR

3. 5GEVE

3.1. Highlights of 5G components/enablers within the facility for use case deployment

5GEVE-SA (Sophia-Antipolis) is the trial site belonging to the ICT-17 5GEVE project. It is one of the fourth sites, where 5G!Drones trials will be conducted. It is located in Sophia Antipolis area, south east of France.

3.1.1. Architecture

Figure 9 illustrates the 5GEVE-SA architecture and its components. To run a trial, 5GEVE-SA provides a Web Portal that allows a vertical to describe its trial, upload the NSD and its set of VNFs or Application Descriptor (AppD) to deploy on top of MEC or Cloud. Note that, the equivalent of the portal functions is available via a Northbound API (NBI), connecting directly to the Slice Orchestrator (SO) of the facility. The latter is in charge of deploying an end-to-end Network Slice to run the trial.

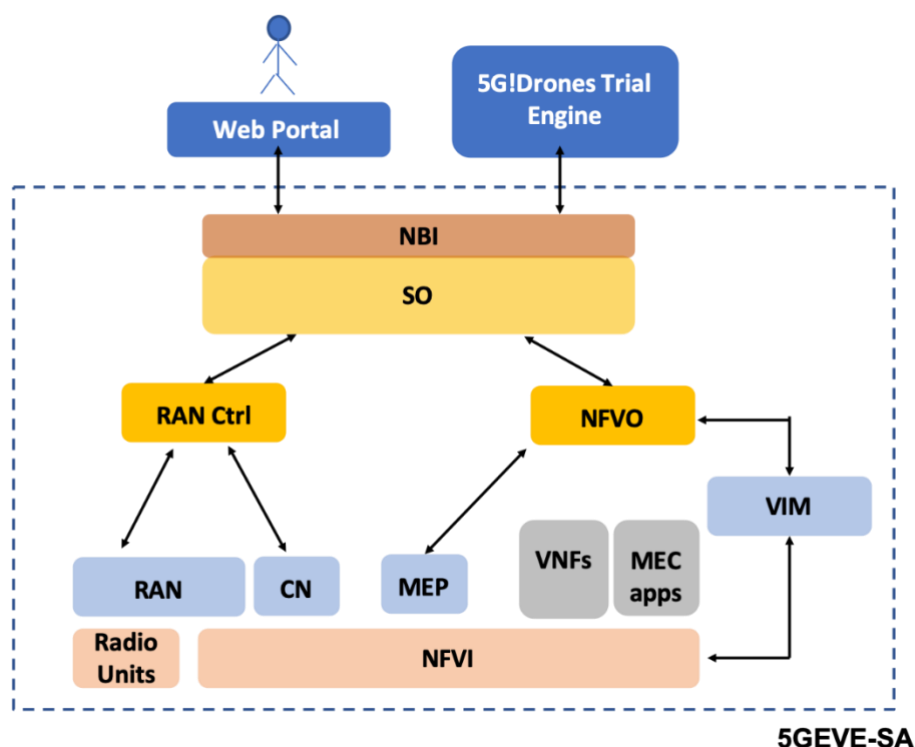


Figure 9 - 5GEVE-SA Architecture

The 5GEVE-SA facility is based on OAI elements, i.e. RAN and Core Network, to build the network infrastructure and provide 5G connectivity to UEs. Regarding the computing infrastructure, it is provided via a cluster of *Intel*-based servers located in a local Data Centre; allowing to have equivalent cloud and MEC resources.

The next sections detail the current list of features available at the facility.

3.1.2. Network Infrastructure

3.1.2.1. RAN

As mentioned earlier, the RAN components are based mainly on OAI. 5GEVE-SA provides a 5G; one eNB (4G) and one gNB (5G) are deployed in the facility. The Core Network is based on 4G EPC using OAI-CN. The RAN features are summarized in Table 13.

Table 13: RAN components of 5GEVE-SA

Component	Details
eNB (OAI) (4G)	<ul style="list-style-type: none"> Release (part) 14 and 15 Functional split (RRU, DU, CU) support, where RRU PHY lower layer, DU PHY upper layer, MAC and RLC functions are located at the DU and PDCP functions at CU. Operates in FDD or TDD. Frequency bands: <ul style="list-style-type: none"> 2580 – 2610 Mhz (band 7)
gNB (OAI) (5G)	<ul style="list-style-type: none"> Release (part) 15 and 16 Support of different 5G NR PHY numerologies

	<ul style="list-style-type: none"> Support of 5G NR PHY Bandwidth part Frequency bands: <ul style="list-style-type: none"> 5G – FR1 (< 6Ghz): 3600 – 3680 Mhz (band 78) 5G – FR2 (Millimetre waves): 27 Ghz (n257/N258)
RAN Controller	<ul style="list-style-type: none"> Real-time (change the MAC scheduling policy, Slice resources) and non-real-time controller (update the configuration of the eNB) based on FlexRAN protocol Support of 4G OAI eNB
UE (tested)	<ul style="list-style-type: none"> OAI UE Oppo Reno 5G for B27 Samsung Galaxy s10 for FR2

3.1.2.2. CN

Since 5GEVE-SA supports only NSA 5G mode, the CN is based on 4G EPC. The OAI-CN is composed by the MME, HSS, SPGW (Serving/Package Gateway) CP and User Plane (UP). OAI-CN implements the Control/User Plane Separation (CUPS) architecture (Release 15), where the SPGW is separated into two entities SPGW-C (Control Plane) and SPGW-U (User Plane). The SPGW-C controls the SPGW-U via the Packet Forwarding Control Protocol (PFCP). All the components of the OAI-CN are virtualized and run in Docker containers.

Figure 10 shows the network infrastructure of 5GEVE-SA, and the supported 3GPP interfaces, interconnecting the RAN with the CN and External networks (typically Internet).

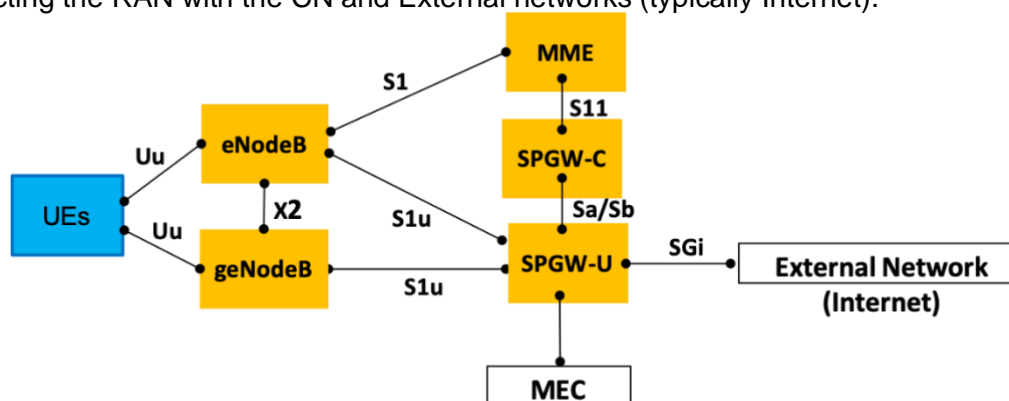


Figure 10 - Network connectivity - 5G NSA

Note that an evolution toward a Standalone 5G connectivity, i.e. deployment of a full 5G Core, is expected by the end of 2020.

3.1.3. Computing infrastructure

3.1.3.1. Cloud and MEC

5GEVE-SA orchestration system is not able to deploy on top of an external computing infrastructure, such as public Clouds as the 5G!Drones will use only the local resources deployed at Sophia-Antipolis site for the trial. Therefore, all computing resources are deployed in the local data centre, hence supporting only edge deployment. The DC of 5GEVE-SA comprises:

- A set of commodity *Intel*-architecture servers (e.g. Dell PowerEdge R640/R630) which execute the OAI RAN software packages (openairinterface5g) (1-2 servers for hard real-time processing)

- Other similar servers for Core Network and software images uploaded by the verticals during a trial.
- High-speed optical interconnection network based on a standard leaf-spine architecture and CumulusOS network operating-system.
- High-speed optical interconnections to outdoor radio-units (RRU)

A Kubernetes Cluster is used to manage the virtualized infrastructure. Kubernetes is deployed on top of bare metal, where VNF and MEC application (MEapp) are run as Docker containers. A custom Virtual Infrastructure Manager (VIM) of ETSI architecture is implemented on top of Kubernetes, i.e. using Kubernetes API.

Regarding MEC, 5GEVE-SA supports different types of MEapp deployment:

- Type1: A MEapp that requires traffic redirection to access the user-plane traffic and requests a MEC Service (ex. Radio Network Service Information (RNIS) or location API). To recall a MEC service is provided by the MEC Platform via mp1 interface (JSON format)
- Type2: A MEapp that requires only access to user plane traffic (need traffic redirection).
- Type3: A MEapp that requires MEC services without needing to access the user-plane traffic.

5GEVE-SA uses MEC ETSI compliant framework based on OAI to deploy the three different types of MEapp, and to provide MEC Service. Table 14 details the different MEC ETSI components available at 5GEVE-SA.

Table 14: ETSI MEC components available at 5GEVE-SA

Components	Functions
MEC Edge Platform (MEP)	<ul style="list-style-type: none"> - Provide, via the interface mp1 (JSON), all the available MEC Services to MEapp - Provide traffic redirection service to the MEO - Connect to the network infrastructure to implement MEC Services
MEC Services	<ul style="list-style-type: none"> - Radio Network Service (RNIS) - Traffic redirection to a MEapp - DNS service - Location API (v1)
MEC Orchestrator (MEO)	<ul style="list-style-type: none"> - On board and instantiate MEapp - Install traffic redirection rules - Integrated to the 5GEVE-SA orchestrator

3.1.4. Orchestration and management

To manage the life-cycle of VNF (including MEapp), a homemade Network Function Virtualization Orchestrator (NFVO) has been developed by EURECOM. It manages the VNF and MEapp deployed and instantiated during the trial. To deploy a service on top of 5GEVE-SA, an NSD needs to be built and passed to the NFVO. To recall a NSD [1] is a template that describes the deployment of a Network Service including service topology (VNFS and the relationships between them, Virtual Links, VNF Forwarding Graphs) as well as Network Service characteristics such as SLAs and any other artefacts necessary for the Network Service on-boarding and lifecycle management of its instances. Each VNF is described through a VNF Descriptor, which is a configuration template that describes a VNF in terms of its deployment (ex. the URL of the software image) and operational behaviour, and is used in the process of VNF on-boarding and managing the lifecycle of a VNF instance. Finally, the VNF Forwarding Graph (VNFFG) is a VNF forwarding graph where at least one node is a VNF, showing how the VNF are interconnected and connected to the external networks. Similar to a VNFD, the AppD has been

defined in [6] to specifically describe a MEapp. It contains several fields that represent the requirements of the MEapp; particularly *appTrafficRule* and *appDNSRule* that concern the traffic redirection requirements of an application, *appServiceRequired* that indicates the required MEC service to run the MEapp, and *appLatency* that indicates the latency requirement of a MEapp.

In 5GEVE-SA, a modified version of the NSD is used in order to include AppD and VNFD. Figure 11 shows the modified NSD to include MEapp via the integration of AppD.

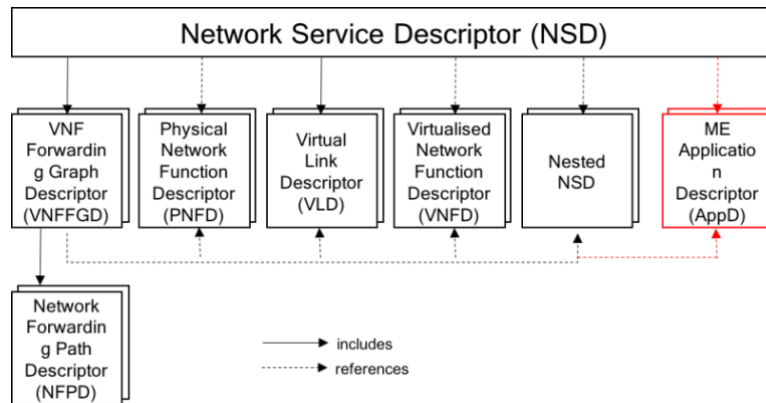


Figure 11 - Integration of AppD into an NSD

3.1.4.1. Network Slicing

5GEVE-SA allows the deployment of an end-to-end network slicing, including RAN slicing. The SO is in charge of deploying a slice according to a NST, which will be detailed later.

The RAN slicing is possible (now) only on top of eNB OAI, allowing via the RAN controller to assign specific number of Physical Resources blocks (PRB) for each slice, or to use pre-emption policy for uRLLC over the other type of Slices. 5GEVE-SA allows also the deployment of dynamic OAI-CN per slice, i.e. each slice has its own OAI-CN, described via a VNFD and included in the NSD. This however requires that each Network Slice has its own PLMN. You should note that ongoing works are done for implementing the same features for gNB, but will be deployed in future releases of the facility.

Regarding MEC, no slicing is implemented, but could be added as 5G!Drones enabler (from WP3). However, at the VIM level, all the slices are isolated.

The SO uses as input a NST to deploy an end-to-end slice on top of the facility. The NST is composed by three main parts:

- Metadata on the slice, such as duration, tenant Id, Slice Id, etc.
- RAN part of slice that describes the RAN resources needed, such as type of slice (uRLLC or eMBB or mMTC), list of UE (IMSI), requested Bandwidth, maximum latency, etc.
- NSD part of slice that describes the virtual resources that need to be deployed at the edge or cloud.

For each part, the list of KPI that the trial owner wants to monitor need to be indicated. Details on KPI will be given in section 3.1.4.2. Figure 12 shows a structure of the NST, particularly the Meta-data fields and the RAN part.

```

"metadata": {
  "name": "Test Slice 1",
  "status": "Not running",
  "provider": "Eurecom",
  "version": "1.0",
  "startDate": "2020-03-15 15:10",
  "endDate": "2020-03-15 16:10",
  "kpi-list": ["Uplink Data Rate", "Downlink Data Rate", "IP Rate"]
},
"ranSubSlice": {
  "type": "URLLC",
  "region": "EURECOM",
  "latency": 10,
  "trafficOrientation": "Uplink",
  "UE": [20000000507],
  "kpi-list": ["Memory Utilization", "Latency Edge", "Latency VIM"]
},

```

Figure 12 - Example of 5GEVE-SA NST

The list of KPIs to measure should be included in the NST passed to the SO. Other KPIs might be added in future releases of the facility.

3.1.4.2. KPI

Table 15 summarizes the list of KPI currently available for measurement in 5GEVE-SA.

Table 15: Supported KPIs in 5GEVE-SA

KPI	Level	Details
Slice-deployment-duration	SO	Time needed to create an end to end slice
Slice-time-decommissioning	SO	Time needed to release all slice resources
Latency-RAN	RAN	Latency at the RAN (aggregated per slice)
Uplink-data-rate	RAN	Uplink data rate (aggregated per slice)
Downlink-data-rate	RAN	Downlink data rate (aggregated per slice)
Packet-Loss-rate	RAN	Packet loss at the RAN after attempts (RLC layer) (aggregated per slice)
IP-rate	RAN	Packet rate (at PDCP) (aggregated per slice)
Latency-eNB-CN	RAN	Measured RTT between the RAN and CN
Bandwidth	RAN	Bandwidth of cells
CPU-utilization	NFVO	Aggregated per slice or per VNF
Memory-utilization	NFVO	Aggregated per slice or per VNF
Number-instances	NFVO	Number of Replica Sets per VNF
Latency-edge	NFVO	Latency from CN to Edge host
Latency-VIM	NFVO	Latency from CN to VIM

3.1.5. Security features in 5GEVE

The 5GEVE-SA ensures security by using 3GPP authentication and encryption solution, i.e. using the IMSI and AKA protocol. All the network slices are isolated at the RAN as well as at the Edge, where no communication is authorized between two slices.

3.2. Facility interaction with the trial controller for use case deployment

3.2.1. Deployment of a Trial

All the trials are deployed as a Network Slice in 5GEVE-SA. This means that the trial needs to be described in the form of an NST. To do so, two options are possible: use a web portal or use the SO NBI.

3.2.1.1. Web portal

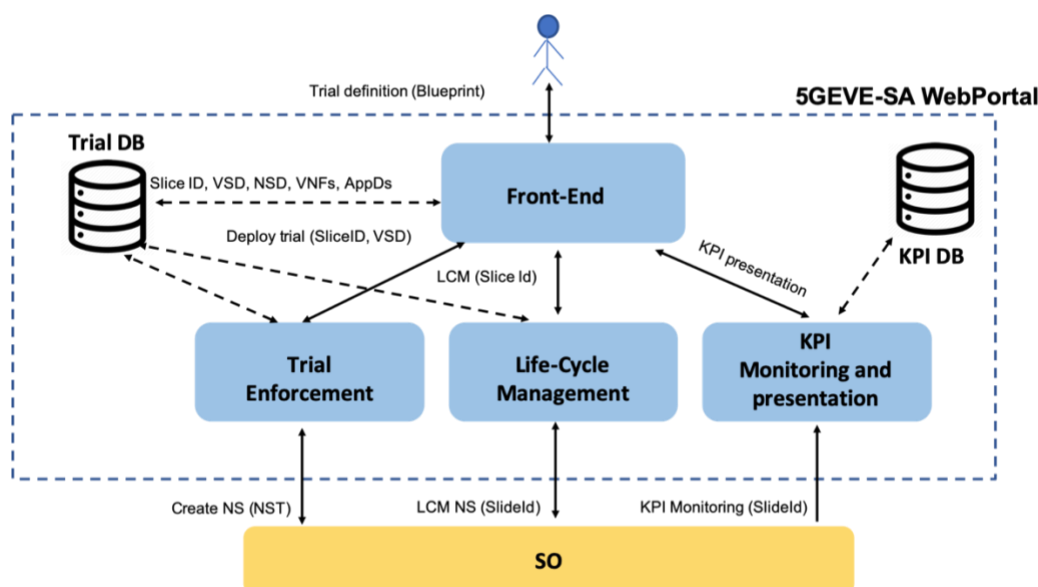


Figure 13 - 5GEVE-SA Web portal architecture

5GEVE-SA has its own web portal, which is different from the one used by 5GEVE central site. The Web portal proposes to fill a form to describe a trial. Figure 13 details the architecture of the Web portal. It is composed by a front-end, where the trial owner fills a form describing the scenario and specify the KPIs to measure. As output, the front-end produces a Vertical Service Descriptor (VSD) that contains all the information entered by the trial owner. The VSD is stored, along with other information in a data-base, and passed to the Trial enforcement, which translates it to a NST, and via a NBI call, it is passed to the SO to request the creation of a network slice to run the trial. Other components compose the Web portal, such as Life-cycle Management, KPI monitoring and results presentation.

