



“5G for Drone-based Vertical Applications”

D1.3 – System Architecture Initial Design

Document ID:	D1.3
Deliverable Title:	System Architecture Initial Design
Responsible Beneficiary:	ORA
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 1st, 2019
Project Duration:	36 Months
Contractual Delivery Date:	M08
Actual Delivery Date:	28/02/2020
Dissemination Level:	PU
Contributing Beneficiaries:	AIR, ALE, AU, CAF, COS, NCSRD, DRR, EUR, FRQ, INF, INV, MOE, NOK, OPL, ORA, RBX, THA, UMS, UO.



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

Document ID: D1.3
Version: V1.0
Version Date: 28/02/2020
Authors: Laurent Reynaud (ORA), Yvon Gourhant (ORA), Marc Lacoste (ORA), Yvan Rafflé (ORA), Serge Delmas (AIR), Arthur Lallet (AIR), Loïc Wassermann (ALE), Abderrahmane Abada (AU), Oussama Bekkouché (AU), Hamed Hellaoui (AU), Tarik Taleb (AU), Tanel Järvet (CAF), Ioanna Mesogiti (COS), Fofy Setaki (COS), Anastasios Gogos (NCSRD), Stavros Kolometsos (NCSRD), Harilaos Koumaras (NCSRD), Paweł Korzec (DRR), Maha Bouaziz (EUR), Adlen Ksentini (EUR), Saadan Ansari (FRQ), Thomas Lutz (FRQ), Vaïos Koumaras (INF), Aggeliki Papaioannou (INF), Mélanie Guittet (INV), Paweł Montowtt (INV), Dimitris Tzempelikos (MOE), Ilkka Kansala (NOK), Riikka Valkama (NOK), Robert Kołakowski (OPL), Sławomir Kukliński (OPL), Lechosław Tomaszewski (OPL), Jonas Stjernberg (RXB), Tero Vuorenmaa (RXB), Pascal Bisson (THA), Farid Benbadis (THA), Cyril Dangerville (THA), Kim Clement (UMS), Tomas Gareau (UMS), Nemish Mehta (UMS), Idris Badmus (UO) and Abdelquodouss Laghrissi (UO).

Security: Public (PU)

Approvals

	Name	Organisation	Date
Coordinator	Jussi Haapola	UO	28/02/2020
Technical Committee	Pascal Bisson	THA	27/02/2020
Management Committee	Project Management Team, Additional Reviewers	UO, THA, AU, AIR, UMS, FRQ, COS	14/02/2020

Document History

Version	Contribution	Authors	Date
V0.1 to V0.3	Initial table of content, collection of inputs from all partners.	ORA, ALL	28/07/2019 to 06/09/2019
V0.4	Consolidation of the table of contents in preparation of the Athens face-to-face meeting.	ORA, ALL	16/09/2019
V0.5 to V0.8	Initial versions of the document taking into account the discussion outputs of the Athens face-to-face meeting and the recurrent D1.3 audio meetings with the partners.	ORA, ALL	19/11/2019 to 02/12/2019
V0.9	Section 3 (5G/MEC), Section 5 (gap analysis).	ORA, AU, CAF, COS, EUR, UO	05/12/2019

V0.10 to V0.14	Sections 2.3 (UTM) 2.4 (use cases), 3.1.4 (5G/slicing), 5.1.4 and 5.2 (gap analysis), 6 (unified Interfaces, Enablers, cybersecurity).	ORA, ALE, AU, CAF, NCSRD, FRQ, INF, OPL, THA	06/12/2019 to 15/12/2019
V0.15	Updates on all sections, taking into account the December D1.3 audio meetings with the partners.	ORA, AIR, ALE, CAF, COS, EUR, FRQ, NOK, OPL, UMS	05/01/2020
V0.16 to V0.19	Updates on all sections, in preparation of the Nice face-to-face meeting.	ORA, ALE, NCSRD, FRQ, OPL, THA, ALL	06/01/2020 to 28/01/2020
V0.20 to V0.21	Updates on all sections, taking into account the outcomes of the Nice face-to-face meeting and in preparation of the Internal Reviews.	ORA, AIR, CAF, INF, NOK, THA, ALL	30/01/2020 to 10/02/2020
V0.22	Preparation of the reviews from Technical Committee.	ORA, AU, COS, FRQ, ALL	11/02/2020 to 17/02/2020
V1.0	Final editorial adjustments	ORA, UO, THA	28/02/2020

Executive Summary

This deliverable presents the 5G!Drones overall architecture design. The objective is twofold: firstly, to support the selected use cases over a federated, multi-domain 5G infrastructure, and secondly, to effectively manage the successful execution of large-scale UAV trials. To that end, the document starts with the presentation of introductory and contextual information, in order to clarify the general purpose of 5G!Drones, and to shed light on the structuring environment that has a significant influence on the project's system architecture. This is notably the case of the UTM and U-Space concepts, which are summarised accordingly, along with the outcomes of relevant European projects.

On that basis, the deliverable then provides a synthetic overview of the main generic aspects of the 5G architecture that are relevant to 5G!Drones. This overview starts with a general description of the 5G system, followed by a more in-depth description of software-defined networking, network function virtualisation, network slicing and multi-access edge computing, which, among other topics explained in this overview, are key concepts for the support of the 5G!Drones overall architecture. In addition, special focus has been put on the different approaches taken by standardisation bodies, such as 3GPP, to consider the interoperability of 5G systems with UTMs. Likewise, a description of the potential interrelations between the 5G!Drones architecture with relevant projects from the 5G Infrastructure Public Private Partnership (5G PPP) is noted.

Having set the context and prevailing principles, the deliverable proceeds with the high-level representation of the overall 5G!Drones architecture that consists of several entities, such as the Portal, the Trial Controller, the Abstraction Layer, the 5G Facility Infrastructure Monitoring, the U-Space entity and the U-Space Adapter. It presents in detail the cornerstone of the envisaged architecture, the 5G!Drones Trial Controller and its components, the Trial Scenario Execution Engine, the Trial Architecture Management Plane and the KPI Assessment and Data Gathering component and how these interact together, as well as with the UAV verticals and the 5G Facilities, in order to enforce the relevant UAV service logic. On top, the presented study investigates how the UAV use case requirements will be met by the member 5G Facilities, by presenting the respective gap analysis in the context of the X-Network, 5GEVE, 5GTN and 5GENESIS Facilities, revealing the focal points for target development per case. It is noteworthy that not all platforms share the same stand-point. While all Facilities miss the UTM functions, 5GENESIS is already furnished with functional experimentation, tools and components that shall be leveraged for comparison and benchmarking of the 5G!Drones architecture on diverse and heterogeneous testbed environments.