3.2.1.2. Northbound API (NBI)

Table 16 shows the list of NBI allowing to manage the life-cycle of a network slice (i.e. a trial) running on top of 5GEVE-SA.

Table 16: NBI of the SO of 5GEVE-SA

API	Details
createSlice (SliceID, NST)	Instantiate the associated NST in the facility (NFVO and RAN Controller)
getSlice (SliceID)	Returns the associated Network Slice Template
stopSlice (SliceID)	Terminate the Slices but without off-boarding the allocated resources (Resources are still allocated but not used)
resumeSlice (SliceID)	Resume the stopped Slice with the same previous allocated resources
deleteSlice (SliceID)	Delete the stopped Slice with off-boarding the allocated resources
listSlices()	Return all the available Slices (running, stopped)
updateSlice(SliceID, NST)	Update the resources of a Slice (Not available yet)

3.3. Detailed mapping of use case scenario components to the 5G facility

5GEVE-SA site will host the trial of three scenarios coming from two use-cases. For each scenario, a pseudo-VNF FG is defined in order to identify the involved components, their requirements that need to be provided in terms of connectivity and computation, which need to be provided by the facility. For each component, we will describe how it will be mapped to a facility resource, and which partner will provide that component.

3.3.1. UC1 scenario 1 - UTM Control and command application

This use case demonstrates a common functionality for all UAV applications, by providing the necessary safe and secure incorporation of drones into the air traffic management. Indeed, the dramatic growth of UAVs over the past decade and the subsequent development of commercial drone activities especially at low altitude have posed the question of drones' safe and secure flight operations in the face of increased air traffic. UTM (UAS Traffic Management) is expected to manage drone traffic in the lower altitudes of the airspace, providing a complete and comprehensive end-to-end service to accumulate real-time information of weather, airspace traffic, drone registration, and credentials of drone operators, among others. The need for UTM systems has been driven by a number of factors such as the recent increase in the number of drones in the airspace, increasing involvement of different governments and emerging regulations, as well as collaboration of key stakeholders for the development of a working architecture. From now on and for more details on all the use-cases please refer to [2]. Figure 14 shows the UC1 scenario1 components and how they are mapped to facility resources. Note that the aim here is to focus on the network connectivity and computation requirements, which can be provided by the facility.

It should be emphasized that the UTM system, in accordance with applicable and planned regulations, will not directly control the drone / drones in any way. UTM may issue recommendations or guidelines on how they must be met, e.g. in controlled zones. It will be the responsibility of the operator or control software to fully and immediately meet the requirements specified in the "U-space order", and in the case of Class G spaces, the requirements will be optional. Examples of cooperation between the UTM system and the drone or control software will be:

- creation of a "no fly" zone

- “no fly zone” creation with instructions on the most effective way to leave it, if the aircraft is already within
- issuing a wait command in the holding airspace
- information, condition and minimum equipment about passing through restricted airspaces

During the flight, the 5G network should ensure C2 link transmission, FPV bandwidth and / or telemetry as promised at the SLA mission planning stage. It is extremely important for SLA to refer to the selected 3D areas at a given time. It is expected that coverage maps will be updated on a regular basis, and the algorithms calculating them will work as close as possible to the actual coverage.

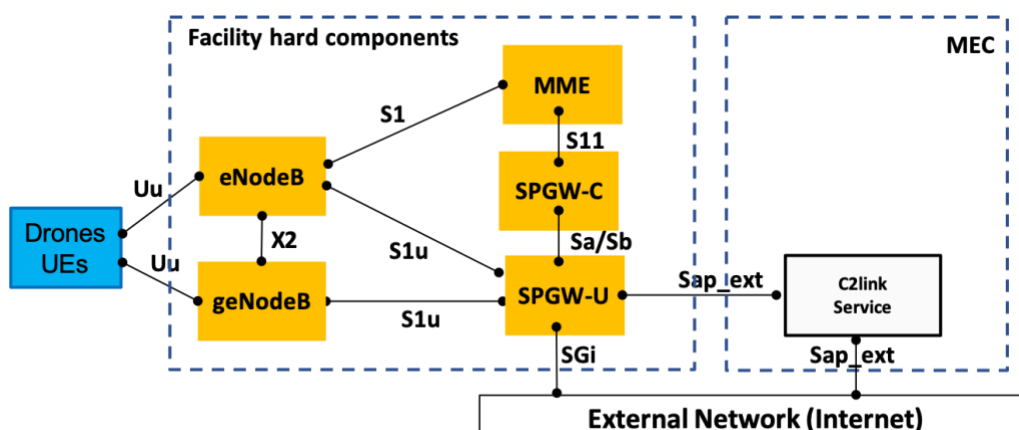


Figure 14 - UC1SC1- Functional components and their mapping to the facility

The facility hard components are those already deployed at the facility, and enable 5G connectivity via the NSA mode. The UE supporting both 4G and 5G radio access is attached to the flying drone. For Deployment 1, the service that needs to be instantiated at the MEC is composed only by the C2link service (i.e. one VNF), and requires two network connections to external networks (Sap_ext: Service Access Point external); one to the UE data plane and one to the Internet. It's worth noting that all the VNF in 5GEVE-SA are described via an AppD, as they need to be deployed at the MEC. The NSD includes only AppD. This is valid for all the use-cases to be deployed at 5GEVE-SA. Tables 17-22 summarize the partners in charge of providing each component for the trial of UC1 scenario 1.

CAFATECH's UGSC Platform (CUP) software for C2 link operation will be installed in MEC. It will assure automatic drone flight control through 5G connection and from the other side it will be connected to the U-Space system, which is located in the internet. The CUP and U-Space will exchange the messages in both directions, ensuring situational awareness of other airspace users and fast reaction to changed conditions or emergency. Deployment 1 of UC1SC1 will use DJI Mavic drone from CAFA Tech and controlled by CAFA Tech CUP software.

Deployment 2 of UC1SC1 will use First Person View (FPV) from Nokia's drone camera, streamed to goggles and controllers provided by Nokia. The connectivity to U-Space system will be the same as for in Deployment 1.

Table 17: UC1SC1 partner/components

Component	Partner
5G connectivity and MEC	EURECOM (5GEVE-SA)
UE (a Drone with 4G/5G connectivity)	CAFA Tech, Nokia
C2 Link service	CAFA Tech
First Person View – inbuilt drone camera	Nokia drone
First Person View – Ground Control Station VR goggles and controllers	Nokia

Table 18: UC1SC1 UAV components

UAV Components	Type (Hw/Sw)	Partner
DJI Mavic drone	Hw	CAF
Nokia drone	Hw	Nokia
Telemetry link to U-space	SW	DRR and FRQ

Table 19: UC1SC1 UAV operator components

UAV Operator Components	Type (Hw/Sw)	Partner
CAFA C2 Ground Control Dock (communicates between 5G MEC based CAFA CUP and drone)	Hw	CAF
Laptop with 5G device for using MEC based CAFA CUP	Hw	CAF
Nokia Goggle for FPV	Hw/Sw	Nokia

Table 20: UC1SC1 UTM components

UTM Components	Type (Hw/Sw)	Partner
Data stream showing the flying objects based on ADS-B, FLARM, OGN, multi-lateration	SW	INVOLI
UTM platform	Service	DRR / FRQ

Data stream from INVOLI can be used in all use cases to increase the security of the experiments and other aerial objects in the nearby vicinity. It will contain the ADS-B and alarm signals detected by INVOLI's Micro Control Tower (MCT) receiver installed in the trial area. Additionally, if UAV can accommodate the INVOLI's KIVU tracker on the board, the flight details (position and altitude) will be also incorporated to the stream, independently of the telemetry stream reported by UAV controller.

Table 21: UC1SC1 5G components

5G Components	Type (Hw/Sw)	Partner
5G UE (smartphones) for CAFA Dock and for DJI Mavic	Hw	CAF
MEC based CAFA CUP	Sw	CAF
MEC based IoT managing software	Sw	CAF
IoT cameras using CatM1/M2	Hw	CAF
MEC based Video Analyzer	Sw	CAF

Table 22: UC1SC1 other components

Other Components	Short description	Type (Hw/Sw)	Partner
Video Analyzer	Video analysing software based on Computer Vision algorithms to analyse drone and IoT cameras photos and videos	Sw	CAF

3.3.2. UC2 Scenario1 - Monitoring a wildfire

This use-case scenario is known as “Monitoring a wildfire”, where UAVs are equipped with HD cameras which can be used for streaming HD video to a remote application hosted at the edge. Using AI tools, the remote application analyses the video to predict the spreading direction of wildlife to the firefighters so they can pay immediate attention to those areas and also avoid using the potentially dangerous routes for rescue operation. In such a case, 5G-based eMBB is needed to handle the video traffic volume efficiently. Moreover, the support of a MEC server to process the video as close as possible to the rescue operation is necessary.

The scenario combines drones with IoT devices (sensors, cameras). Drones can deliver IoT sensors/cameras to crossroads or other strategic viewpoints and IoT sensors provide data to control the spread of wildfire, toxic gases or people’s movements. Figure 15 illustrates the mapping of the use-case to facility components.

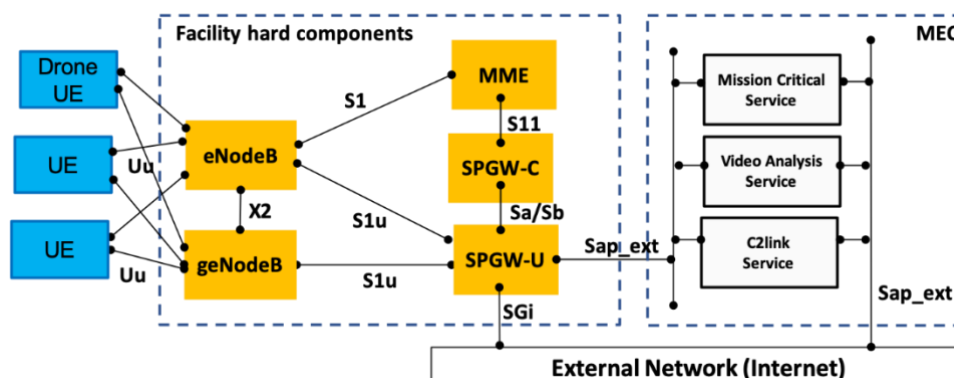


Figure 15 - UC2 scenario 1- Functional components and their mapping to the facility

In this scenario, one drone UE and two other classical UEs are connected to the 5G RAN. All the UEs have 4G/5G radio. The drone sends video stream to the video analysis service. The service to be instantiated is composed by three VNFs to be deployed at the MEC. One for the Mission Critical System (MCS) service, one for video analysis and one for the C2link service to control the drones. All the three VNFs have two external connections, one for to the UE data plane and one for Internet. The MCS platform uses the first connection to share multimedia and data streams between all the UEs, and the second one to communicate with command centre, in charge of tactical operation (defining subscribers, rights, communications, etc.) and to load maps tiles. Tables 23-27 show the partners in charge of providing each component needed to trial UC2 scenario 1.

Table 23: UC2 Scenario1 partner/components

Component	Partner
5G connectivity and MEC	EURECOM (5GEVE-SA)
UE (a Drone with 4G/5G connectivity)	CAFA Tech
UEs	AIRBUS
C2 Link service	CAFA Tech
Video analysis service	CAFA Tech
Mission Critical service	AIRBUS

Table 24: UC2 Scenario1 UAV components

UAV Components	Type (Hw/Sw)	Partner
DJI Mavic drone	Hw	CAF

Table 25: UC2 Scenario1 UAV operator components

UAV Operator Components	Type (Hw/Sw)	Partner
CAFA C2 Ground Control Dock (communicates between 5G MEC based CAFA CUP and drone)	Hw	CAF
Laptop for using MEC based CAFA CUP	Hw	CAF

Table 26: UC2 Scenario1 UTM components

UTM Components	Type (Hw/Sw)	Partner
Support for dFPL (drone Flight Plan). Situational awareness (airspace perspective) service to submit dFPL.	SW	DRR FRQ
U-space telemetry endpoint	SW	DRR FRQ
Mission prioritization support for 112 missions	SW	DRR FRQ

Table 27: UC2 Scenario1 5G components

5G Components	Type (Hw/Sw)	Partner
5G UE (smartphones) for CAFA Dock and for DJI Mavic	Hw	CAF
MEC based CAFA CUP	Sw	CAF
MEC based IoT managing software	Sw	CAF
IoT cameras using CatM1/M2	Hw	CAF
MEC based VideoAnalyzer	Sw	CAF

3.3.3. UC2 Scenario 2 - Disaster recovery

This use-case scenario is a “disaster recovery” simulation in which UAVs are used to simultaneously and autonomously provide on-demand network connectivity and video footage of the affected area. UAVs can interconnect and communicate with ground stations over direct D2D links, allowing for the

rapid deployment of a wireless backhaul in situations where capacity is needed on an expedited basis. These UAVs can then bridge the signal for backhaul interconnect to provide ultra-reliable, low-latency wireless connectivity to end-users in need. These networks allow both victims and emergency workers to communicate when it is most important. Figure 16 illustrates the mapping of the use-case to components hosted at the facility.

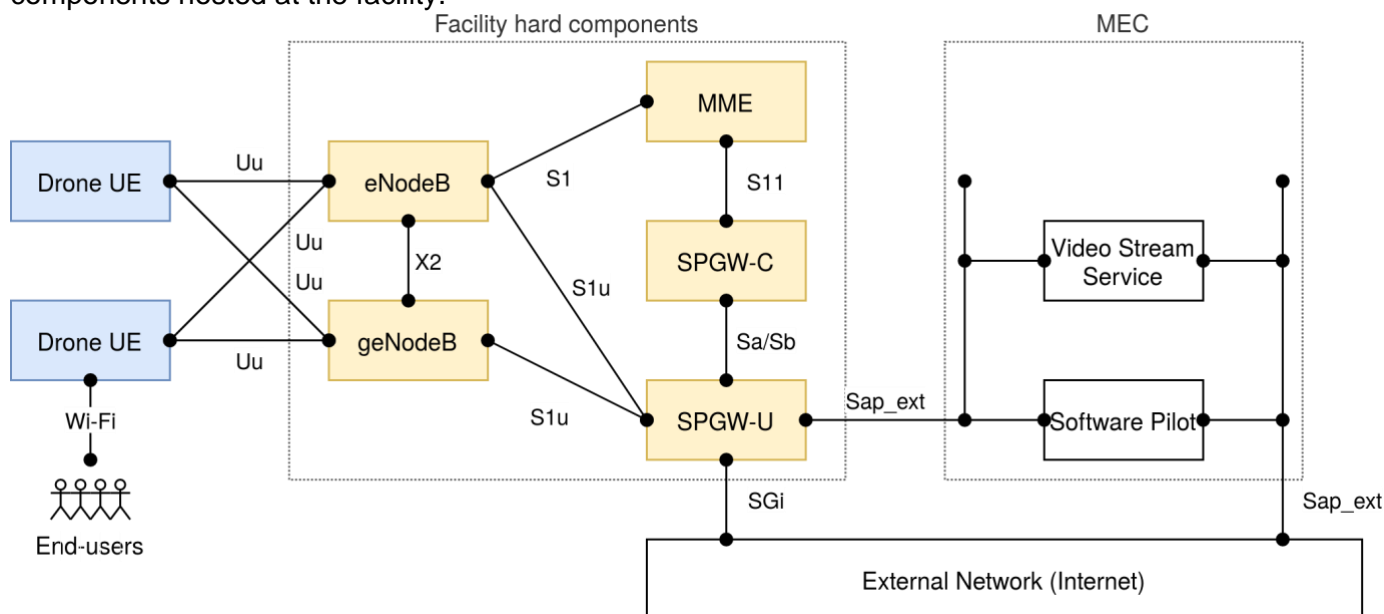


Figure 16 - UC 2 scenario 2 - functional components and their mapping to the facility

This scenario will make use of two UAVs (hereafter referred to as the network UAV and the video UAV). Both UAVs will be augmented by a small on-board computer (UL-ACE) and managed by a software pilot (UL-CCP) hosted at the MEC. Initially, the video UAV will patrol the affected area, streaming video to services hosted at the MEC. These services will analyse the video stream for potential humans on-site. Once a human is detected in the video stream, the network UAV will be autonomously dispatched to the detection coordinates in order to provide ad-hoc network connectivity to the end-user in the disaster area.

The network connectivity will be provided via a Wi-Fi access point, although this can optionally be substituted for a 4G small cell (if available). The minor changes from the scenario description in D1.1 [2] have been incorporated in order to account for the unavailability of portable 5G small cells during the planned test dates.

This service will require two VNFs running at the MEC. The first provides the C2 link service (UL-CCP) for controlling and coordinating between the UAVs in use. The second VNF provides video stream reception and analysis. Both VNFs require two connections – one to the internet and one to the UEs (i.e., the video and network UAVs). The external network connection is required to communicate with externally hosted services such as UTM and the 3020 LifeX Solution. Tables 28-32 show the partners in charge of providing each component needed to trial UC2 scenario 2.

Table 28: UC2 scenario 2 UAV components

UAV Components	Type (Hw/Sw)	Partner
Matrice M600	HW	HEP
Video Streaming Camera	HW	HEP
Wi-Fi Access Point	HW	UMS
5G Smartphone (w/ USB tethering)	HW	EUR (integration with drone to be done by UMS)

Table 29: UC2 scenario 2 UAV operator components

UAV Operator Components	Type (Hw/Sw)	Partner
UL-ACE	HW/SW	UMS
UL-CCP	HW/SW	UMS
Video Stream Analysis	SW	UMS

Table 30: UC2 scenario 2 UTM components

UTM Components	Type (Hw/Sw)	Partner
Support for dFPL (drone Flight Plan). Situational awareness (airspace perspective) service to submit dFPL.	SW	DRR FRQ
U-space telemetry endpoint	SW	DRR FRQ

Table 31: UC2 scenario 2 5G components

5G Components	Type (Hw/Sw)	Partner
5G Network	HW/SW	EUR
MEC	HW/SW	EUR

Table 32: UC2 scenario 2 other components

Other Components	Short description	Type (Hw/Sw)	Partner
3020 LifeX Solution	Mission-critical communications service	SW	FRQ

4. X-NETWORK

4.1. Highlights of 5G components/ enablers within the facility for use case deployment

X-Network is the trial site provided by Aalto University. It is located at the Otaniemi campus of the university, and covers an area of 5.2 Km2. X-Network is a supporting site to the ICT-17 trial facilities (5GEVE and 5Genesis). It is part of the Finnish national project 5GTNF (5G Test Network Finland) which is incrementally built throughout several research projects with academic and industrial partners.

4.1.1. Architecture

The trial site of Aalto University, X-network, offers trailing support of mobile telecommunication networks. The facility includes different components including 4G LTE eNBs, 5G NR gNBs, MEC/edge platforms, EPC and experimental 5G cores. An overview of the current deployment at Aalto University trial site is shown in Figure 17. In addition to these components at the infrastructure layer, the facility is incrementally building a solution for the management and the orchestration of the virtual resources.

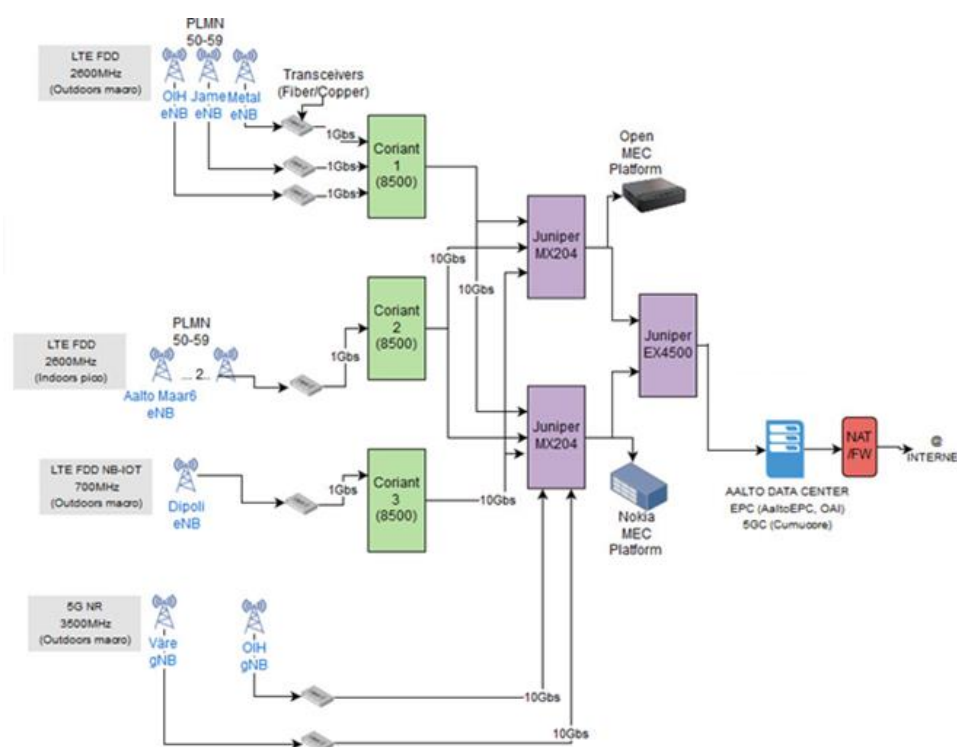


Figure 17 - overview of the network deployment in Aalto University

4.1.2. Network Infrastructure

4.1.2.1. RAN

The trial site of Aalto University, X-Network, operates different types of RAN. This includes LTE and NB-IoT networks. Furthermore, the facility also operates a NR gNB as described in Table 33 (the gNB is currently operating in NSA mode). In order to perform 5G tests, Aalto University has been granted by national regulatory authority, TRAFICOM, the license to 3.5 Ghz. Two commercial UEs have been tested with the current NR gNB which are also listed in the below Table.

Table 33: RAN components of X-network

Component	Details
eNB (4G)	<ul style="list-style-type: none"> Ericsson NB-IoT <ul style="list-style-type: none"> 3.6 – 3.8 GHz Nokia LTE <ul style="list-style-type: none"> FDD 2.6 GHz (band 7)
gNB (5G)	<ul style="list-style-type: none"> Nokia AirScale gNB Functional split (RRU, DU, CU) support Frequency bands: <ul style="list-style-type: none"> 3.6 – 3.8 GHz
RAN controller	<ul style="list-style-type: none"> X-Network makes use of commercial RAN. The controller of the RAN is currently based on WEM (Web Element Manager).
UE (tested)	<ul style="list-style-type: none"> Huawei Mate 20 5G Samsung A90 5G

4.1.2.2. CN

The core network includes three different virtualized EPC core network implementations which are Nokia core, Aalto core and CMC core (Cumucore). The latter implements a prototype of 5G core architecture including AMF, SMF, UPF, NSSF and NRF. The core network will be running in a datacentre located at the campus. An overview of the CMC core network is shown in Figure 18. Other core networks can also be considered to be used during the project

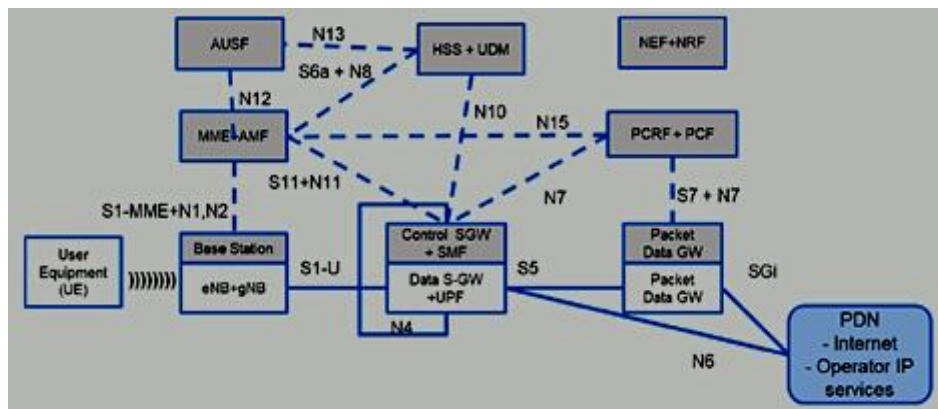


Figure 18 - Overview of the EPC/5GC architecture.

4.1.3. Computing infrastructure

4.1.3.1. Cloud and MEC

The computing infrastructure deployment at the trial site of Aalto University consists of cloud and MEC deployments. The data centre is physically located in the premises of the campus (Otakaari building) and hosts the different cloud-based 4G/5G network functions.

Different MEC/edge solution are available which are deployed between the data centre and radio access networks. This includes Nokia MEC, Nokia edge and Aalto MEC. The latter is not considered as ETSI compliant and consists of VM hosting the UPF and the vertical applications. The connections between eNB/gNB is based on fibre converge in SDN-ready Juniper MX204 edge routing platform with capacity up to 400Gbs (an overview is provided in Figure 19).

4.1.4. Orchestration and management

In order to manage the different VNFs and their lifecycles, Aalto University is building a homemade orchestration solution. An overview is shown in Figure 19. While the NFVO is responsible for managing the different VNFs on the top of the virtualized environment, the RAN controller is used to control gNB. Aalto University trial site makes use of a commercial gNB (Nokia AirScale gNB). Currently, the gNB can be managed only via a Web Element Manager (WEM).

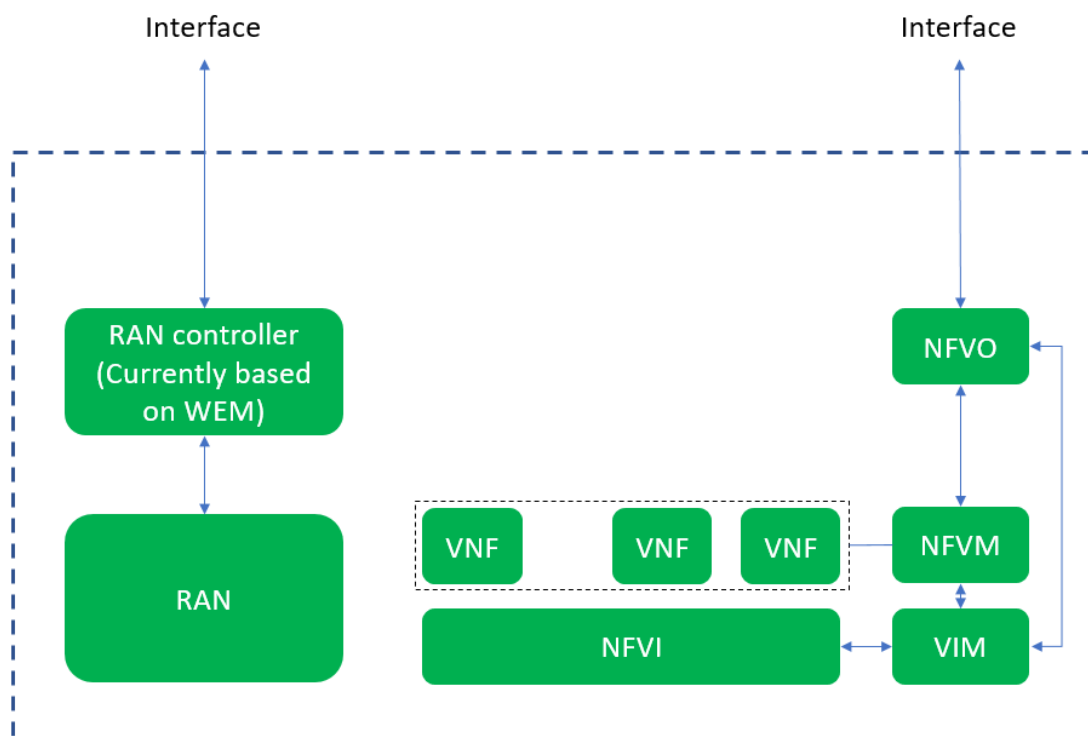


Figure 19 - Overview of the current/planned orchestration solution at X-Network

4.1.4.1. Network Slicing

The deployment of a network slice is based on an NST. An example of a NST used in X-Network is shown in Figure 20. Different information is considered, including the set of VNFs, the service category, the start and the end dates, etc.

```
--data-row '{
  "blueprint": 33,
  "vnfs": [
    5
  ],
  "name": "slice21",
  "type": "controlplan",
  "startDate": "2021-08-12",
  "endDate": "2023-08-14",
  "domainName": "dd.example.com",
  "description": "sdfdsf sdf sf sf",
  "startDate": "2021-08-12",
  "endDate": "2023-08-14",
  "type": "controlplan"
}'
```

Figure 20 - An example of a NST used in X-Network.

4.1.4.2. KPI

A number of KPIs can be measured in the trial site. This can be captured from different levels which are summarized in Table 34.

Table 34: List of KPIs that can be measured at X-Network

KPI	Level	Details
Cell availability	RAN	Cell availability
Cell throughput	RAN	Cell throughput
Average connected UEs	RAN	Average connected UEs
Latency	RAN	Latency related to F1-U interface
CPU utilization	NFVO	CPU utilization per VNF
Memory utilization	NFVO	Memory utilization per VNF
Slice deployment duration	NFVO	Time needed to create a slice
Slice decommissioning duration	NFVO	Time needed to release a slice

4.1.5. **Security features in X-Network**

The trial facility of Aalto University is managed by IT team. The latter ensures security features including firewalls and SSH to the different network components. The physical access to the datacentres and the base stations is limited to authorized persons ensuring therefore physical security.

4.2. **Facility interaction with the trial controller for use case deployment**

4.2.1. **Deployment of a Trial**

The deployment of a trial is translated into deploying and managing network slices on the top of the facility. This can be performed using a dedicated Web portal and also via a set of interfaces.

4.2.1.1. **Web portal**

Figure 21 shows a screenshot of the web portal used at the trial site of Aalto University. It provides a user-friendly interface allowing to interact with the experimenter. Among the different features, a user can manage the different network slices, the underlying VNFs, etc.

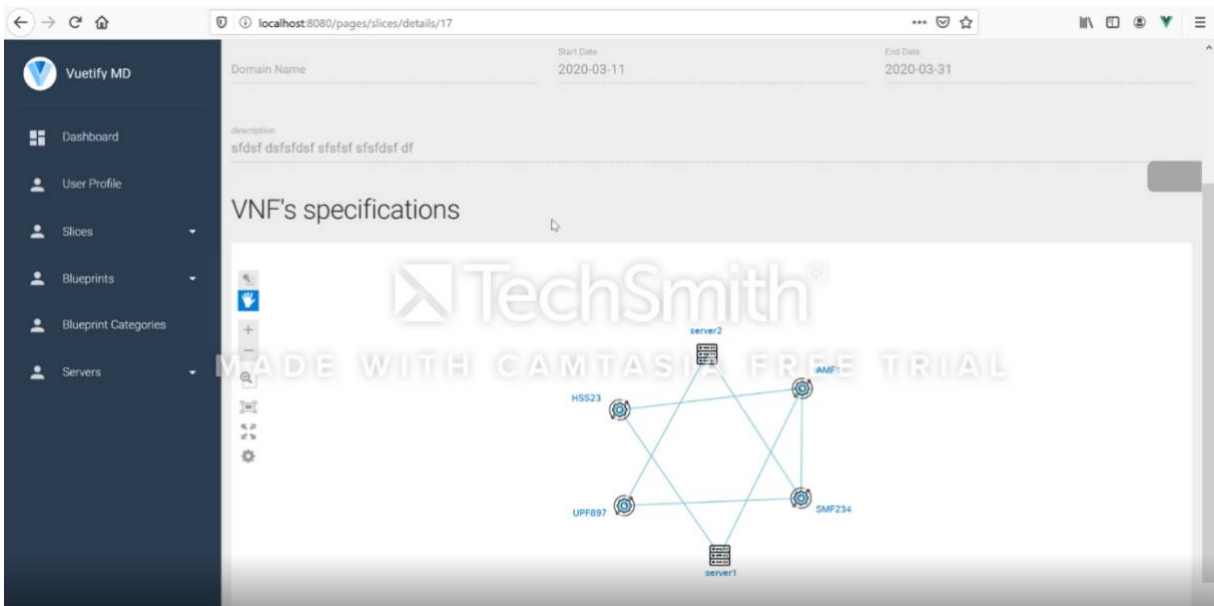


Figure 21 - Screenshot of the Web portal used at Aalto University

4.2.1.2. **Northbound API (NBI)**

In addition to the web portal, the trial site is incrementally building interfaces allowing to deploy and manage network slices. In particular, we are building interfaces allowing run time configuration of network resources (after deployment). This will allow the interaction with the trial controller. The below table lists the interfaces provided by the facility to manage the network slices.

Table 35: NBI of the SO of X-Network

API	Details
ListSlices()	List the available network slices
CreationSlice(NST)	Create a network slice
TerminateSlice(id)	Termination of a Network slice

4.3. Detailed mapping of use case scenario components to the 5G facility

4.3.1. UC3 scenario 2 - UAV-based IoT data collection

In this scenario UAVs will be used to provide IoT services from height. Each UAV will be equipped with a set of IoT devices to measure different parameters such as temperature, humidity, etc. The drones will be controlled by a software pilot ensuring C2 services, while the data collected by the drones will be processed by a dedicated service. For this end, the facility will make use of its cloud/edge server to host the application services (the software pilot and the IoT data processing services). Figure 22 depicts the scenario components and how they are mapped to the facility.

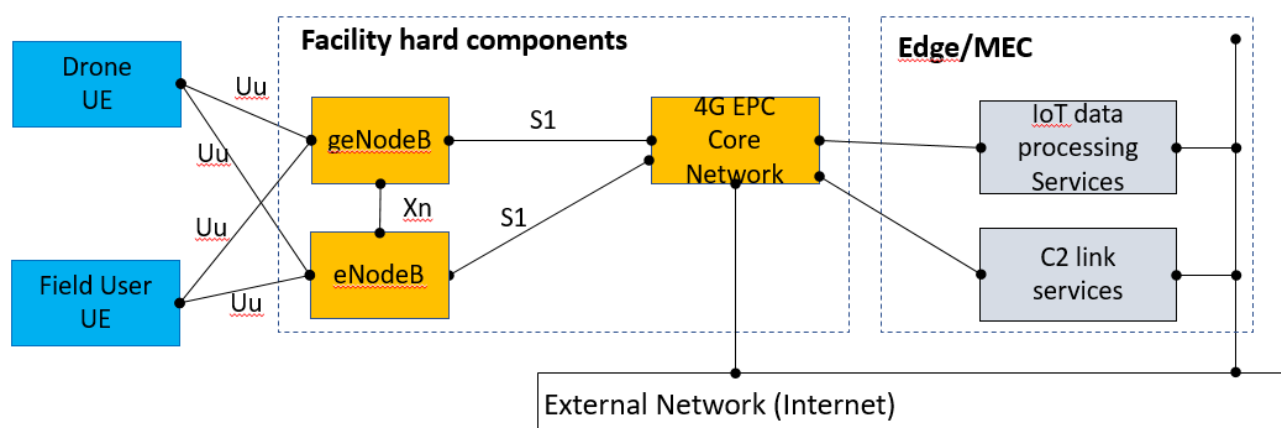


Figure 22 - UC3 scenario 2 - Functional components and their mapping to the facility

Tables 36-39 show the partners in charge of providing each component needed to trial UC3 scenario 2.

Table 36: UC3 scenario 2 partner/components

Component	Partner
5G connectivity and MEC/Edge	Aalto University (X-network)
UE (a Drone with 4G/5G connectivity)	Aalto University
C2 Link service	Aalto University
IoT data processing	Aalto University

Table 37: UC3 scenario 2 UAV components

UAV Components	Type (Hw/Sw)	Partner
Homemade drones	Hw	Aalto University
IoT devices (on-board of the drones)	Hw	Aalto University

Table 38: UC3 scenario 2 UAV operator components

UAV Operator Components	Type (Hw/Sw)	Partner
Software pilot	Sw	Aalto University
IoT data processing	Sw	Aalto University

Table 39: UC3 scenario 2 UTM components

UTM Components	Type (Hw/Sw)	Partner
Support for dFPL (drone Flight Plan). Situational awareness (airspace perspective) service to submit dFPL.	SW	DRR, FRQ
U-space telemetry endpoint	SW	DRR, FRQ

4.3.2. UC1 scenario 3 - Drone logistics

The purpose of this scenario is to demonstrate how UAVs through 5G network capabilities can provide logistics solutions. The first scenario is the delivery of a drug to a sick person with a drone. A sick person who cannot go to a pharmacy can receive his/her medicine through a personal delivery by subscribing to a Drone Logistics Network (DLN). The delivery box has IoT (NB-IoT or LTE-CatM1) device which ensures communication with the DLN to coordinate parcel drop-off, landing, etc. Parcel drop off and landing functions need very low latency and therefore DLN Delivery Software (DLN DS) works on MEC. A DJI Mavic-2 drone takes one medicine (up to 50g) from a virtual pharmacy and flies towards the customer delivery box. Approaching the delivery box, the drone has bad GPS signal quality between houses. Drone streams video over 5G and DLN human operator takes over the drone control and uses 5G communication based remote control. For parcel drop-off DLN DS communicates between drone remote controller and delivery box IoT. Figure 23 depicts the scenario components and how they are mapped to the facility.