Furthermore, the document provides a high-level architectural description of the 5G system components as well as the UAV Enablers which shall be designed in the 5G!Drones project. With this last part, the objective is to support, on the architectural level, the design and development of these components within the project Work Packages WP2 and WP3, as well as their trial in Work Package WP4.

Finally, the concluding section of this deliverable formulates the next steps towards the final revision of the system architecture, which will be reported in deliverable D1.6.

Table of Contents

EXECUTIVE SUMMARY	4
TABLE OF CONTENTS.....	5
LIST OF ABBREVIATIONS	7
LIST OF FIGURES	10
LIST OF TABLES	11
1. INTRODUCTION.....	12
1.1. OBJECTIVE OF THE DOCUMENT	12
1.2. STRUCTURE OF THE DOCUMENT	12
1.3. TARGET AUDIENCE.....	13
2. 5G!DRONES KEY ASPECTS	14
2.1. PROJECT OBJECTIVES.....	14
2.2. THE 5G!DRONES CONCEPTUAL REPRESENTATION	15
2.3. UTM SYSTEMS.....	17
2.3.1. Context and Requirements	17
2.3.2. Interoperability within 5G!Drones	18
2.4. TARGET USE CASES AND TRIAL SCENARIOS.....	21
2.4.1. Target Use Cases.....	21
2.4.2. The context of the selected 5G Facilities	22
3. 5G ARCHITECTURE	24
3.1. RELEVANT 5G FEATURES.....	24
3.1.1. NG-RAN, 5G Core	24
3.1.2. Principles of SDN/NFV	27
3.1.3. Slicing Mechanisms.....	30
3.1.4. Multi-Access Edge Computing	35
3.1.5. Beamforming	39
3.1.6. Spectrum and Spectrum Efficiency	40
3.1.7. Focus on mMTC	42
3.1.8. Multimedia Mission Critical Services	43
3.2. UTM INTEGRATION INTO STANDARDISED 5G SYSTEMS.....	43
3.3. EXTENDED SCOPE AND OPPORTUNITIES	45
3.3.1. Interrelated 5G PPP Architectures	45
3.3.2. Further enhancements with next 3GPP Releases	47
4. OVERALL ARCHITECTURE DESIGN	49
4.1. HIGH-LEVEL OVERVIEW.....	49
4.2. ARCHITECTURAL BREAKDOWN INTO COMPONENTS.....	49
4.2.1. Portal.....	50
4.2.2. Trial Controller	50
4.2.3. Abstraction Layer	51
4.2.4. 5G Facility Infrastructure Monitoring	51
4.2.5. U-Space	51
4.2.6. U-Space Adapter	52
5. GAP ANALYSIS	53

5.1.	PER SITE GAP ANALYSIS.....	53
5.1.1.	X-Network	53
5.1.2.	5GEVE.....	55
5.1.3.	5GTN	58
5.1.4.	5GENESIS	61
5.2.	HARMONISED ANALYSIS, MAIN TAKEAWAYS.....	66
6.	5G!DRONES ENABLERS	67
6.1.	5G SYSTEM ENABLERS.....	67
6.1.1.	Slicing for Drone-based Services	67
6.1.2.	MEC Extensions and Architectural Impact of Trial Facilities	68
6.1.3.	Unified Interfaces over Heterogeneous Facilities.....	69
6.1.4.	Use Case Data Storage and Analysis Services	70
6.1.5.	MCS Solution	71
6.2.	UAV SERVICE ENABLERS.....	72
6.2.1.	Required Set of Service Enablers per Scenario	72
6.2.2.	Use Case 1: UAV Traffic Management	72
6.2.3.	Use Case 2: Public Safety/Saving Lives.....	74
6.2.4.	Use Case 3: Situation Awareness	76
6.2.5.	Use Case 4: Connectivity During Crowded Events	78
6.3.	CYBERSECURITY SUPPORT.....	79
6.3.1.	Identity and Access Management (IAM) Services	80
6.3.2.	Digital Certificate Services (PKI)	81
6.3.3.	Cryptography Services	81
6.3.4.	Network Access Control Services (NAC)	82
6.3.5.	Security Policy Management and Orchestration Service (SPS)	82
6.3.6.	Security Policy Enforcement Point Services (PEP)	83
6.3.7.	Security Information and Event Management Services (SIEM)	83
6.3.8.	Security SLA Management Service	84
6.3.9.	Airbus MCS Security.....	84
6.3.10.	Security for IoT solutions	84
6.3.11.	Cybersecurity tests	86
7.	CONCLUSION	87
	REFERENCES	89

List of Abbreviations

3GPP	3 rd Generation Partnership Project
5G	5 th Generation
5GC	5G Core
5G PPP	5G infrastructure Public Private Partnership
5GS	5G System
AIM	Aeronautical Information Management
AMF	Access and Mobility Management Function
ANSP	Air Navigation Service Provider
APN	Access Point Name
ATM	Air Traffic Management
BTS	Base Transceiver Station
BVLOS	Beyond Visual Line of Sight
C2	Command and Control
CMS	Configuration Management Server
CN	Core Network
CONOPS	Concept of Operations (U-Space)
COTS	Commercial Off-The-Shelf
CPRI	Common Public Radio Interface
CSP	Communication Service Provider
CU	Centralized Unit
DDoS	Distributed Denial of Service
DTM	Drone Traffic Management
DU	radio Digital Unit (first meaning) or Distributed Unit (second meaning)
Dx.y	Deliverable number y of WP x
eMBB	enhanced Mobile BroadBand
eNB	enhanced Node-B
EPC	Evolved Packet Core
ETL	Extract, Transform, Load
FIMS	Flight Information Management System
GCS	Ground Control Station
GMS	Group Management Server
gNB	Next Generation Node-B
GOF	U-space demonstration in the Gulf of Finland
GPRS	General Packet Radio Service
GTP	GPRS Tunnelling Protocol
HAP	High Altitude Platform
HSS	Home Subscriber Server

IALA	International Association of Marine Aids to Navigation and Lighthouse Authorities
IAM	Identity and Access Management
IdMS	Identity Management Server
IM	Infrastructure Monitoring
IRP	Integration Reference Point
ISG	Industry Specification Group
ITU	International Telecommunications Union
KMS	Key Management Server
KPI	Key Performance Indicator
LBO	Local Breakout
LPWA	Low Power Wide Area
MANO	MANagement and Orchestration
MCS	Multimedia Mission Critical Services
MEAO	Multi-access Edge Application Orchestrator
MEC	Multi-access Edge Computing
MEP	MEC Platform
MFA	Multi-Factor Authentication
MIMO	Multiple Input Multiple Output
MME	Mobility Management Entity
mMTC	massive Machine-Type Communications
NAC	Network Access Control
NEF	Network Exposure Function
NFV	Network function virtualisation
NG-RAN	Next Generation - Radio Access Network
NR	New Radio
NRF	Network Functions Repository Function
NSA	Non-Standalone
NSI	Network Slice Instance
NSSF	Network Slice Selection Function
NSSI	Network Slice Subnet Instance
NTN	Non Terrestrial Network
NWDAF	NetWork Data Analytics Function
OAI	OpenAirInterface
OSM	Open Source MANO
PEP	Policy Enforcement Point
PGW	Packet Data Network Gateway
PM	Performance Monitoring
PNF	Physical Network Function
ProSe	Proximity Services

QoE	Quality of Experience
QoS	Quality of Service
RAN	Radio Access Network
RF	Radiofrequency
RU	Radio Unit (first meaning) or Remote Unit (second meaning)
SA	StandAlone
SBA	Service-Based Architecture
SCC	Security Control Classes
SDN	Software-Defined Networking
SECaaS	SECurity as a Service
SD-SEC	Software-Defined SECurity
SESAR	Single European Sky ATM Research
SGW	Serving Gateway
SIEM	Security Information and Event Management
SNMP	Simple Network Management Protocol
S-NSSAI	Single Network Slice Selection Assistance Information
SWIM	System-Wide Information Management
TRL	Technology Readiness Level
UAS	Unmanned Aerial System
UAV	Unmanned Aerial Vehicle
UDM	Unified Data Management
UE	User Equipment
UPF	User Plane Function
URLLC	Ultra-Reliable Low Latency Communications
USP	U-Space Service Provider
UTM	UAS Traffic Management
VIM	Virtualised Infrastructure Manager
VLD	Very Large Demonstrator
VLOS	Visual Line of Sight
VM	Virtual Machine
VR	Virtual Reality
WP	Work Package

List of Figures

FIGURE 1 - THE 5G!DRONES CONCEPTUAL REPRESENTATION	16
FIGURE 2 - UTM DEPLOYMENT OVERVIEW AS DEPICTED IN CORUS [62]	18
FIGURE 3 - GOF USPACE HIGH LEVEL ARCHITECTURE [17]	19
FIGURE 4 - GOF USPACE SERVICE DESCRIPTIONS [63]	20
FIGURE 5 - 5G NG-RAN	25
FIGURE 6 - 4G AND 5G DEPLOYMENT OPTIONS [78]	26
FIGURE 7 - 5G CORE SERVICES BASED ARCHITECTURE	26
FIGURE 8 - NFV MANO ARCHITECTURE [79]	28
FIGURE 9 - THREE-TIER STRUCTURE OF A TYPICAL SDN CONTROLLER [79]	30
FIGURE 10 - NETWORK SLICE SUBNETS, NETWORK SLICE AND COMMUNICATION DEPENDENCIES (BASED ON [34])	32
FIGURE 11 - CREATION OF END-TO-END 3GPP COMPLIANT SLICES (BASED ON [37])	32
FIGURE 12 - 5GC SUPPORT FOR NETWORK SLICING (BASED ON [7])	33
FIGURE 13 - NETWORK SLICE INSTANCE MANAGEMENT PHASES [34]	34
FIGURE 14 - 5G SERVICE ARCHITECTURE AND A GENERIC MEC SYSTEM ARCHITECTURE [1]	35
FIGURE 15 - MULTI-ACCESS EDGE SYSTEM REFERENCE ARCHITECTURE VARIANT FOR MEC IN NFV [3]	36
FIGURE 16 - NEW APPLICATION DEVELOPMENT PARADIGM INTRODUCED BY MEC [4]	37
FIGURE 17 - MULTI-ACCESS EDGE COMPUTING FRAMEWORK [3]	38
FIGURE 18 - 5G BEAMFORMING BENEFITS FOR UAVs	40
FIGURE 19 - COVERAGE AND SPECTRUM USAGE COMPARISON BETWEEN 4G AND 5G [83]	41
FIGURE 20 - ESTIMATION OF RADIO COVERAGE FOR SEVERAL 5G NR FREQUENCIES [10]	41
FIGURE 21 - UAS REFERENCE MODEL IN 3GPP ECOSYSTEM TS22.125 [61]	45
FIGURE 22 - C2 COMMUNICATION MODELS (BLUE ARROWS SHOW C2 COMMUNICATION LINKS) [60]	45
FIGURE 23 - 5G PAN-EU TRIALS ROADMAP – TIME PLAN [69].	46
FIGURE 24 - OVERALL RAN TIMELINE. 5G IN RELEASE 17 – STRONG RADIO EVOLUTION [71].	47
FIGURE 25 - HIGH-LEVEL OVERVIEW OF THE 5G!DRONES ARCHITECTURE	49
FIGURE 26 - THE ABSTRACTION LAYER HANDLES THE 5G FACILITIES DIVERSITY (5GEVE, 5GTN, X-NETWORK AND 5GENESIS)	51
FIGURE 27 - HIGH LEVEL ARCHITECTURE DATA STORAGE & ANALYSIS SERVICES	70
FIGURE 28 - PROPOSED IOT NETWORK FORENSICS FRAMEWORK [44]	84

List of Tables

TABLE 1 - HIGH-LEVEL CLASSIFICATION OF THE 4G AND 5G RADIO FREQUENCY SPECTRUM	40
TABLE 2 - LTE CAT-M1, LTECAT-M2, NB-IOT COMPARISON [87]	42
TABLE 3: AALTO EVOLUTION ANALYSIS	53
TABLE 4: 5GEVE EURECOM SITE EVOLUTION ANALYSIS	55
TABLE 5: 5GTN OULU EVOLUTION ANALYSIS	59
TABLE 6 - 5GENESIS EVOLUTION ANALYSIS	62
TABLE 7 - TARGET PLANES FOR ABSTRACTING AND UNIFIED THE EXPOSED INTERFACES	70
TABLE 8: UC1SC1 SERVICE ENABLERS	73
TABLE 9: UC1SC2 SERVICE ENABLERS	73
TABLE 10: UC1SC3 SERVICE ENABLERS	74
TABLE 11: UC2SC1 SERVICE ENABLERS	74
TABLE 12: UC2SC2 SERVICE ENABLERS	75
TABLE 13: UC2SC3 SERVICE ENABLERS	76
TABLE 14: UC3SC1SUB1 SERVICE ENABLERS	76
TABLE 15: UC3SC1SUB2 SERVICE ENABLERS	77
TABLE 16: UC3SC1SUB3 SERVICE ENABLERS	77
TABLE 17: UC3SC2 SERVICE ENABLERS	78
TABLE 18: UC3SC3 SERVICE ENABLERS	78
TABLE 19: UC4SC1 SERVICE ENABLERS	78

1. INTRODUCTION

1.1. Objective of the document

The primary objective of this deliverable is the presentation of the overall architecture design to support the selected use cases over a federated, multi-domain 5G infrastructure, and also to execute large-scale UAV trials. To that end, the document gives a synthetic view of the underlying 5G architecture needed to deploy the target vertical services, as defined in the use cases elaborated in D1.1. Furthermore, deliverable D1.3 seeks to identify and give a high-level description of the architectural components to provide the necessary infrastructure support for these selected use cases. Consequently, this document is intended to provide an initial support for the activities of WP3, in which those architectural components will be further devised and implemented. It is worth highlighting that this notion of architectural component both encompasses all necessary 5G system components, as well as all the 5G!Drones enablers more specifically needed by the service logics of the target use cases. In particular, this deliverable intends to provide a high-level design of the management plane for the execution of the UAV trials, with the intention to support the detailed design and implementation of the 5G!Drones trial controller, in WP2.