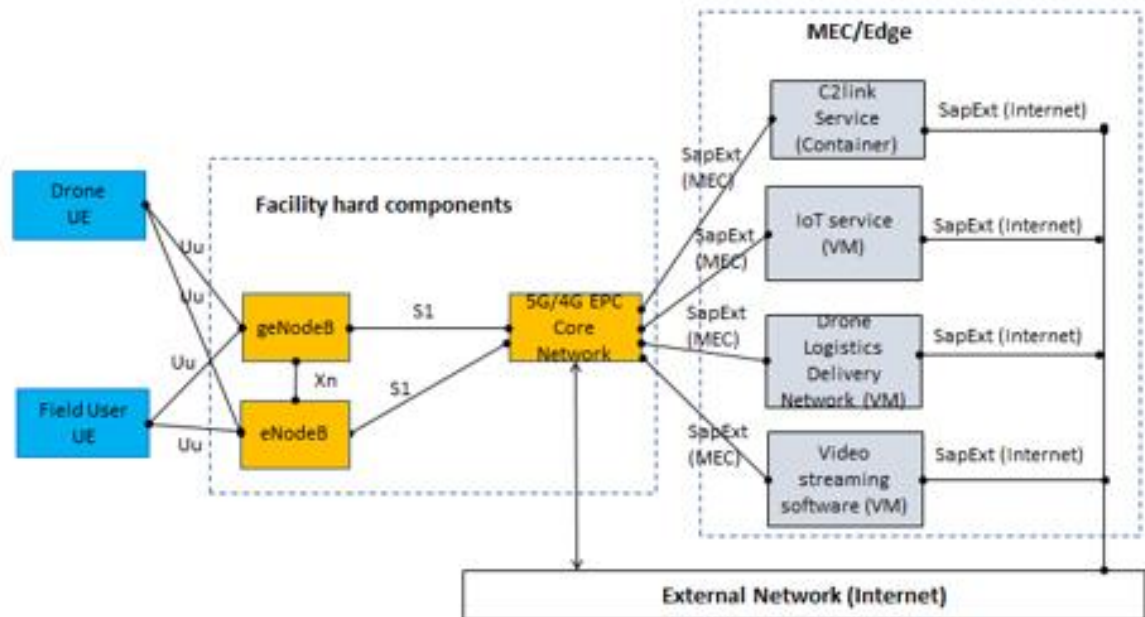


Figure 23–UC1 scenario 3 - Functional components and their mapping to the facility

Tables 40-45 show the partners in charge of providing each component needed to trial UC1 scenario 3.

Table 40: UC1 scenario 3 partner/components

Component	Partner
5G connectivity and MEC/Edge	Aalto University (X-network)
UEs (two 5G smartphones)	Aalto University
C2 Link service	CAF
IoT data processing	CAF

Table 41: UC1 scenario 3 UAV components

UAV Components	Type (Hw/Sw)	Partner
DJI Mavic	Hw	CAF
DJI Matrice 210	Hw	CAF

Table 42: UC1 scenario 3 UAV operator components

UAV Operator Components	Type (Hw/Sw)	Partner
CAFA C2 Ground Control Dock (communicates between 5G MEC based CAFA CUP and UAV)	Hw	CAF

Laptop for communicating MEC based CAFA CUP	Hw	CAF
---	----	-----

Table 43: UC1 scenario 3 UTM components

UTM Components	Type (Hw/Sw)	Partner
Support for dFPL (drone Flight Plan). Situational awareness (airspace perspective) service to submit dFPL.	SW	DRR FRQ
U-space telemetry endpoint	SW	DRR FRQ

Table 44: UC1 scenario 3 5G components

5G Components	Type (Hw/Sw)	Partner
5G UE (smartphones) for CAFA Dock and for DJI Mavic/Matrice	Hw	Aalto University

Table 45: UC1 scenario 3 other components

Other Components	Short description	Type (Hw/Sw)	Partner
Drone Logistics Network Delivery Software (DLN DS)	Drone Logistics Network Delivery Software (DLN DS)	Sw	CAF
NB-IoT or Cat M1/M2 IoT device for delivery box	To communicate between box and drone	Hw	CAF
CAFA IoT software	C2 soft for controlling IoT devices	Sw	CAF
Drone video streaming software	Video stream from drone to DLN DS or operator	Sw	CAF
MEC based CAFA CUP	C2 soft for controlling UAV	Sw	CAF

5. 5GTN

5.1. Highlights of 5G components/ enablers within the facility for use case deployment

5.1.1. Architecture

5GTN is one of the supporting sites to ICT 17 facilities within the project (i.e., 5GEVE and 5GENESIS). It is located in Oulu, Finland. Figure 24 illustrates 5GTN UO architecture and its components. The 5GTN facility is based on Nokia elements, i.e. RAN and Core Network, to build the network infrastructure and provide 5G connectivity to UEs. The computing infrastructure is provided via a cluster of Intel-based servers located in the university campus premises, allowing to have adequate cloud and MEC resources. The next sections will detail the current list of features available at the facility.

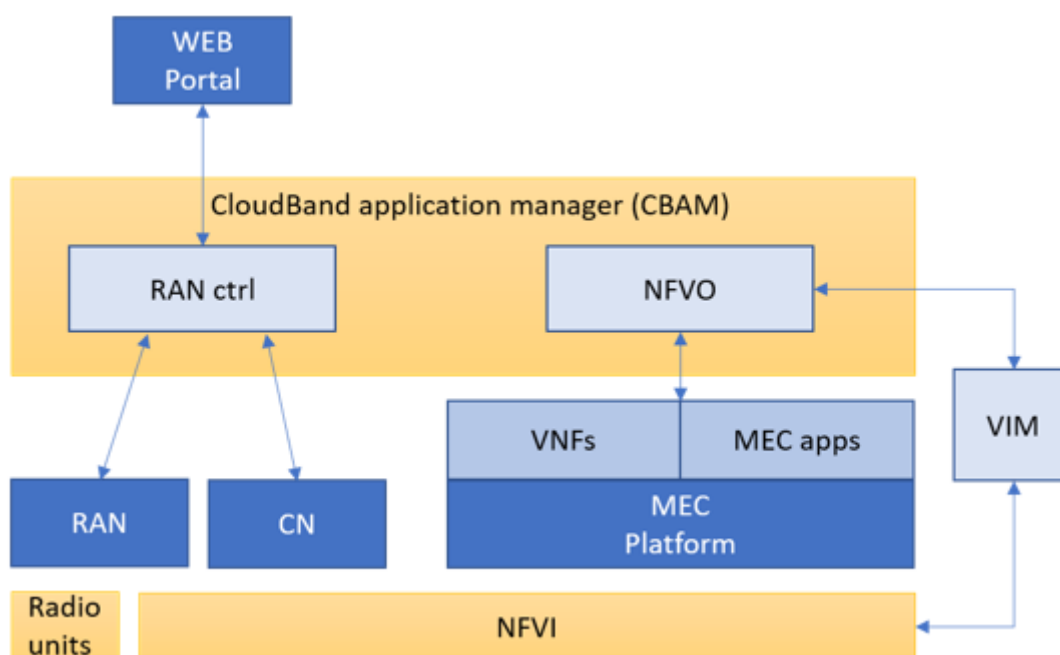


Figure 24 - 5GTN UO network architecture

5.1.2. Network Infrastructure

5.1.2.1. RAN

5GTN has one implementation of 5G NR, provided by Nokia. At the moment, 5G NSA option 3a is supported. 5G SA will be installed as soon as it becomes available which is expected in late 2020. Two Macro eNBs are outside in high mast, with Nokia FRHD and FZQE for 4G. Two Nokia Airscale 5G Macro Cells are installed outside in high mast, with Nokia AEQN. The deployment already supports fully operational 4G LTE and 5G NSA equipment. Inside the UO campus area, there are Nokia eNB Macro Cells in three different locations. The RAN features are summarized in Table 46.

Table 46: RAN components of 5GTN Oulu Platform

Component	Details
eNB (4G)	<ul style="list-style-type: none"> 2 NOKIA Macro eNB at outdoor location (high mast) providing coverage to UO campus area. Several NOKIA “Flexi Zone Multiband Indoor Pico BTS” small cells (3 different locations in UO campus)
gNodeB (5G)	Macro gNB / NOKIA Airscale System for outdoor coverage (high mast in UO campus)
UE	Commercial 4G and 5G mobile phones

5.1.2.2. CN

In 5GTN UO platform, the 4G and 5G Core network functions are deployed at the available NFVIs, in stand-alone servers. The deployment supports the 4G LTE and 5G NR Core implementations (Nokia Cloud Mobile Gateway (CMG)). A CMG instance consists of multiple virtual machines (i.e., MME, SGW, PGW) running on a generic computing infrastructure such as x86 servers. HSS is deployed in another city connected with VPN. UO has its own SIM cards. Each VM is dedicated to a specific set of functions that can be replicated across many similar VMs. A group of VMs is represented as a single instance of an application as they operate in sync with other similar VMs in the group to support a network function. Figure 25 shows the network infrastructure of 5GTN UO, interconnecting the RAN with the CN and External networks (typically Internet).

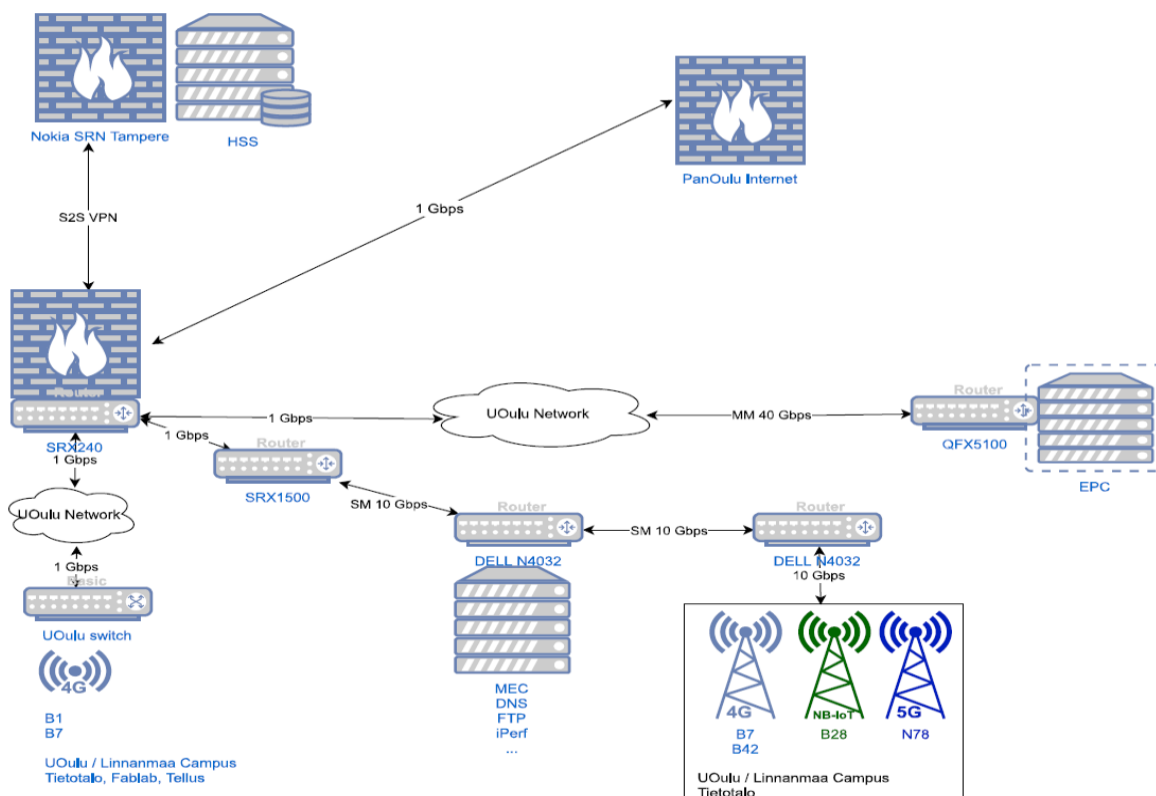


Figure 25 - 5GTN network infrastructure

Note that an evolution toward a Standalone 5G connectivity, i.e. deployment of a full 5G Core, is expected by late 2020.

In line with the Nokia core network used in the network, 5GTN also integrates the network with open source core network solutions. The open source core used in 5GTN include OpenEPC and NextEPC which are basically LTE technologies. 5GTN will have an open source 5GCore added to its network as soon as it becomes available.

5.1.3. Computing infrastructure

5.1.3.1. Cloud and MEC

The MEC server will be used for processing videos, 3D maps, and sending the output back to the control centre and to the trial controller. The MEC operation is set up such that, after the drone takes video, The MEC solution use a multi-media virtual server at the University of Oulu to process the video and transmit it to a multiple output sources. The MEC in 5GTN is a virtual MEC solution from Nokia based on ETSI MEC solution. It consists of an open platform for hosting applications at the edge and supports independent software vendors in developing and testing their applications. As depicted in Figure 27, the Nokia vMEC release is deployable on Nokia AirFrame Rack Mount, and OpenEdge platforms. Hybrid Nokia AirFrame Cloud Infrastructure for Real-time Applications (NCIR) provides the hybrid cloud environment using OpenStack (for VMs) and Kubernetes (for containers). Although University of Oulu have other edge servers running that aren't based on ETSI server, the Nokia MEC Implementation of vMEC is fully based on ETSI standard and the MEC architecture of the 5GTN supports the multi-access edge system reference architecture variant for MEC in NFV.

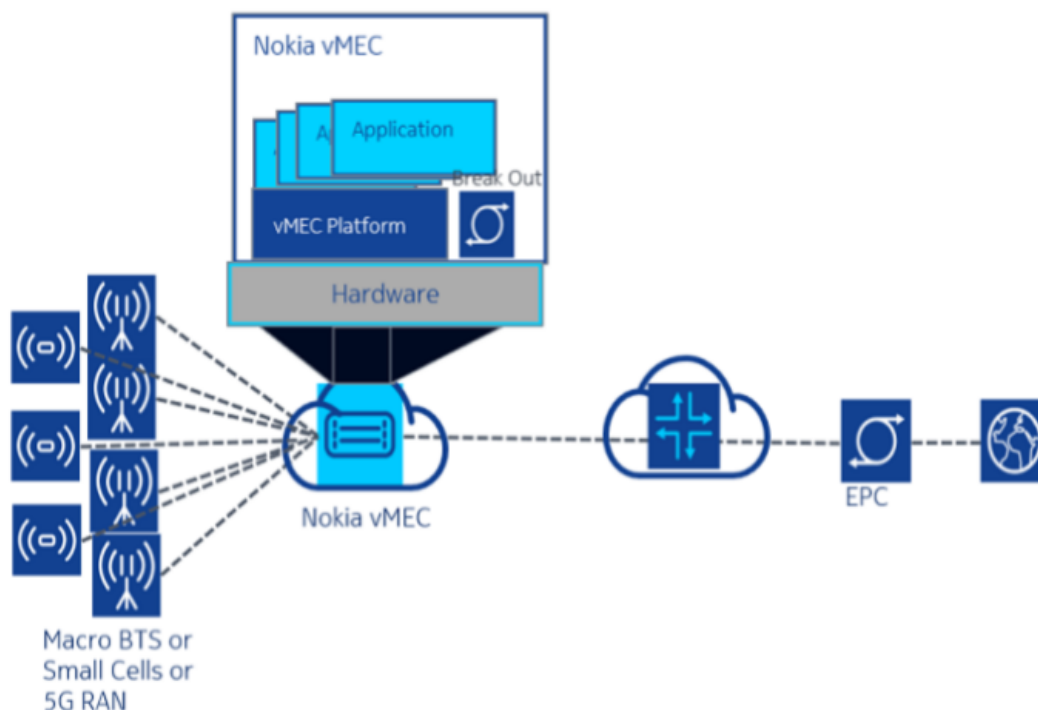


Figure 26 - Overall description of Nokia vMEC used in the 5GTN

5.1.3.1.1. Orchestration framework in MEC

Generally, the MEC supports two orchestration frameworks depending on the virtualization tool:

1. VM (basically KVM) can be orchestrated using the Heat Orchestrator within OpenStack (VIM).
2. Containers can be orchestrated using Kubernetes.
3. The vMEC uses a Hybrid cloud, namely NCIR.

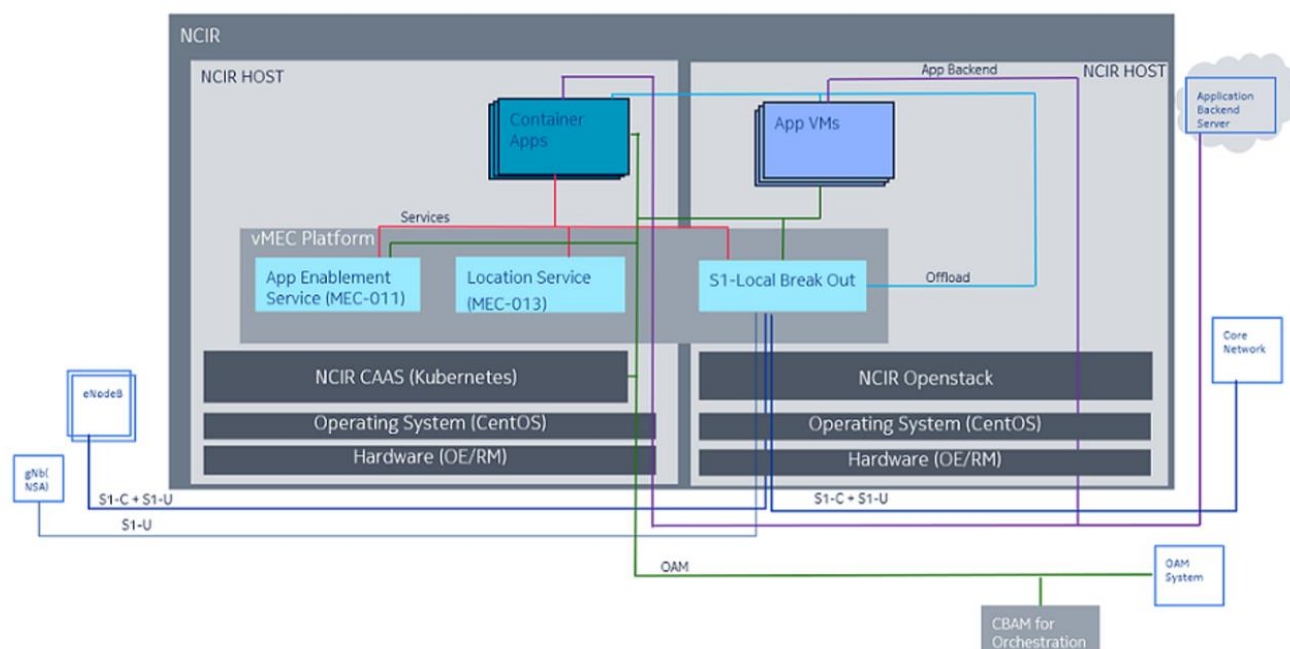


Figure 27 - NCIR architectural display

The MEC NCIR architecture is depicted in Figure 27, and it supports the following:

- For container-based services and applications, orchestration is provided using Helm charts.
- For VM based components, HEAT based templates are used for orchestration. Note also that vMEC platform VM can be orchestrated using Nokia CloudBand Application Manager (CBAM) as well.
- vMEC applications such as Video Analytics (VA 4.0) and Edge Video Orchestration (EVO 4.0) are also orchestrated using CBAM.
- A full support for Micro-Core Network.

5.1.3.1.2. APP deployment in UO vMEC

Application deployment can happen in the CBAM dashboard, which uses the HEAT orchestrator to instantiate a VNF on the VIM, with the help of the CBAM graphical user interface. We can also delete or redeploy VNFs using the GUI directly. The deployment of images in the VIM follows the same standard patterns of OpenStack, and this time it can be done also via the CBAM GUI. Deployment can happen directly at the CBAM GUI, where flavours, networks, nova and glance parameters are described.

The description above is related to the Nokia MEC 19 that is being currently deployed in the University of Oulu. The version deployed at 5GTN at the moment is MEC 17. For deployment and instantiation of

applications, we follow the Nokia approach using the Application Life Cycle Manager (ALCM) which is implemented in TOSCA description. APP VNFD is implemented in ALCM written in TOSCA format as well; similar description but different pattern of writing the code for Heat orchestrator or Kubernetes and it can be used for app deployment on VM or Docker. The basic high-level flow of operation in the ALCM is illustrated in Figure 28.

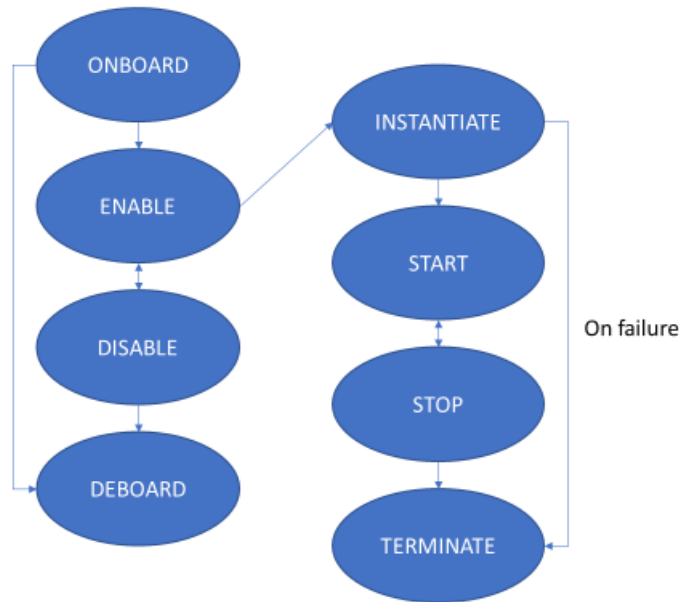


Figure 28 - high-level flow of ALCM operations

For the VM, the basic configuration and flavour is made available. However, a VM is launched using an image already packaged with the required application. To do this, we use the Nokia ALCM application packing approach following the set of techniques below:

- The needed application package is installed already in the VM.
- Then the VM containing the required application is recreated / snapshotted into a new image.
- The new image will launch a VM and automatically starts the application.

We can also package the application in a Docker container and link the source of the Docker when instantiating the VNFD. In the Docker approach, we don't need to recreate the image and we just link the Docker source in the descriptor (VNFD descriptor is different from earlier method)

In general, in the current MEC solution, to instantiate or deploy an application in the MEC, we package the application directly in the VM, we re-create the image, and we use an ALCM VNFD to launch the new VM. Once the VM is instantiated, the application will start automatically. All internal interfaces will also be taken into consideration when repackaging the VM. After the application is packaged in the VM, we use a VNFD based on TOSCA description to launch the VM and subsequently the underlying application.

5.1.3.1.3. Future use of the MEC

Since we are currently using the MEC 17 solution for 5GDrone use case deployment, we will be following the approaches above. However, if the current version is still in use, every use case that needs to be launched in 5GTN and requires a MEC application, needs to follow the following procedures:

- We need to identify the use cases.
- List the number of applications that need to be launched in the MEC.
- Package the application together with the VM and create a new image.
- Use the VNFD approach to launch the VM and application simultaneously.

After deploying MEC 19, we can use the CBAM GUI for an easy deployment and orchestration of applications in the cloud. In MEC 17, the ALCM is responsible for both Docker and VM deployments while in MEC 19, the ALCM is responsible for app deployment in VM over OpenStack VIM, while the application enablement service is responsible for Docker containers in app deployment.

5.1.4. Orchestration and management

For the management and orchestration of VNFs in 5GTN, we used the Open Source MANO (OSM) for VNF deployment, operation and lifecycle management. Since 5GTN has both virtualized open source core network and a sandboxed Nokia core, the orchestration of the virtualized core network VNFs in 5GTN is achieved following the ETSI-NFV architectural standard. OpenStack cloud infrastructure is used as the VIM and VM images are currently based on NextEPC core while we expect the 5G core. The orchestration of VNFs using OSM in 5GTN follows a hierarchical stack such that VMs flavours are described in the VDU and multiple Virtual Deployment Units (VDUs) are described together using the VNFD to get the desired VNF. The instantiation of one or more VNFs is achieved using the NSD. The NSD is launched via an HTTP REST or the OSM client. Each of the descriptors such as the VNFD and the NSD are described in YAML following TOSCA. An example of a VNFD used for the orchestration of VNFs in 5GTN can be seen in Figure 29.

```

1  vnfd:vnfd-catalog:
2    vnfd:
3      - id: spgw_vnfd
4        name: spgw_vnfd
5        short-name: spgw_vnfd
6        description: mme_vnfd_generated for the 5GDrone project containing 2 vdu, one
7        vendor: University of Oulu
8        version: '1.0'
9        mgmt-interface:
10         cp: sgw_S11_mme-mgmt
11
12        connection-point:
13         - name: sgw_S11_mme-mgmt
14           type: VPORT
15         - name: sgw_S5_pgw-data
16           type: VPORT
17         - name: pgw_S5_sgw-data
18           type: VPORT
19         - name: pgw_Gx_pcrf-mgmt
20           type: VPORT
21         - name: pgw_Sgi-data
22           type: VPORT
23
24        ip-profiles:
25         - name: s5
26           description: s5_network
27           ip-profile-params:
28             ip-version: ipv4
29             gateway-address: 0.0.0.0
30             subnet-address: 10.0.1.0/24
31             dhcp-params:
32               enabled: true
33
34        internal-vld:
35         - id: s5_internal
36           ip-profile-ref: s5
37           internal-connection-point:
38             - id-ref: sgw_S5_pgw-data
39               ip-address: 10.0.1.122
40             - id-ref: pgw_S5_sgw-data
41               name: s5_internal
42             short-name: s5_internal
43             type: ELAN
44
45        vdu:
46         - count: 1
47           id: sgw-vdu

```

Figure 29 - VNFD example used in 5GTN

For the network resource monitoring of VNFs, we exposed the resource metrics from the VIM (i.e., OpenStack) using Ceilometer and Gnocchi, and we view the resource parameters using Prometheus, and graphically using Grafana which takes its data from Prometheus. An example of metrics that can be collected from the 5GTN includes the CPU utilization, memory utilization, packets sent, and packets communicated between different VNFs.

5.1.4.1. Network Slicing

Network slicing implementation in 5GTN is carried out using OSM as the orchestrator. In 5GTN the OSM implementation of network slice is based on the end-to-end management technique where the entire slice management and resource orchestration is carried out using OSM. Since OSM is responsible for the orchestration and management of VNFs, the slice implementation falls on the layered hierarchical stack as seen in Figure 30.

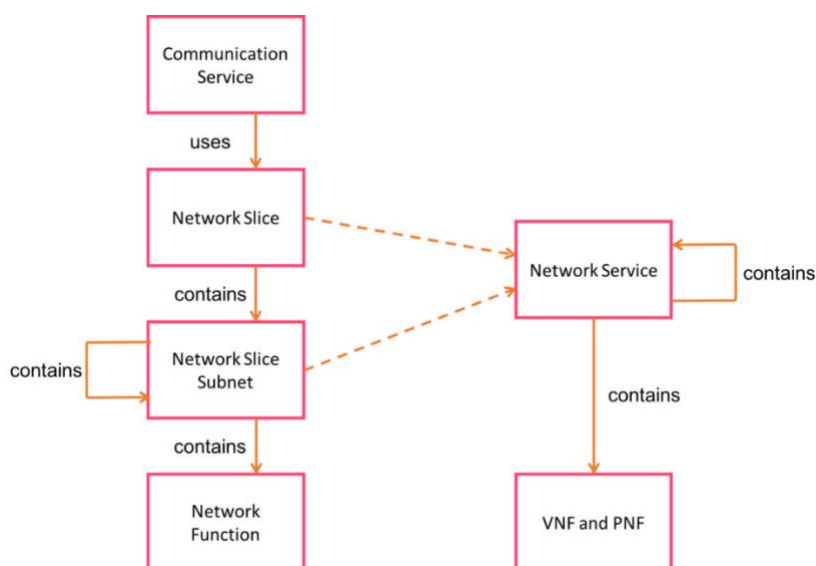


Figure 30 - OSM Hierarchical approach for network slicing used in 5GTN¹⁰

The basis of the virtualized network is made of VMs deployed on top of a NFVI in the cloud (VIM). The VMs are described using a VDU. The VDU depicts the basic information about instantiating the VM in the cloud, such as the VM flavour, VM image, computing capacity etc. Multiple VDUs are described together with a VNFD to instantiate a VNF. Multiple VNFs are combined to describe a Network Service (NS) which is the same as NSSI in the slicing MANO. The NSSI can be instantiated using a NSD and managed by the NSSMF.

Different NS/NSSIs are described together to form a NSI using a Network Slice Template (NST) and managed by the NSMF. Finally, an instantiated NSI is transmitted as a communication service. The NST can be launched via an HTTP REST or the OSM client and the slice template is described in YAML. An example of NST used for the orchestration of VNFs is depicted in Figure 31. Metrics can also be collected during the orchestration of network slices in 5GTN.

¹⁰ https://osm.etsi.org/wikipub/index.php/OSM_Scope_and_Functionality

```

shared_slice.yaml
1  #NST for shared slice with middle NSSI being shared with new NSSIs
2  nst:
3  - id: slice_shared_nstd
4    name: slice_shared_nstd
5    SNSSAI-identifier:
6      slice-service-type: eMBB #this can be eMBB, uRLLC or mMTC
7    quality-of-service:
8      id: 1
9
10   netslice-subnet:
11
12   - id: left_non_shared_nsd
13     is-shared-nss: 'false' #no sharing of this resource
14     description: NetSlice Subnet (service) composed by 1 vnf with 2 cp
15     nsd-ref: left_right_nosha_nsd
16   - id: middle_sharing_nsd
17     is-shared-nss: 'true' #sharing of this resource
18     description: NetSlice Subnet (service) composed by 1 vnf with 3 cp
19     nsd-ref: middle_shared_nsd
20   - id: right_non_shared_nsd
21     is-shared-nss: 'false' #no sharing of this resource
22     description: NetSlice Subnet (service) composed by 1 vnf with 2 cp
23     nsd-ref: left_right_nosha_nsd
24
25   netslice-vld:
26   - id: left_middle_vld
27     name: left_middle_vld
28     type: ELAN
29     nss-connection-point-ref:
30       - nss-ref: left_non_shared_nsd
31         nsd-connection-point-ref: nsd_cp_mgmt
32       - nss-ref: middle_sharing_nsd
33         nsd-connection-point-ref: nsd_cp_mgmt
34   - id: middle_right_vld
35     name: middle_right_vld
36     type: ELAN
37     nss-connection-point-ref:
38       - nss-ref: middle_sharing_nsd
39         nsd-connection-point-ref: nsd_cp_mgmt
40       - nss-ref: right_non_shared_nsd
41         nsd-connection-point-ref: nsd_cp_mgmt
42
43   - id: left_middle_vld
44     name: left_middle_vld
45     type: ELAN
46     nss-connection-point-ref:
47       - nss-ref: left_non_shared_nsd
48         nsd-connection-point-ref: nsd_cp_data

```

Figure 31 - NST example used in 5GTN

Some of the limitations with OSM orchestration for network slicing include the following:

- 1) Currently, we have network slice instance with defined slice service types (i.e., eMBB, uRLLC, mMTC slice) in the network slice template, however, the defined slice service type is actually not implemented in the slice, and it's just defined. To implement those slice service types on core network functions for instance, we need the right VNF placement approach. We also need to use juju proxy charm (supported by OSM) for automating specific VNFs (EPC or 5GC) in order to create the required slice.
- 2) The separation of slice selection between access and core network functions is not available at the moment.
- 3) The separation of slice management for each layer is currently not available. i.e., having NSSMF for NSSI, or NSMF for NSI, or CSMF for communication service is not available.

Most of these limitations will be investigated during the course of the project and they will be implemented at the start of the trial's execution. We also plan to use the standalone management for network slicing where we can separate slicing management and orchestration from the resource management and orchestration following the Vanilla SOL005 API.

5.1.5. Security features in 5GTN

Nokia EPC and vMEC use secure protocols to provide confidentiality, integrity, and authentication based on keys and certificates, whereas a security protocol such as SSH and Internet Protocol Security (IPSec) are used for authorization and verification. Figure 32 depicts an overview of security in 5GTN, with each component detailed in the following sub-sections.

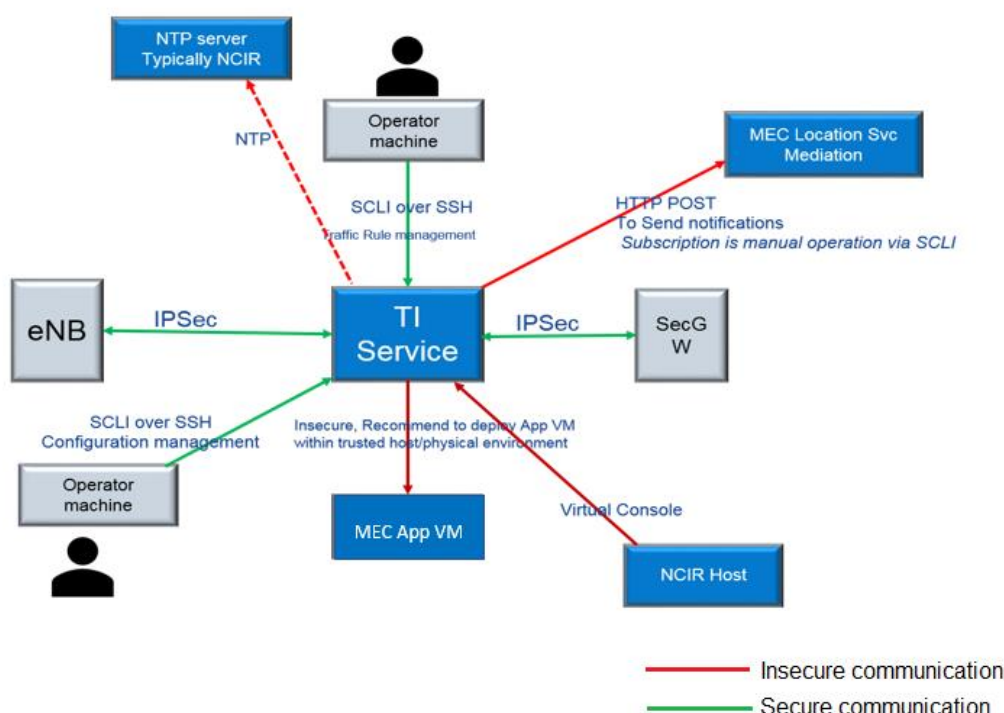


Figure 32 - Overview of 5GTN security

5.1.5.1. Firewall

Firewalls in EPC and vMEC platform are configured such that only the necessary ports are opened for communication. This ensures that the unnecessary traffic does not enter the EPC and vMEC platform. Also, there is a restriction on the traffic that can leave the EPC and vMEC platform.

5.1.5.2. SSH

SSH is the only protocol supported for the operator to access vMEC for operations and management. The SSH server does not allow remote access with the root account. The SSH server allows using SFTP (an SSH subsystem) and SCP for file transfers. Table 47 details the IKEv2 profiles used for LTE SSH in 5GTN.

Table 47: IKEv2 profiles for LTE SSH

Function	IKEv2
Encryption/ciphering algorithms	AES128-CTR, AES192-CTR, AES256-CTR
Key exchange	DIFFIE-HELLMAN-GROUP-EXCHANGESHA256
Integrity protection algorithm	HMAC-SHA1, HMAC-SHA2-512, HMAC-SHA2-256

5.1.5.3. IPSec

From the external connectivity point of view, IPSec tunnels are connected towards eNBs/gNBs and to the overall operator's core network. eNBs/gNBs can possibly connect to the core network security gateway directly using the secondary IPSec tunnels (in dotted lines) which get activated in case of failure of the one primary tunnel towards vMEC platform and MEC applications. The following figure shows the connectivity while IPSec tunnel is in use.

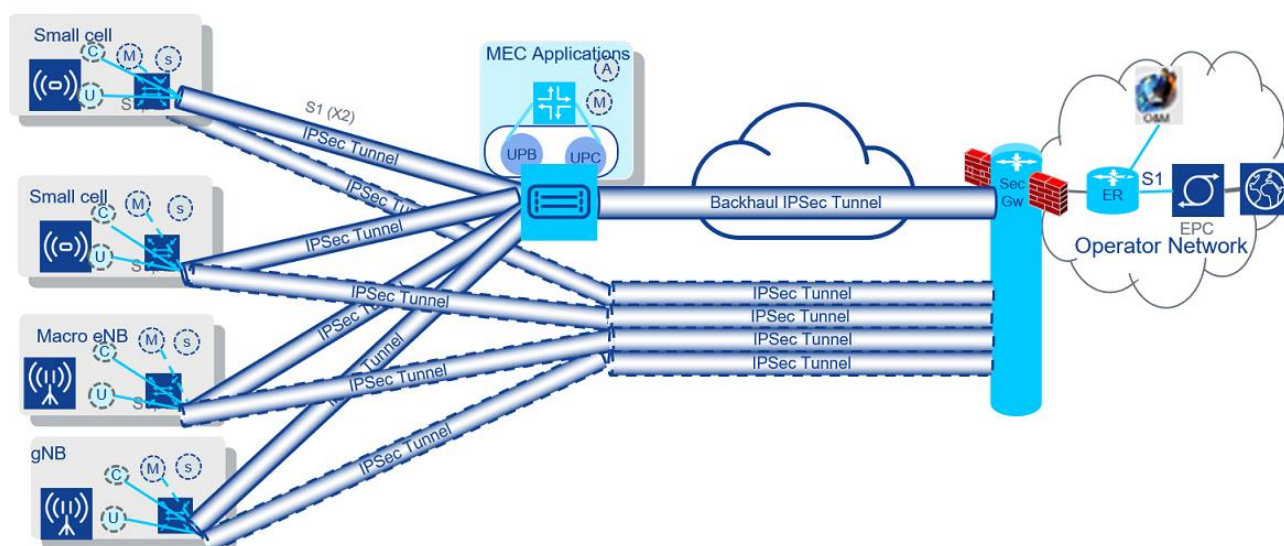


Figure 33 – vMEC IPSec connectivity

vMEC platform supports IPsec in tunnel mode. The interfaces to eNB/gNB and core network can optimally be secured using IPsec. vMEC platform supports multiple IPsec tunnels in the RAN or core network and also supports IPsec tunnels to multiple eNBs/gNBs simultaneously. In addition to supporting the user plane data and control plane Stream Control Transmission Protocol (SCTP) messages, the IPsec also provides security for the management plane communication. The vMEC platform encapsulates all traffic into IPsec in tunnel mode, using Encapsulated Security Payload (ESP). Encryption and integrity protection algorithms can be selected from the algorithm list. vMEC platform supports both policy and route-based VPN protocols for IKE versions 1 and 2 to setup a security association. IKE authentication is based on digital signature certificate. Operator's digital certificates of X.509v3 format are enrolled using Certificate Management Protocol (CMP) based certificate management framework to the system to support secure Operation, Administration, and Maintenance (OAM) connection. Table 48 highlights different IKEv2 profiles for LTE IPsec used in the 5GTN.