1.2. Structure of the document

After a concise introductory section, **Section 2** gives general key aspects so that the reader understands the general purposes of 5G!Drones as well as the structuring environment that impacts the project system architecture. In particular, Section 2 provides a conceptual representation of the entities and roles at stake, as well as an outline of the general landscape of UTMs and relevant regulatory bodies. Section 2 also briefly outlines the UAV use cases which are relevant in the rest of this document and provides references to the in-depth studies reported in other deliverables of the project.

On that basis, the purpose of **Section 3** is to provide a synthetic overview of the main generic aspects of the 5G architecture that are relevant to 5G!Drones. In particular, a large subsection is dedicated to the different approaches taken by standardisation bodies such as 3GPP, to consider the interoperability of 5G systems with UTMs. **Section 4** then gives a high level and conceptual representation of the overall 5G!Drones architecture design. In particular, it presents the main 5G!Drones Trial Controller components which allow interacting with the UAV verticals and 5G Facilities to enforce the relevant UAV service logic.

Furthermore, since the project envisions the trial of UAV use cases associated to specific 5G Facilities, four gap analyses are conducted in **Section 5**, respectively in the context of the X-Network, 5GEVE, 5GTN and 5GENESIS Facilities. The objective here is to identify which of the UAV service requirements can be met with the provided 5G architectures, and which UAV use case features require the development of specific components, whose identification is the purpose of this section.

On that premise, **Section 6** gives a high-level architectural description of the 5G system components as well as the UAV service components which shall be designed in the 5G!Drones. The outcome of this section is notably intended to support the detailed component designs and implementations of WP2 and WP3. Finally, **Section 7** gives the concluding remarks as well as the next steps towards the final revision of the system architecture, due at Month 18.

1.3. Target Audience

This document mainly targets the following audience:

- **The Project Consortium and Stakeholders**, especially contributing beneficiaries of the design and implementation work packages (WP2 & WP3) but also the ones in charge of the integration and trial validation (WP4). In this regard, the initial architecture design delivered by this document will support the further elaboration of the components to provide the necessary infrastructure support for the selected use cases. That includes all the necessary 5G system components, as well as the specific 5G!Drones enablers. It is also worth noting that the high level description of the management plane for the execution of the trials is intended to support the rest of the project consortium, notably in the context of WP2, as the basis for the detailed design and implementation of the 5G!Drones trial controller;
- **The Research Community, Industry and funding EC Organisation** to i) summarise the 5G!Drones scope, objectives and intended project innovations and ii) detail the initial design of the 5G!Drones system architecture. The objective is to facilitate the understanding of which architectural components need to be designed by the project so as to be able to fully demonstrate and measure the provided technological advancements on all target ICT-17 5G Facility sites;
- **The broadest possible technical and non-technical audience (General public)** to obtain a better understanding of the scope, objectives and general architecture of the 5G!Drones project.

2. 5G!DRONES KEY ASPECTS

With this section, general key aspects are presented, for a better understanding of the purposes of 5G!Drones as well as the structuring environment that is likely to impact the project system architecture. Therefore, after a brief description of the project objectives, Section 2 provides a conceptual representation of the entities and roles at stake, including the concepts of UAV vertical, Trial Controller and 5G Facility in the context of 5G!Drones. This is followed by an outline of the general landscape of UTM's, the relevant regulatory bodies and associated research programs, in particular at a European level. Section 2 also briefly outlines the UAV use cases which are relevant in the rest of this document and provides references to other deliverables featuring in-depth use case studies.

2.1. Project Objectives

The 5G!Drones project aims to trial several UAV use cases covering eMBB, URLLC and mMTC 5G services, and validate the relevant 5G KPIs that apply to such challenging use cases. The project builds on top of the 5G Facilities provided by the ICT-17 projects, identifies and develops the missing components to trial the UAV use cases. To ease and automate the execution of trials by the verticals, that are the main users of 5G!Drones, the project builds a software layer that exposes a high-level API to be used in order to request the execution of a trial according to the scenario of interest.

In this respect, the main objectives of the project include:

1. The analysis of the performance requirements of UAV verticals' applications and business models in 5G;
2. The design and implementation of the 5G!Drones software layer (or system) to execute UAV trials;
3. The design of a high-level scenario descriptor language to run and analyse the results of the UAV trials;
4. The design and implementation of 5G!Drones enablers for UAV trials and operations;
5. The validation of the 5G KPIs that demonstrate the adequate execution of UAV use cases;
6. The validation of UAV KPIs using 5G;
7. The use of advanced data analytics tools to visualise and deeply analyse the trial results, and provide feedback to the 5G and UAV ecosystem;
8. And finally, the dissemination, standardisation and exploitation of 5G!Drones.

The project plans to offer innovations in the UAV vertical industry through application scenarios that harness the 5G potential, and in the network and infrastructure domain through the development of the necessary system support. Furthermore, the project sets out to contribute to innovative methodologies and tools for large-scale experimentation. In summary, the main innovations expected by 5G!Drones are:

- Business and regulatory aspects, through the definition of a business and financial analysis framework for the UAV ecosystem considering vertical-service-related KPIs and the ongoing regulatory developments;
- Trial Execution, through the development of automation tools for 5G trials, innovative data management analysis and visualisation tools, and monitoring & management interfaces towards verticals, facility operators and experimenters;

- 5G Infrastructure support, through multi-domain slice orchestration, MEC architecture extensions and E2E network slicing security;
- Vertical Services, through development of new 5G enabled vertical services including public safety, emergency response, situation aware IoT and enhanced connectivity services. Furthermore, innovation is expected in the area of novel UAS traffic management including virtual reality-based services and Beyond Visual Line Of Sight (BVLOS) operations.

On this basis, the outcomes of deliverable D1.3 support the project Objectives 2 and 4, by providing a high-level architectural view on top of which the design and implementation the 5G!Drones software system layer (Objective 2) and the enablers for UAV trials and operation (Objective 4) can be built. Indeed, the identification and architectural description of the 5G system components, as well as of the 5G!Drones enablers, is intended to provide a high-level and initial support for the activities, notably in WP2 and WP3, that seek to address both objectives. It is also worth noting that this deliverable gives a high level description of the way the 5G!Drones trial controller will interact, via its components and specific interfaces, to the Network Slices, UAV components and the 5G Facilities to gather all required 5G KPIs and service-level KPIs, thereby providing early support to the project Objectives 5 and 6.

2.2. The 5G!Drones Conceptual Representation

The 5G!Drones system can be conceptually described by three distinct actors, whose interactions are guiding the overall approach taken by the project, regarding how the selected UAV use cases will be trialled on the 5G Facilities of concerns and that apply among the ones in scope (ICT-17: 5GEVE and 5Genesis as well as X-Network and 5GTN). These actors are the UAV vertical, the 5G!Drones trial controller and the 5G Facility, as illustrated in Figure 1.

The **UAV vertical** is the actor in charge of performing the trials of UAV use cases on top of a 5G infrastructure provided by 5G Facilities. To do so, it uses a dedicated set of APIs, referred to as northbound APIs in this high-level representation, to interact with the second actor in this representation, the **5G!Drones Trial Controller**. The northbound APIs allow several types of interactions, including the possibility to run and control a test, by for instance selecting the desired KPIs to test and the UAV application to run. In addition, this set of APIs allows the UAV Vertical to gain a secured access to the network slices running the UAV applications. Moreover, those APIs also allow obtaining the results of the trial, under the form of 5G KPI and UAV KPI values.

In addition, the 5G!Drones Trial Controller is in charge of enforcing the trial scenario by interacting with the third actor of this representation, the **5G Facility**. This interaction is allowed by APIs provided by the 5G Facility through the 5G!Drones Enablers. It is worth noting that both the Trial Component and the Enablers are designed and developed by the 5G!Drones project. In this regard, the 5G!Drones Enablers are components developed within the 5G!Drones project to allow running these UAV use cases on top of the 5G Facilities.

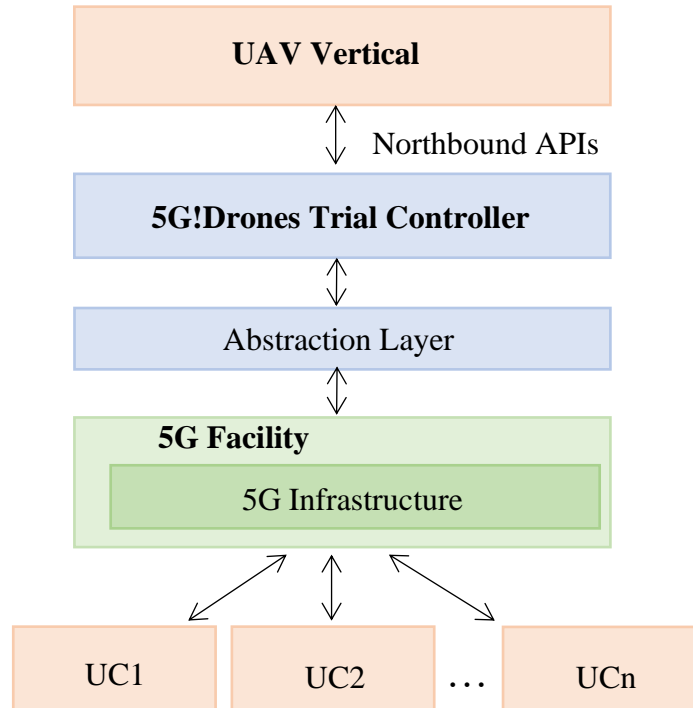


Figure 1 - The 5G!Drones conceptual representation

On this basis, the role of the Trial Controller is to translate the high-level trial scenario description, provided by the UAV Vertical, to a set of 5G network components required to run on top of the 5G Facility. As an example, the UAV Vertical may provide a high-level description which is mapped by the Trial Controller into a 5G secured network slice using, if available, the 5G Facility blueprint, i.e. a description of all the necessary network components to run the trial, such as the VNFs, RAN resources, and duration of the trial. During the execution of the selected use case trial, the Trial Controller accesses the UAV VNFs and UEs, whether embedded aboard the drones or on the ground, to obtain the necessary results and KPIs at the application level. In addition, the Trial Controller is able to access the 5G Facility, via specific 5G!Drones components to monitor the 5G KPIs.

At this point, it is important to note that the intended use of the 5G!Drones Trial Controller goes beyond the scope of this first description, which has only considered so far a simple test scenario, in which a single use case is trialled. However, the 5G!Drones architecture will be elaborated so that the Trial Controller allows the simultaneous run and control of multiple UAV use cases, demonstrating the capability of 5G to guarantee different service requirements at the same time. Likewise, it is worth highlighting that in the context of 5G!Drones, we have considered different 5G Facilities for in-situ trials, including ICT-17 5G Facilities (5GEVE and 5Genesis) as well as X-Network and 5GTN Facilities. This is detailed in deliverable D1.2 and is summarised later in subsection 2.4. Consequently, this set of target 5G Facilities poses specific heterogeneity challenges for the 5G!Drones project, since they exhibit in particular different 5G features and enforce different types of low-level APIs. This notably provides a strong rationale for the gap analysis that is detailed in Section 5. This analysis assesses the need for specific 5G adaptation components and more generally for the design of an Abstraction Layer, which in turn allows extending the 5G Facilities by defining a complete Southbound interface, to eventually comply with the incurred heterogeneity.

2.3. UTM Systems

To continue the description of the key 5G!Drones objectives, this subsection provides an outline of the general landscape of **Unmanned Aerial Systems Traffic Management** (UTMs). As will be seen in the rest of this deliverable, this context, as well as the activity of the relevant regulatory bodies, are structuring for the project overall architecture, and in particular for the approach taken to integrate the UTM and U-Space concepts with the overall 5G!Drones architecture.