Table 48: IKEv2 profiles for LTE IPSec

Function	IKEv2
Services	Data Integrity Protection, Origin Authentication and Anti-Replay Protection, Confidentiality
Protocol	ESP
IPSec mode	Tunnel mode
Encryption/ciphering algorithms	3DES (3DES encryption algorithm), AES-128-CBC (AES 128 bit encryption algorithm), AES-128-GCM (AES-128-GCM16 encryption algorithm), null (non-encryption)
IKE Encryption algorithms	3DES-192-CBC (3DES-192-CBC encryption algorithm), AES-128-CBC (AES-128-CBC bit encryption algorithm), AES-128-GCM (AES-128-GCM16 encryption algorithm)
Authentication type for IKE negotiation IKE phase	X.509 certificates, Secret (pre-shared keys for authentication)
Authentication algorithm for IKE negotiation IPsec phase	HMAC-MD5 (MD5 authentication), HMAC-SHA1 (SHA1 authentication), AES-128-GCM16 (AES-128-GCM16 authentication), HMAC-SHA256 (SHA256 authentication)
Pseudo-random function	HMAC-SHA1
Key exchange	RFC 4306
Diffie-Hellman group	1, 2, 5, and 14
Hash algorithms for IKE negotiation IKE phase	HMAC-MD5 (MD5 authentication), HMAC-SHA1 (SHA1 authentication), HMAC-SHA256 (SHA256 authentication)

5.1.5.4. Separation of traffic classes

Traffic classes in 5GTN and vMEC are separated to increase the level of security and prevent interference among them. The following are the different traffic classes supported:

- User plane traffic
- Control plane traffic
- OAM plane traffic

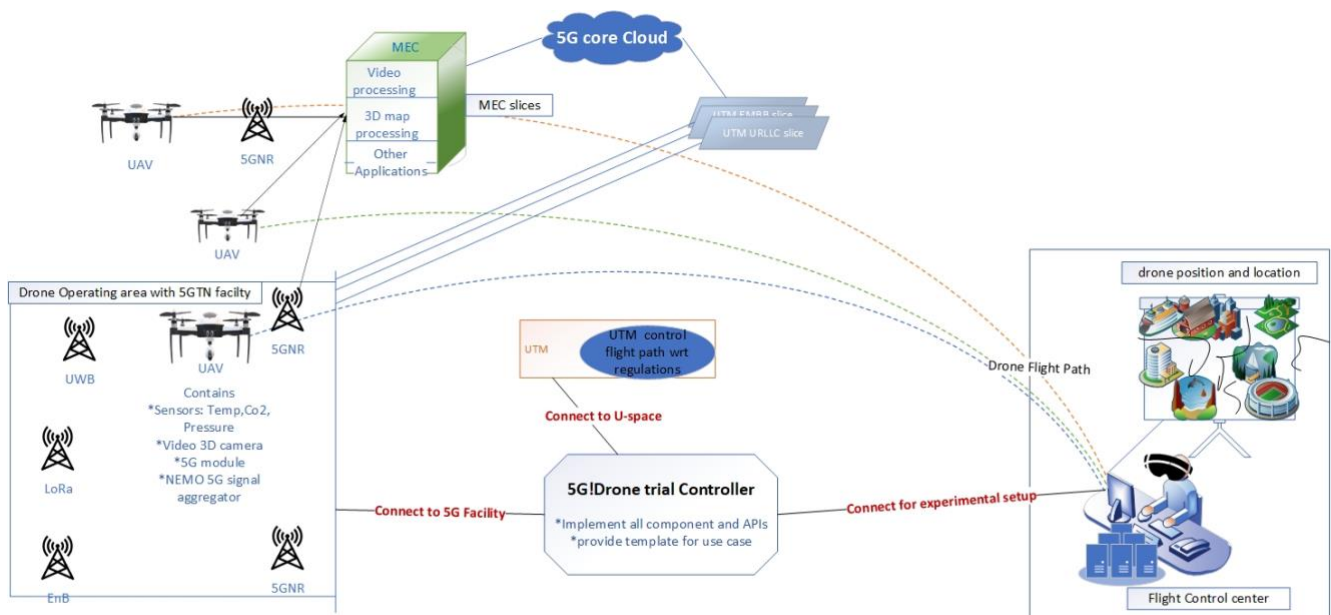
The traffic offload to the vMEC applications is not encrypted. It is expected that the communication between UE and vMEC application happens in a trusted environment and/or there will be end to end encryption of traffic using protocols like HTTPS.

5.2. Facility interaction with the trial controller for use case deployment

5.2.1. Deployment of a Trial

From the 5G facility perspective, all the trials will be deployed as a network slice in 5GTN. This means that the trial needs to be described in a form of a slice template highlighted in the previous section. As stated earlier, the slice can be instantiated either via the HTTP REST API or via the OSM client. In order to automate the instantiation of slices in 5GTN, the required interface between the trial controller and the 5GTN needs to be established and then the slice can be instantiated.

For the deployment of use cases in 5GTN, we will follow the approach highlighted in section 3.3.11. of deliverable D1.1 [2], whereby the deployment is done in four stages after the trial is started in the facility. The stages include, the preparation stage, the preliminary flight stage, the flight stage, and the analysis and reporting stage. Using the deployment architecture in Figure 34 for the representation of use case deployment in 5GTN, the sequence diagram in Figure 35 will highlight all the stages of deployment of a use case based on that architecture.



Use case Deployment in 5GTN

Figure 34 - Use case deployment architecture in 5GTN

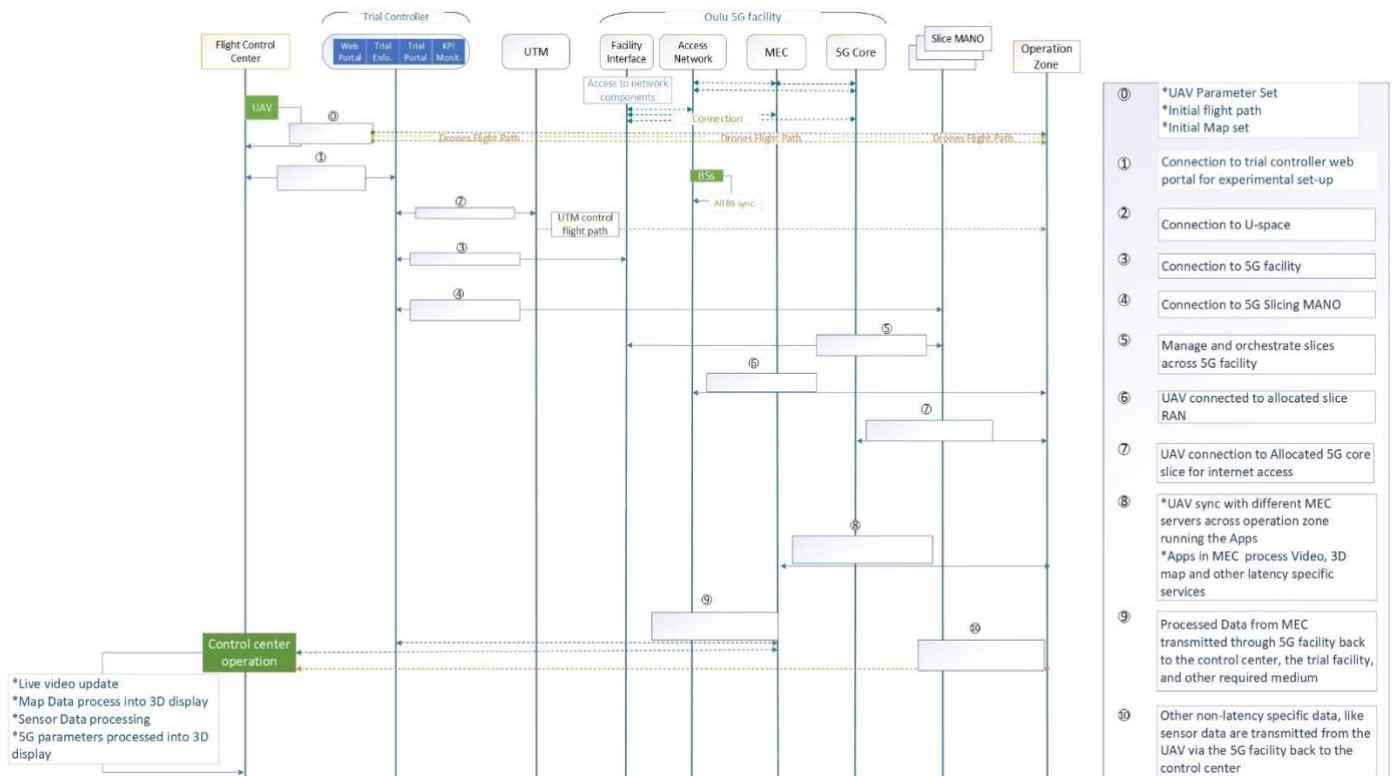


Figure 35 - Sequence diagram for trial deployment in 5GTN

5.2.2. KPI Metrics

The sequence diagram in Figure 35 represents the flow of operation from the control centre to the operation centre. From the sequence diagram, we can see that different KPIs metrics can be required at different stages of the scenario operation. In this description, we are setting overall view of what KPI metrics can be measured during the deployment of a trial in 5GTN.

KPIs to be collected at the preparation stage (0 and 1 from sequence diagram): The following set of KPIs can be collected during the preparation stage of the trials;

- a) Deployment time: Drone deployment time from the control centre, this time will include the service preparation time at the control centre. The idea of this performance metric is to ensure that not much time is used for starting the operation.
- b) Control centre metrics can include, number of drones, possible number of instantiations, rate for map update, speed/BW for translating the received streams.
- c) Processing condition: After the reception of video streams or general app updates data from the MEC, KPI metrics will be collected to know the speed of processing this into the 3D display. Example of KPIs to be measured includes the latency of processing applications in the MEC or edge server.

KPIs within the trial controller (2, 3, and 4 from sequence diagram) will be described in WP2 deliverable D2.1.

KPIs within the 5GTN (5, 6, 7 and 8 from the sequence diagram):

For the 5GTN proprietary 5G network KPI metrics can be collected across different components in the network as seen in the 5G architecture. The metrics that can be measured include latency, bandwidth, and throughput. For example, KPI values for 3D mapping use case scenario to be trailed in the 5GTN facility are given as:

- a) Capacity > 100mbps (maximum capacity can be seen in the network topology above)
- b) Latency for the whole network < 10ms
- c) Latency to the MEC < 1ms

For the MEC server in 5GTN, different metrics can be measured such as the latency, bandwidth, and throughput between the 5G User-Plane functions and the MEC during traffic redirection to the MEC applications. However, one of the most important components that affects the KPIs in the MEC server is the multi-media application itself i.e. the processing operations of the applications in the MEC. Hence, KPIs in the MEC will be specific to the MEC application. For example, a video processing APP like NGIX, must take a processing time < 3ms per video stream from the drone camera while for the map processing, latency < 5ms per received map update.

KPIs within the Open source virtualized EPC in 5GTN:

Since 5GTN uses open source solutions such as NextEPC and OpenEPC, OpenStack cloud infrastructure, and OSM orchestrator, their own KPI metrics can be measured and added to the 5GTN list of KPI metrics. Each network component makes up the EPC VNFs and hence we can have specific KPI metrics for their instantiation in the cloud. Basically, the KPI metrics that can be measured between the VNF components include the following: CPU utilization, Memory utilization, rate of packets sent between VNFs, rate of packets received between VNFs, calculation of latency of operation between components, capacity, and throughput.

KPI Metrics can be collected via monitoring tools like Prometheus or Grafana. Table 49 summarizes the list of KPIs currently available for measurement in 5GTN.

Table 49: KPIs available for measurement in 5GTN

KPI Metrics	Level	Details
Network Capacity	RAN/CORE	<p>Reach a peak use data rate between 50Mbps and 1Gb/s for specific deployment scenarios and use cases for each user supported in the system. The 50 Mbps as a minimum target value is in line with the 3GPP targets that foresee ~30 Mbps uplink data rate for a 4K video streaming, without audio</p> <p>1000 times higher mobile data volume per geographical area. 10 to 100 times more connected devices.</p>
Overall Latency	RAN/CORE	<p>Latency is important for the accurate control of the UAV in the case controlling it over the mobile network (e.g. with 5G radio interface). Considering that various parameters may influence the KPI value, such as the height and the speed of the drone, an average case for control latency requires 10 ms delay according to the 3GPP target values for different services, such as 8K video live broadcasting, Laser mapping and HD patrol surveillance and remote UAV controller through HD video. Considering also the URLLC capabilities of 5G networks, 5G end to end latency should be less than 1ms.</p>

Service creation time/Trial deployment time	NFVO	Service creation time / Trial deployment time from the control centre, this time will include all service preparation time at the control centre. The idea of this performance metrics is to ensure that not much time is used for starting the operation.
Control centre metrics	Trial controller	Control centre metrics can include, number of drones, possible number of instantiations, rate for map update, speed/BW for translating received streams
Processing metrics	MEC	Processing metrics include KPI that can be collected when use case outputs are being processed. For example, after reception of video stream data from the MEC, KPI metrics will be collected to know the speed to processing this into the 3D display, KPI to be assessed include processing time of video stream, time of processing application
VNF related Metrics	NFVO	This include KPI metrics that can be acquired due to the use of 5G VNFs. Metrics that can be collected include the CPU utilization, memory utilization, Rate of packet sent/received between VNFs, VNF instantiation time, etc.
Trial operational metrics	Trial controller	This include KPI metrics that can be measured during the operational phase of the trial. For example, metrics include the synchronization time of different radio to be used (UWB, eNB, 5GNR,etc)
UAV related metrics	Trial controller	This include all form of metrics that can be collected from the UAV deployment.

5.2.2.1. Web portal

At the moment, there is a web portal solution for the configuration of network components in 5GTN. However, this solution is based on Nokia CBAM interface that is shown in the network architecture in Figure 25. Due to the proprietary nature of the Nokia solution, the web portal cannot be used in the context of the 5G!Drones project as it does not allow direct modifications to support 5G!Drones trials deployments and configuration in 5GTN. As a consequence, a new web portal for the implementation of 5G!Drones trials in 5GTN will be developed to support the features required.

5.2.2.2. Northbound API

Table 50 shows the list relevant to the NBI, allowing the management of the life-cycle of a network slice running on top of 5GTN. The Northbound interface is based on REST and it allows performing actions over the following entities: tenant, VNF, VIM, NSD, NST and NSI, as listed in the table.

Table 50: NBI of the SO in 5GTN

API	Details
vnf_instances (tenant_id)	Return the list of VNFs of a specific tenant. The 'tenant_id' can be replaced by 'any' to obtain the list for all tenants.
vnf_instances (tenant_id, vnf_id)	Returns the information of a specific VNF. It lists the virtual machines which compose the VNF.
deletevnf(tenant_id , vnf_id)	Deletes a VNF from the database, and images and flavours in VIM when appropriate. The parameter 'tenant_id' can be replaced by 'any' when the VNF belongs to other tenants.
vnf_packages(tenant_id)	Returns the list of all VNF descriptors.
vnf_packages(tenant_id, vnfd_id)	Returns the information of a specific VNF descriptor.
ns_descriptors_content(nsd_id)	Returns the content of a specific network service descriptor.
ns_descriptors()	Return the list of all network service descriptors.
netslice_templates_content(nstid)	Returns a specific network slice template
ns_instances()	Returns all the available network services
createSlice (nsiid, NST)	Instantiate the associated NST in the facility
listSlices()	Returns all the available slices
updateSlice(nsiid, nstid)	Update the resources of a slice

5.3. Detailed mapping of use case scenario components to the 5G facility

5.3.1. UC1 scenario 2 - 3D mapping and supporting visualization/analysis software for UTM

This scenario leverages on a set of enabling technologies to visualize the real time operation of drone fleets using VR as a visualization platform, and diverse sources of data relying on 3D mapping. The scenario studies also the possibility of using VR for drone operation and real time visualization.

The main objective of the scenario is to help the UAV operator to determine the best physical and 5G service conditions for flying the drones, in terms of terrains and environmental factors such as temperature, and pressure, as well as 5G measurements such as latency, signal quality, and bandwidth for video transmission. Figure 36 depicts the scenario components and how they are mapped to 5GTN resources. Note that the aim here is to focus on the network connectivity and computation requirements, which can be provided by 5GTN. UAV hardware & software overview are described in what follows. In that regard, there are two deployment options for this scenario. The first one consists of leveraging on the capabilities of ETSI MEC 19 using NOKIA vMEC. The main services required for the operation of this scenario will be running on the MEC within 5GTN, as depicted in Figure 36.

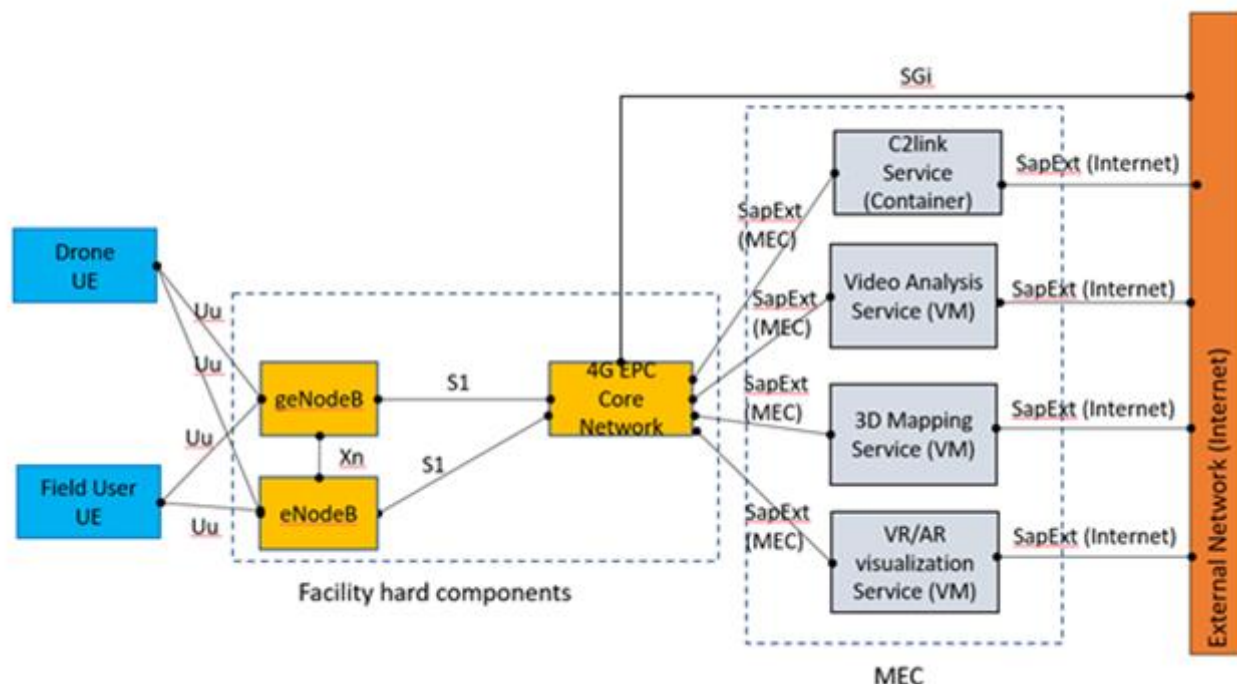


Figure 36 - UC1 scenario 2- Functional components and their mapping to the facility in the first deployment option

The second option will consist of using edge devices to perform most of the functionalities of the scenario, as illustrated in Figure 37. The main component in the software side is the Robot Operating System (ROS), which is used to handle software node interconnections. ROS is the “glue” that attaches all the sensors and control hardware on-board the UAV to the data processing and control algorithms. In the ROS system, each sensor and algorithm has its own processing node that communicate with each other by publishing and subscribing to data streams, called topics in the ROS system. Establishing connections between different software nodes is handled by a ROS Master package (roscore), which runs a stateless XMLRPC HTTP-based server on top the TCP/IP stack, controlling the communication establishment and monitoring between nodes. For data recording purposes, ROS also includes roscord and rosbag packages to record any data being handled by the ROS system in to binary data files called rosbags. All the recorded ROS messages are timestamped, so that rosbag data can be replayed later as it was when being recorded. The most important ROS software nodes in this use case are the UAV control node, the sensor nodes for reading sensors, like the ones used for cameras and localization, data processing nodes for mapping, object detection, and simultaneous localization, node for navigation handling, collision avoidance, and UAV movement, and the edge network / external database access node handling communications between the UAV and any external computational and control related resources.

In Figure 37, the UAV control node transforms commands issued in ROS and communicates with the UAV flight control unit (FCU) via MAVLINK protocol for Pixhawk FCU based UAVs, or DJI's protocol for DJI based UAVs. Mapping, object detection and localization nodes handle the production of the coarse, light weigh, point cloud of the environment in to a 3D occupancy grid map using the OctoMap framework. Object detection is handled by a deep learning neural network, currently based on the YOLOv3 implementation, from camera streams and localized based on depth and UAV tracking sensors. UAV localization can be based on the UWB localization, SLAM, or other methods, depending on the availability and processing power. For navigation & collision avoidance, the data produced by the aforementioned approaches can be fused in to the same reference frame using ROS transform trees with the ROS tf2 transform library package. All the processed data can be sent over the 5G network to the edge servers / cloud applications via the edge network access & database management node, for example, to the UAV control application implemented in the VR environment. The navigation

& collision avoidance node handles the on-board collision avoidance and UAV movement, based on the control and support data received from the robot mission control applications at the edge network.

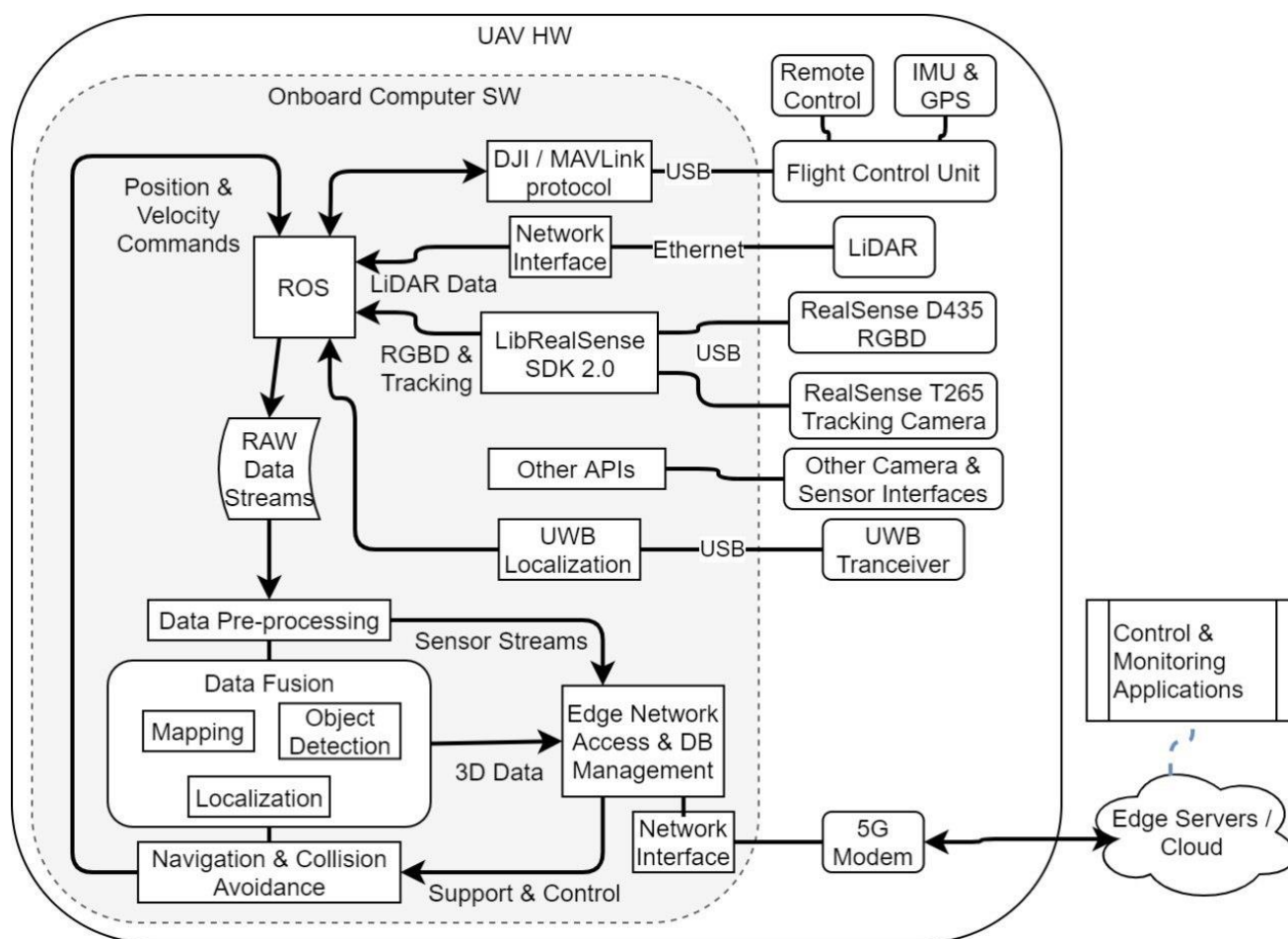


Figure 37 - UC1 scenario 2- Functional components and their mapping to the facility in the second deployment option

In the current ROS implementations, although the ROS node communication is all implemented on top of the TCP/IP stack, making it possible to run any ROS node anywhere in the network the ROS master is running in, in practice the software nodes represented in Figure 37 can only run locally on-board the UAV because of very strict reliability and latency requirements between the components. Also, only one ROS master can exist in a common network at a time, so the crucial nodes on-board the UAV only communicate through the localhost, as losing any node during operation would be catastrophic to the functioning of the UAV. However, the object detection, mapping and localization nodes can be made to utilize edge services so that, for example, object detection and semantic information-based mapping related processing could be handled in cloud-based applications. Also, the edge services / control applications can facilitate maintaining of the real-time environment model, that the UAV's navigation and task planning algorithms can use as a support data source. From the control perspective, the edge network services / control applications would be used to handle controlling multiple UAVs in a common air space and relay information between autonomous UAVs / robots.

The facility hard components, UEs, sensory equipment, and software are detailed in the following tables.

Table 51: UC1 scenario 2 UAV components

UAV Components	Type (Hw/Sw)	Partner
UWB localization beacon	Hardware	Nokia
	Software	Nokia
Cable Drone	Hardware	UO
DJIM210 Drone	Hardware	UO
NVIDIA Jetson embedded computer	Hardware	UO
network switch Ethernet	Hardware	UO
Laser scanner Velodyne Puck 17	Hardware	UO
Intel real sense depth camera	Hardware	UO
Axis wide angle camera	Hardware	UO
UWB Tag	Hardware	UO
XSense IMU for orientation	Hardware	UO
5G UE	Hardware	UO
SLAM and 3D reconstruction	Software	UO

Table 52: UC1 scenario 2 UAV operator components

UAV Operator Components	Type (Hw/Sw)	Partner
Indoor localization system	Hw	CAF
	Sw	CAF
SLAM and 3D reconstruction	Software	UO
NETWORK STORAGE drive	Hardware	UO
Game PC with high performance GPU	Hardware	UO
Valve Index VR headset	Hardware	UO
VR visualisation	Software	UO, NOKIA

Table 53: UC1 scenario 2 UTM components

UTM Components	Type (Hw/Sw)	Partner
Support for dFPL (drone Flight Plan). Situational awareness (airspace perspective) service to submit dFPL.	SW	DRR, FRQ
U-space telemetry endpoint	SW	DRR, FRQ

Table 54: UC1 scenario 2 other components

Other Components	Short description	Type (Hw/Sw)	Partner
UWB localization receiver	Reference location point in the test area	Hardware Software	Nokia Nokia
UWB beacons	- 3 different systems for comparison	Hardware	UO, NOKIA
UWB pose triangulation		Software	CAFATECH/UO/NOKIA
Reference location		Hardware	CAFATECH/UO/NOKIA

5.3.2. UC2 scenario 3 - Police and counter-UAS

This use case will demonstrate how a remotely piloted UAV and video analytics can be used for police tasks, including C-UAS activities using 5G communication.

The police are preparing for a VIP visit. The police drone delivers an area scanning IoT camera to the roof of a building which is located at the centre of the risky area (hereinafter main building). The camera based on IoT LTE Cat-M1 technology sends photos and video clips of any suspicious movements to police video analyser software.

The police also use a drone that automatically flies and streams 4K video to the video analyser software and the command centre. The video analysing software installed on the MEC uses videos and photos provided by the IoT cameras and drone. It also sends the gathered data to the central servers of the police.

As a part of the VIP visit, a temporary No Fly Zone (NFZ) is established. During the visit, the police drone detects an intruder drone in the NFZ. To stop the intruder drone, a human operator in the police control centre starts a remotely piloted flight of the police drone. At the same time, AI (computer vision software) notices a suspicious person with a drone remote controller near the main building. The remotely piloted drone then flies near the suspicious person and affects the pilot to stop the illegal activity.

Figure 38 shows the UC2 scenario 3 components and how they are mapped to facility resources. Note that the aim here is to focus on the network connectivity and computation requirements, which can be provided by the facility.

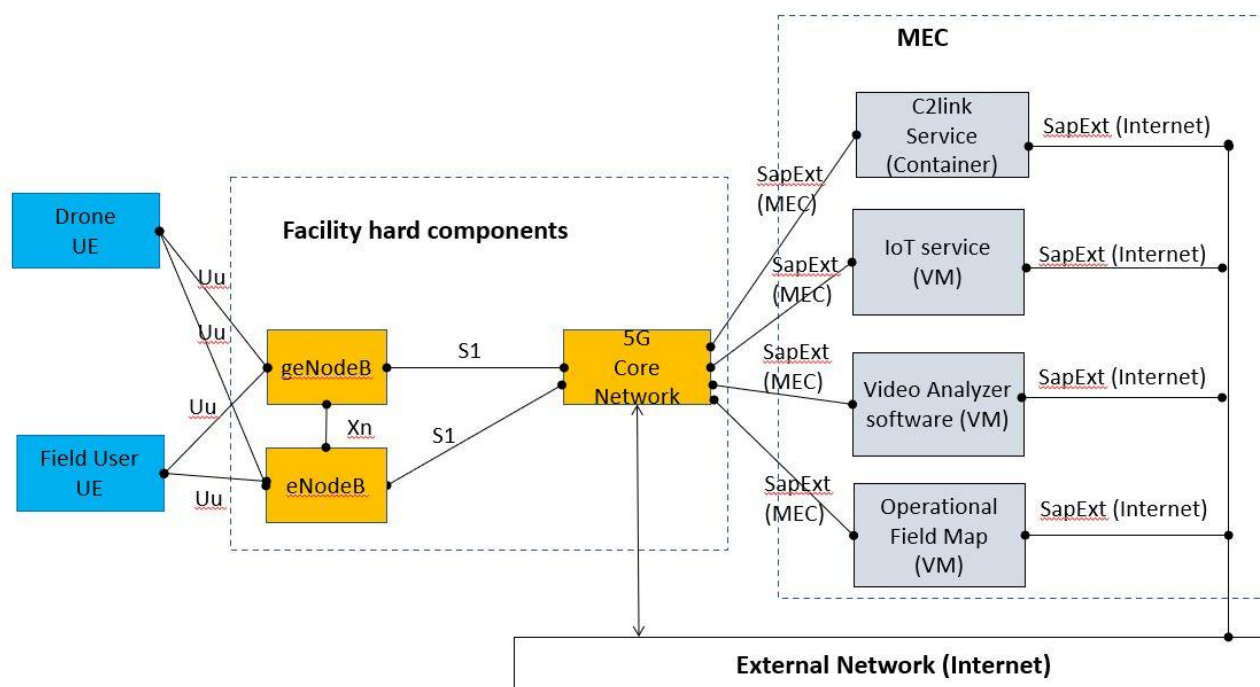


Figure 38–UC2 scenario 3 - Functional components and their mapping to the facility

The facility hard components are those already deployed at the facility, and enable 5G connectivity via the NSA mode. The tables below summarize the partners in charge of providing each component for the trial of UC2 scenario 3.

Table 55: UC2 scenario 3 UAV components

UAV Components	Type (Hw/Sw)	Partner
DJI Mavic	Hw	CAF
DJI Matrice	Hw	CAF

Table 56: UC2 scenario 3 UAV operator components

UAV Operator Components	Type (Hw/Sw)	Partner
CAFA C2 Ground Control Dock (communicates between 5G MEC based CAFA CUP and drone)	Hw	CAF
Laptop for communicating MEC based CAFA CUP	Hw	CAF
5G MEC based CAFA CUP C2 software	Sw	CAF

Table 57: UC2 scenario 3 UTM components

UTM Components	Type (Hw/Sw)	Partner
In the strategic phase, the definition and dissemination of NoFlyZone to the CIS, about airspace restriction	SW	DRR, FRQ
Support for dFPL submission	SW	DRR, FRQ
Mission prioritization support	SW	DRR, FRQ
U-space telemetry endpoint	SW	DRR, FRQ

Table 58: UC2 scenario 3 5G components

5G Components	Type (Hw/Sw)	Partner
5G UE (smartphones) for CAFA Dock and for DJI Mavic/Matrice	Hw	OU, CAF
5G UE for laptop	Hw	OU, CAF

Table 59: UC2 scenario 3 other components

Other Components	Short description	Type (Hw/Sw)	Partner
PC with high performance GPU		Hw	CAF
Cat M1/M2 IoT device for surveillance	To provide photos from hotspot	Hw	CAF
CAFA IoT software	C2 soft for controlling IoT device	Sw	CAF
CAFA Video Analyzer	5G MEC based video analytics solution	Sw	CAF
Police Command Center and Operational Field Map	CAFA Tech Operational Field Map	Sw	CAF

5.3.3. UC3 scenario 1 Sub-Scenario 1 -3D Mapping of 5G QoS

This use case will demonstrate how 5G QoS mapping is done using 5G MEC based on software for measuring 5G QoS the communication company ordered from a drone company for the 3D mapping of

5G QoS. At first, the drone (DJI Mavic) take photos which are then processed into a 3D map. This is followed by placing the 5G base stations on the 3D map.

The drone then carries 5G communications equipment to measure the quality of 5G coverage from various positions with 3D coordinates (x, y, z). During the measuring process radio base station signal parameters (directions and strength etc.) will be changed. Measuring results are transferred to the server and then results visualised on the 3D Map.

Figure 39 shows the UC3 scenario 1 sub-section 1 components and how they are mapped to facility resources.