2.3.1. Context and Requirements

With the so-called Warsaw Declaration after a high-level conference in November 2016, the notion of U-space was introduced [15]: *“U-space is a set of new services and specific procedures designed to support safe, efficient and secure access to airspace for large numbers of drones. These services rely on a high level of digitalisation and automation of functions, whether they are on board the drone itself, or are part of the ground-based environment. U-space provides an enabling framework to support routine drone operations, as well as a clear and effective interface to manned aviation, ATM/ANS service providers and authorities. U-space is therefore not to be considered as a defined volume of airspace, which is segregated and designated for the sole use of drones. U-space is capable of ensuring the smooth operation of drones in all operating environments, and in all types of airspace (in particular but not limited to very low-level airspace). It addresses the needs to support all types of missions and may concern all drone users and categories of drones.”*

In 2007, the Single European Sky ATM Research (SESAR) Joint Undertaking [90] was set up in order to define, develop and deploy what is needed to increase ATM performance and build Europe’s intelligent air transport system. In the context of unmanned traffic, a series of SESAR projects was kicked off, ranging from “exploratory research” (initial work) to very large demonstrators, i.e. demonstrating systems with preoperational Technology Readiness Level (TRL). An important project was the so-called CORUS project [16]. With part-funding from the EU’s Horizon 2020 programme through grant 763550, and in the context of the SESAR 2020 exploratory research programme, the SESAR Joint Undertaking (SJU) has sponsored the CORUS project to write a low-level Concept of Operations (ConOps) for U-space. As one target of U-space is the creation and facilitation of an open & competitive market, CORUS proposes a flexible high-level deployment architecture that can realise different actual deployments, ranging from a rather monolithic approach to more federated architectures, as depicted in Figure 2.

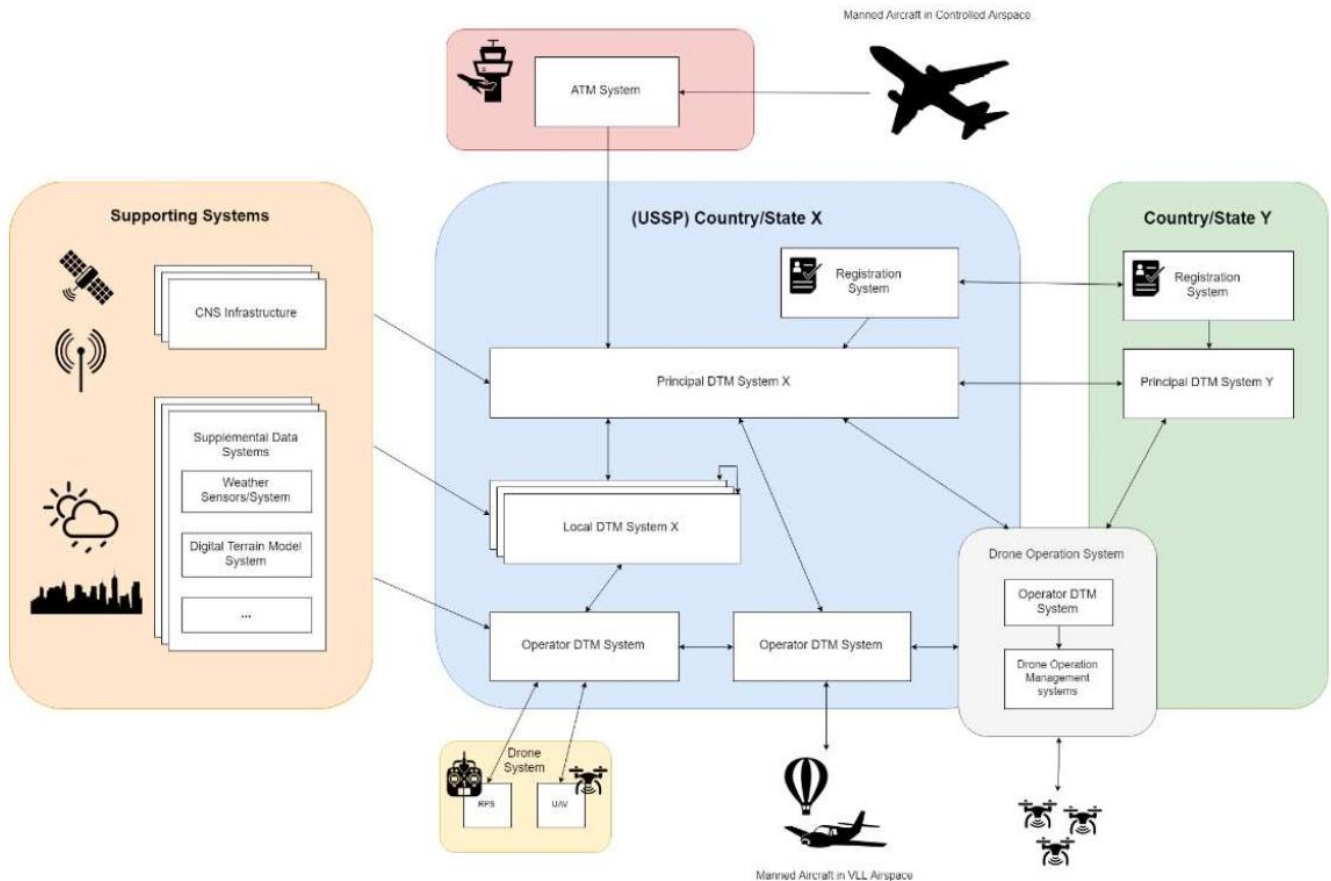


Figure 2 - UTM Deployment Overview as depicted in CORUS [62]

A principal DTM (Drone Traffic Management system) integrates one or more Local DTM, which integrate several Drone Operator Systems. CORUS defines DTM as “variant of UTM” [62], with in 5G!Drones DTM is to be understood equivalent to UTM₁. Drone Operator Systems could be directly integrated to the Principal DTM as well.

2.3.2. Interoperability within 5G!Drones

For validation of U-space concepts described in CORUS, several VLD (Very Large Demonstrators) were started in parallel. To facilitate technical harmonisation between those projects, principles for U-space architecture were published by SESAR [17], including examples for U-space architectures.

With a strong focus on SWIM (System Wide Information Management) & interoperability validated in demonstrations including five service providers, the Gulf Of Finland (GOF) USPACE architecture [17], as shown in Figure 3, is deemed to be a suitable candidate for the overall 5G!Drones UAV Verticals architecture. In this context, the Air Navigation Service Provider (ANSP), the Flight Information Management System (FIMS) and the U-Space Service Providers (USP) are notable entities of this architectural representation. The GOF USPACE architecture provides a framework for actors in and

¹ Typically, an UAV (Unmanned Aerial Vehicle, commonly referred to as drone) is part of an UAS (Unmanned Aerial System). Other components of an UAS (next to the drone) could be e.g. the GCS (Ground Control Station), ground infrastructure like radio base stations for command & control. As a UTM is meant to manage traffic, DTM is an equivalent part, focussing on the moving part of an UAS, the drone.

connected to U-space based on common principles for U-space architectures and SWIM principles – as summarised in the ICAO 10039 Manual [18]: “*SWIM consists of standards, infrastructure and governance enabling the management of ATM information and its exchange between qualified parties via interoperable services.*”