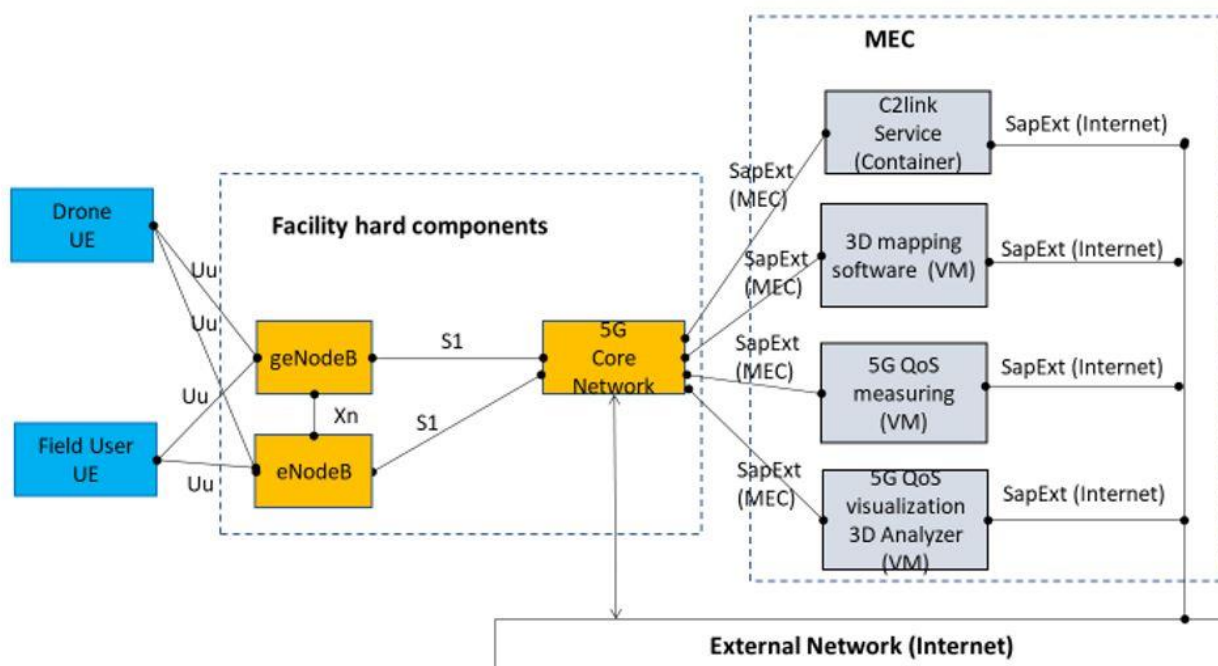


Figure 39 - UC3 scenario 1 sub-scenario 1 - Functional components and their mapping to the facility

The facility hard components, UAV, UTM as well as software will be described in the tables below.

Table 60: UC3 scenario 1 sub-scenario 1 UAV components

UAV Components	Type (Hw/Sw)	Partner
DJI Mavic	Hw	CAF

Table 61: UC3 scenario 1 sub-scenario 1 UAV operator components

UAV Operator Components	Type (Hw/Sw)	Partner
CAFA C2 Ground Control Dock (communicates between 5G MEC based CAFA CUP and drone)	Hw	CAF

Laptop with 5G device for communicating MEC based CAFA CUP	Hw	CAF
5G MEC based CAFA CUP C2 software	Sw	CAF

Table 62: UC3 scenario 1 sub-scenario 1 UTM components

UTM Components	Type (Hw/Sw)	Partner
Interface to upload to the UTM/U-space system information about RAN 3D coverage in time with SLA	SW	DRR, FRQ

Table 63: UC3 scenario 1 sub-scenario 1 5G components

5G Components	Type (Hw/Sw)	Partner
5G UE (smartphones) for CAFA Dock and for DJI Mavic	Hw	OU
5G UE (smartphone) for laptop	Hw	CAF

Table 64: UC3 scenario 1 sub-scenario 1 other components

Other Components	Short description	Type (Hw/Sw)	Partner
PC with high performance GPU	For running 3D mapping and 3D Analyzer software	Hw	CAF
3D mapping software (5G MEC based)	Processing 3D map from drone photos	Sw	CAF
5G QoS measuring software	Measuring signal quality with xyz coordinates information	Sw	CAF
CAFA 3D Analyzer	3D Analyzer for showing 5G QoS measurements	Sw	CAF

5.3.4. UC3 scenario 1 Sub-Scenario 2 -Long range power line inspection

The purpose of this sub-scenario is to demonstrate how UAVs could be used in well-connected 5G urban areas for power line inspection and fault detection. This is an essential and time critical service, which can greatly benefit from the advantages of 5G networks. For example, there is a power outage because of a strong storm. Currently, drones are used in VLOS operations where the UAV collects large amounts of data using LIDAR and cameras which is later analysed. This kind of operation has two limiting factors, firstly the drone operator has to maintain VLOS which means all kinds of physical obstacles on the ground limit the operator's movement which in turn limits the UAV's use. Secondly large amounts of data are saved and later processed, which takes time. 5G networks with low latency and high bandwidth will help UAV operators carry out BVLOS operations transmitting the LIDAR and camera payload data in real time, giving quicker and more efficient results.

Figure 40 depicts the UC3 scenario 1 Sub-Scenario 2 components and how they are mapped to facility resources.

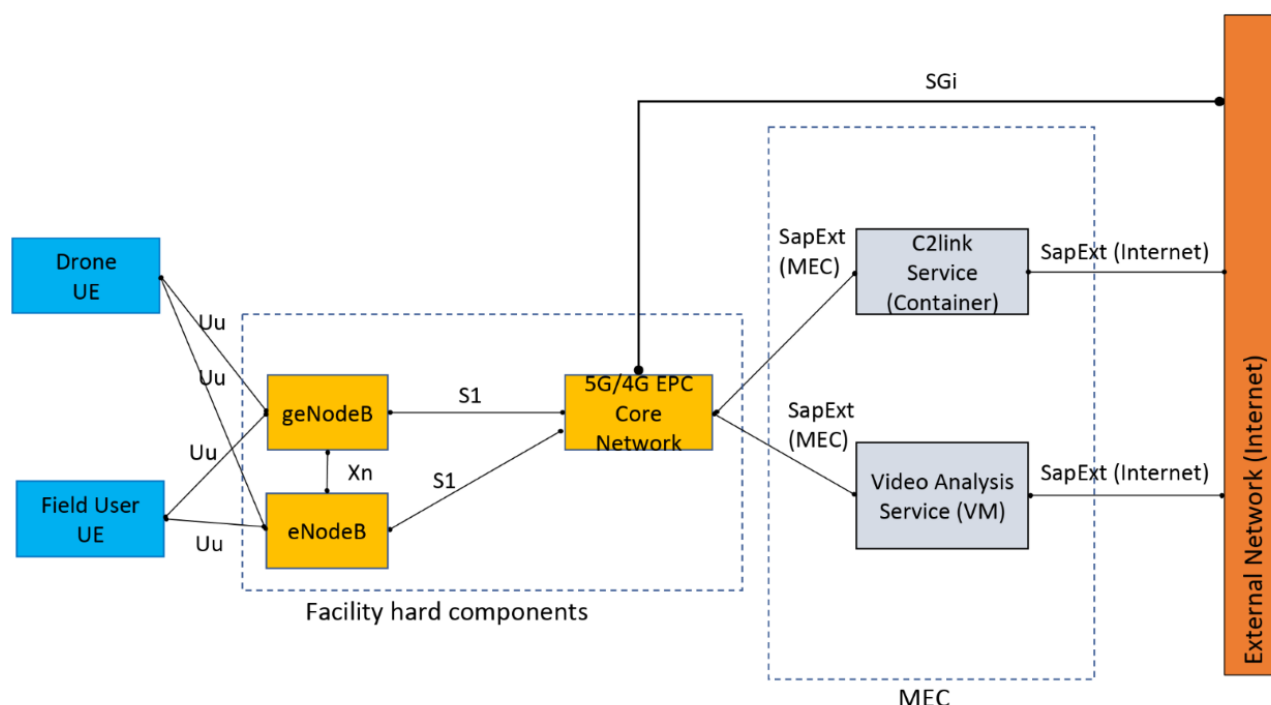


Figure 40 - UC3 scenario 1 sub-scenario 2 - Functional components and their mapping to the facility

The tables below summarize the partners in charge of providing each component for the trial of UC3 scenario 1 Sub-Scenario 2.

Table 65: UC3 scenario 1 sub-scenario 2 UAV components

UAV Components	Type (Hw/Sw)	Partner
Hepta drone	Hw	HEP
Payload (2 LIDARs, camera)	Hw/Sw	HEP

Table 66: UC3 scenario 1 sub-scenario 2 UAV operator components

UAV Operator Components	Type (Hw/Sw)	Partner
GCS (remote + laptop)	Hw/Sw	HEP
Payload visualisation	Sw	HEP
PC	Hw/Sw	HEP

Table 67: UC3 scenario 1 sub-scenario 2 UTM components

UTM Components	Type (Hw/Sw)	Partner
U-Space interface	Sw	FRQ
U-Space interface	Sw	DRR

Table 68: UC3 scenario 1 sub-scenario 2 5G components

5G Components	Type (Hw/Sw)	Partner
5G network	Hw/Sw	UO
5G adapters (smartphones for drone and GCS)	Hw	UO

Table 69: UC3 scenario 1 sub-scenario 2 other components

Other Components	Short description	Type (Hw/Sw)	Partner
Mockup course	Necessary things to create a mockup course simulating power line insulators.	Hw	HEP

5.3.5. UC3 scenario 1 Sub-Scenario 3 - Inspection and search & recovery operations in large body of water

The goal of the scenario is to monitor the state and the evolution of water bodies such as rivers, streams and lakes, and to perform search and recovery in case of emergencies in the same environments. For this purpose, one or more hybrid drones equipped with the required sensors (such as water quality probes, sonar/lidar, etc.) are sent and patrol on the water and gather data. This data is processed to produce a report on the water quality and maps of water and underwater characteristics from these data. Besides, and for the case of a Search & Recovery where teams of divers must inspect the depths of the water, the real time resulting map will help divers to know their working environments and help ensure safer operations.

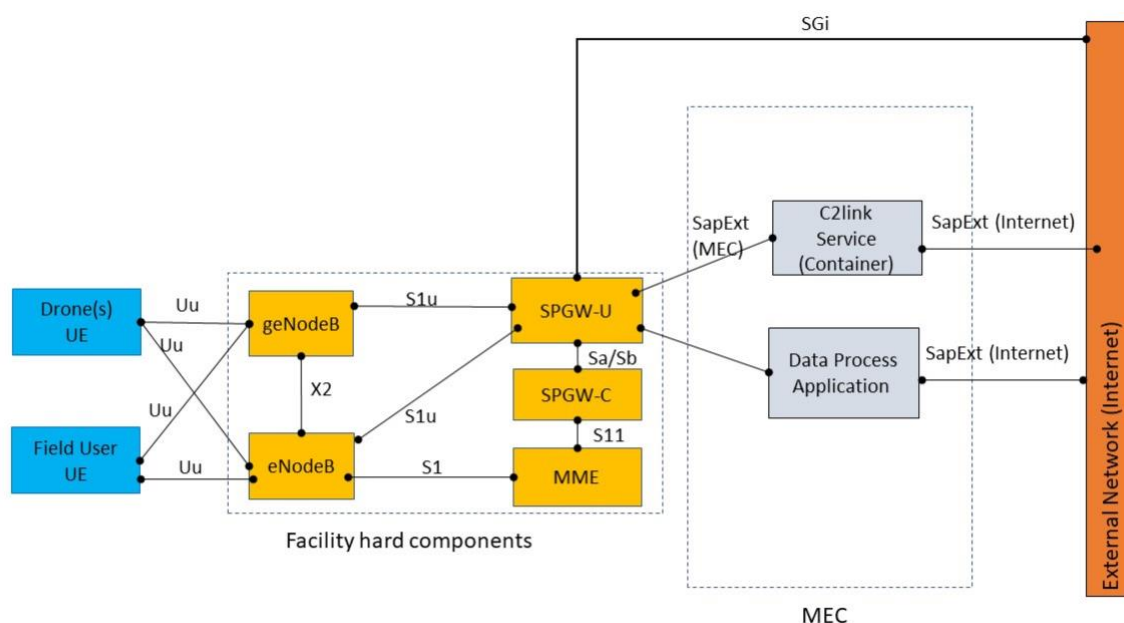


Figure 41 - UC3 scenario 1 Sub-Scenario 3- Functional components and their mapping to the facility

The facility hard components are those already deployed at the facility and enable 5G connectivity via the NSA mode. The UEs are drones with 5G communication capabilities. The services that need to be instantiated at the MEC are composed of a data process application whose purpose is to process data from the drone sensors and visualize them. The tables below summarize the components required for the trial of UC3 scenario 1 sub-scenario 3

Table 70: UC3 scenario 1 Sub-Scenario 3 UAV components

UAV Components	Type (Hw/Sw)	Partner
UE (Drones) Multirotor(x8) Hydradrone	HW & SW	ALE
5G UE, m.2 card (preferred) or phone, for integration and test purposes.	HW & SW	ALE
Payload (including LIDAR, FPV Camera (x2), Sensors, onboard computer)	HW & SW	ALE
Autopilot flight stack	SW	ALE

Table 71: UC3 scenario 1 Sub-Scenario 3 partner/components

UAV Operator Components	Type (Hw/Sw)	Partner
Alerion GCS	SW	ALE

Table 72: UC3 scenario 1 Sub-Scenario 3 partner/components

UTM Components	Type (Hw/Sw)	Partner
Support for dFPL (drone Flight Plan). Situational awareness (airspace perspective) service to submit dFPL.	SW	DRR, FRQ
U-space telemetry endpoint	SW	DRR, FRQ

Table 73: UC3 scenario 1 Sub-Scenario 3 5G components

5G Components	Type (Hw/Sw)	Partner
Modem 5G	HW	UO
5G Network	HW/SW	UO

Table 74: UC3 scenario 1 Sub-Scenario 3 other components

Other Components	Short description	Type (Hw/Sw)	Partner
Data Process Application	Application running at the edge whose purpose is to process data from the drone sensors	SW	ALE

5.3.6. UC3 scenario 3 - Location of UE in non-GPS environments

This use case will demonstrate other means to locate an UAV than a GNSS (Global Navigation Satellite System). There are spaces like metro tunnels, malls or situations when GPS signal can't be received by UAV. GNSS denial attacks or hacked UAVs creates other reasons to not always trust to received position information coming from UAVs, for example, near geo-fenced area like airports or prisons. In this scenario a lots of different positioning related data is first gathered, transmitted via 5G or other means to 5G!Drones MEC and cloud services to be used to calculate UAV(s) position. The Figure 42 shows the UC3 scenario 3 components and how they are mapped to facility resources.

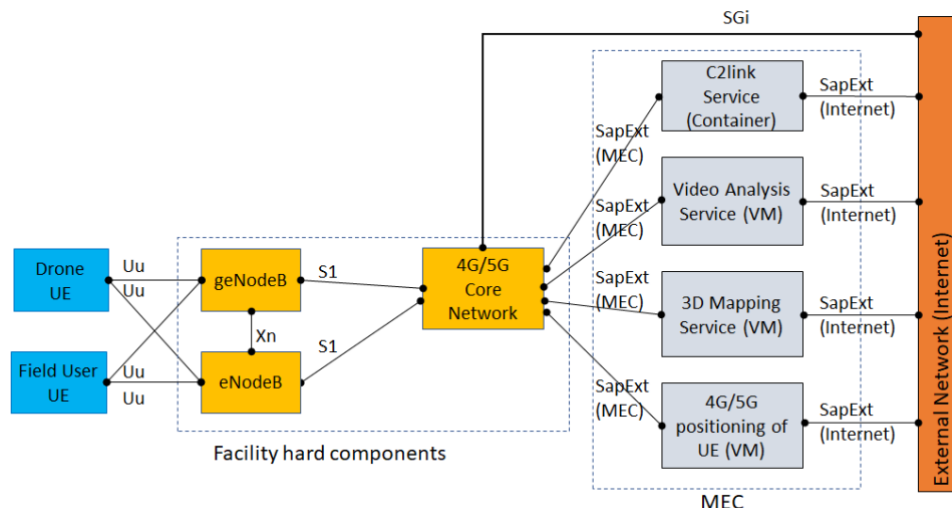


Figure 42 - UC3 scenario 3- Functional components and their mapping to the facility

The facility hard components are those already deployed at the facility and enable 5G connectivity via the NSA mode. The UEs are 5G capable modems and mobile phones. Detailed UAV component presentation is on “UC1 scenario 2- Functional components and their mapping to the facility” as this scenario relies on mostly the same components. The services that need to be instantiated at the MEC are composed of different services to pre-process and calculate position information to user-friendly format. The tables below summarize the components needed for the trial of UC3 scenario 3. Note that no UTM components are involved, since the trial is deployed indoors.

Table 75: UC3 scenario 3 UAV components

UAV Components	Type (Hw/Sw)	Partner
Matrice M210RTK	HW	UO
UWB beacon	HW	NOK, UO
Wire Drone	HW	UO
NDN Drone	HW	NOK
Lidar	HW	UO
Video camera	HW	UO/NOK
On-board computer unit	HW	UO/NOK
5G / WLAN / Bt modem	HW	UO/NOK
Slam	SW	UO
Accelometers / gyros / barometer etc.	HW	UO/NOK
Decawave based positioning system	SW	UO

Table 76: UC3 scenario 3 UAV operator components

UAV Operator Components	Type (Hw/Sw)	Partner
Default UAV control DJI	HW	UO
Nokia UAV control	HW	NOK
Wire Drone control unit	HW	UO

Table 77: UC3 Scenario 3 5G components

5G Components	Type (Hw/Sw)	Partner
5G Modem	HW	UO/NOK
5G mobile phones (e.g. Mediatek, Samsung, Nokia)	HW	UO/NOK

Table 78: UC3 Scenario 3 other components

Other Components	Short description	Type (Hw/Sw)	Partner
Positioning data collector	Collect different poisoning related data	SW	UO/NOK
Positioning engine	Give positioning coordinates of desired UAV	SW	UO/SW
Slam offloading engine	Give mapping and positioning coordinates of desired UAV	SW	UO
UWB based positioning engine (e.g. Poxyz)	Give positioning coordinates of desired UAV	SW	UO/NOK

Conclusions

This Deliverable provided a detailed description of the 5G trial facilities involved in 5G!Drones project. The description provides advanced details on the components of each of the facilities from the RAN, CN, and MEC capabilities, to the security features offered at each site. The current capabilities of each of the platforms are an extension of the initial description and outlook on the facilities roadmap provided in D1.2, and D1.3. The deliverable provided also a detailed mapping of all the use cases to be trialled in the scope of 5G!Drones. Detailed outlooks on test facility roadmap alignment with the identified use case scenarios are translated through architectural descriptions of each scenario as well as the functional components, on the level of UAVs, UAV operators, UTM, and 5G.

References

[1] ETSI GS NFV 003, “Network Functions Virtualisation (NFV); Terminology for Main Concepts in NFV”, v1.2.1, Dec. 2014.

[2] 5G!DRONES D1.1 5G!Drones deliverable, “D1.1. Use case specifications and requirements”.

[3] 5G!DRONES D1.2 “Initial description of the 5G trial facilities”,
<https://5gdrones.eu/deliverables/>

[4] 5G!DRONES D1.3 “5G!Drones system architecture initial design”,
<https://5gdrones.eu/deliverables/>

[5] 5GENESIS D2.2 “Initial overall facility design and specifications“ https://5genesis.eu/wp-content/uploads/2019/12/5GENESIS_D2.2_v1.0.pdf

[6] ETSI White Paper “MEC Deployments in 4G and Evolution Towards 5G”
https://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp24_MEC_deployment_in_4G_5G_FINAL.pdf