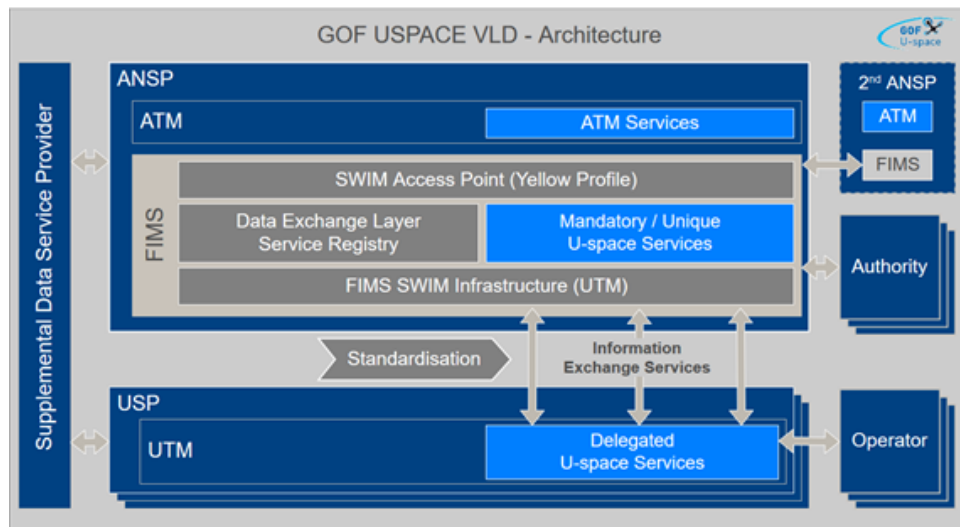


Figure 3 - GOF USPACE High Level Architecture [17]

To integrate existing U-space service implementations by different vendors, Information exchange services were introduced to facilitate standardised data exchange. They are described using formal templates, separating logical, technical and runtime concerns into different standard documents. Descriptions on logical level, so called Service Specifications, are technology agnostic. They enable a modular and open system, as they are easier to keep self-contained and foster reuse of concepts while technology evolves in incremental steps. Service Specifications allow for technical variants in implementation. In Technical Designs, by describing APIs and protocols clear contracts are defined for data exchange. Technical contracts are key in Service-Oriented Architecture, and important to facilitate interoperability for stakeholders in the system.

The relation of the Service Specifications, Technical Designs & Service Instances is depicted in Figure 4.

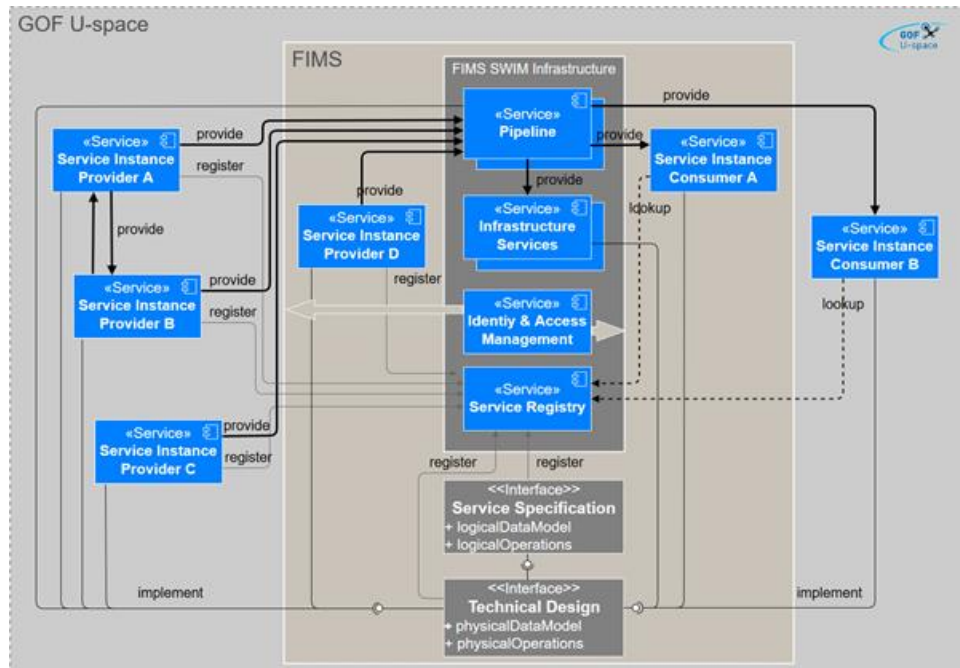


Figure 4 - GOF USPACE Service Descriptions [63]

Service Specifications were created in GOF USPACE to describe Information Exchange Services for:

- Telemetry (Position Data);
- Operation Plans (Drone Flight Plans);
- Aeronautical Information Management (AIM)/Geofencing (Geo-awareness);
- Alerts;
- Registration Data.

5G!Drones UAV Verticals will integrate existing products/systems based on the GOF USPACE architecture. Focus is put on the interface to the 5G ecosystem, which from a U-space perspective is seen as supplemental Data Service Provider. The existing service specifications will be reused and further evolved where necessary / applicable. These service specifications were created using templates, which have been evolved & proven in various domains and projects, and were even adopted by the International Association of Marine Aids to Navigation and Lighthouse Authorities (IALA) for specification for E-Navigation Technical services [64]. Based on the templates provided by the GOF USPACE project, services specification(s) for the interaction with network providers / trial Facilities will be created.

Information exchange services ensure data exchange between both ecosystems, they connect business services on 5G (in the project scope especially at the test Facilities) and on U-space side. Specification for those services will be done in WP3.

2.4. Target Use Cases and Trial Scenarios

2.4.1. Target Use Cases

As a part of the 5G!Drones project, four UAV-based use cases have been identified where the use of 5G technology would have the greatest impact. Within each use case there are several scenarios (10 in total) that the 5G!Drones consortium plans to trial using the 5G infrastructure present at ICT-17 selected Facilities (i.e. 5G-EVE and 5GENESIS), as well as at the University of Oulu and Aalto University 5G testbeds. The details of the use cases and their respective scenarios are as follows:

- a. **Use Case 1: UAV Traffic Management** - The goal of this use case is to demonstrate the safe and secure incorporation of multiple UAVs into air traffic:
 - i. **Scenario 1:** UTM command and control (C2) application: The purpose of this scenario is to showcase the C2 of multiple UAVs flying BVLOS using telemetry and video streaming data over 5G. The detailed description of this scenario can be found under Section 3.4.1.1 within D1.1;
 - ii. **Scenario 2:** 3D Map and supporting visualisation/analysis software for UTM: The main objective of this use case scenario is to assist UAV flight planners and operators in determining the best physical and 5G service conditions for flying their UAVs. A detailed description of this scenario can be found under Section 3.4.1.2 within D1.1;
 - iii. **Scenario 3:** UAV logistics: The purpose of this scenario is to demonstrate how UAVs through 5G Network capabilities can provide logistics solutions. Further details about this scenario can be found under Section 3.4.1.3 within D1.1.
- b. **Use Case 2: Public Safety** - The aim of demonstrating this use case is to showcase the need for 5G-enabled UAV applications to provide emergency response in public safety situations:
 - i. **Scenario 1:** Monitoring a wildfire: Within this scenario, a swarm of UAVs will be used to stream real-time video of a wildfire to fire fighters and rescue command centres. A detailed description of this scenario can be found under Section 3.4.2.1 within D1.1;
 - ii. **Scenario 2:** Disaster recovery: The goal of this scenario is to showcase the use of on-demand 5G connectivity provided by UAVs to disaster-affected individuals and assisting first response teams by providing video analyses of real-time videos streamed by UAVs. Further details of this scenario can be found under Section 3.4.2.2 within D1.1;
 - iii. **Scenario 3:** Police, incl. Counter-UAS: The purpose of this scenario is to demonstrate how to remotely pilot UAV and use video analytics for Police tasks, including C-UAS activities, thanks to 5G communication. The detailed description can be found under Section 3.4.2.3 within D1.1.
- c. **Use Case 3: Situation Awareness** - The objective of this use case is to showcase how UAVs equipped with IoT devices can be used in various applications to gain further awareness of a particular situation:
 - i. **Scenario 1:** Infrastructure inspection: Three sub-scenarios have been identified within this scenario which will showcase how UAVs equipped with IoT sensors and video camera can be used for inspection and surveillance applications. A detailed description can be found under Section 3.4.3.1;

- ii. **Scenario 2:** UAV-based IoT data collection: Within this scenario, UAVs equipped with sensors will collect data from multiple IoT devices on the ground and transmit the information to an edge server to conduct analyses. The detailed description of this scenario can be found under Section 3.4.3.2;
- iii. **Scenario 3:** Location of UE in non-GPS environments: This scenario intends to provide UAV operators and ground control stations (GCS) visibility of UAVs in non-GPS environments when they are flying in visual line of sight (VLOS) and BVLOS. A detailed description can be found under Section 3.4.3.3 within D1.1.

d. Use Case 4: Connectivity During Crowded Events

- i. **Scenario 1:** Connectivity extension and offloading: Within this scenario, UAVs will be used to understand network quality, video streaming and on-demand connectivity in the context of large showcasing events. The detailed description of this scenario can be found under Section 3.4.4.1 within D1.1.

2.4.2. The context of the selected 5G Facilities

As described earlier, the 10 use case scenarios are planned to be trialled at one of the four 5G Facilities located in France, Greece, and Finland. Given below is a brief summary of the four 5G testbeds and the scenarios that are going to be trialled within those Facilities:

5G-EVE: EURECOM's site which is a part of the 5G-EVE ICT-17 project, located in Nice, France, will be used to conduct multiple trials. The site deploys 5G NSA network, an OpenAirInterface RAN (OAI-RAN), and an ETSI-compliant MEC platform which will be used to trial the following use cases. A detailed description of 5G EVE's Facilities can be found in D1.2 and on that basis, a dedicated gap analysis is performed in Subsection 5.1.2, later in this document.

- Use Case 1: Scenario 1 - UTM command and control application;
- Use Case 2: Scenario 1 - Monitoring a wildfire;
- Use Case 2: Scenario 2 - Disaster recovery.

5GENESIS: DEMOKRITOS's site which is a part of the 5GENESIS ICT-17 project, located in Athens, Greece, will be used to trial the scenario provided below. The 5GENESIS Facility has OAI 5G-NR based on the NSA Option 3 and a MEC platform that will be used to trial the scenario. Further details of the 5GENESIS site can be found in D1.2 and on that basis, a dedicated gap analysis is performed in Subsection 5.1.4, later in this document.

- Use Case 4: Scenario 1 - Connectivity extension and offloading.

X-Network: The X-Network is a 5G testbed which is a part of Aalto University. The Facility's core network includes three virtualised EPC core network implementations and two MEC platforms which will be used to trial the following use case scenarios. A detailed description of the X-Network can be found in D1.2 and on that basis, a dedicated gap analysis is performed in Subsection 5.1.1, later in this document.

- Use Case 1: Scenario 3 - UAV logistics;
- Use Case 3: Scenario 2 - UAV-based IoT data collection.

5GTN: The University of Oulu (Finland) 5GTN network currently has an Option 3 NSA deployment and Nokia's MEC solution which will be used to trial the following use case scenario. A detailed

description of 5GTN can be found in D1.2 and on that basis, a dedicated gap analysis is performed in Subsection 5.1.3, later in this document.

- Use Case 1: Scenario 2 - 3D mapping and supporting visualization/analysis software for UTM;
- Use Case 2: Scenario 3 - Police, incl. Counter-UAS;
- Use Case 3: Scenario 1 - Infrastructure inspection;
- Use Case 3: Scenario 3 - Location of UE in non-GPS environments.

3. 5G ARCHITECTURE

This section gives a synthetic overview of the salient features of the 5G mechanisms that are relevant to the 5G!Drones architecture.

In particular, subsection 3.1 starts with a general description of the 5G System, through the outline of both the next-generation radio access network and 5G core network architectures. In that context, one of the significant challenges faced by the 5G!Drones project is the deployment and resource isolation of end-to-end slices in the context of heterogeneous 5G Facilities. In addition, to handle the heterogeneous requirements for low-latency, high throughput and support for massive numbers of IoT and other devices simultaneously and over a shared infrastructure, 5G!Drones targets to make heavy use of network slicing and Multi-access Edge Computing (MEC) [5]. Therefore, the concepts of Software Defined Networking (SDN) / Network Function Virtualisation (NFV), slicing mechanisms and MEC are respectively introduced in 3.1.2, 3.1.3 and 3.1.4. Similarly, the envisioned deployment of UAV services supported, notably to enforce advanced BVLOS operations, requires an understanding of the introduction of UAVs in 5G systems. Therefore, a careful consideration must be given to the notions of capacity, spectral efficiency, coverage and spectrum usage. In that regard, subsections 3.1.5 and 3.1.6 give a relevant summary of how these concepts are handled in the context of 5G. Finally, since 5G!Drones also addresses scenarios for which IoT-based sensors represent a significant aspect of the trials, the concept of Massive Machine-Type Communications (mMTC) is described in 3.1.7, along with the summary of how legacy 4G technologies like NB-IoT and LTE-M are set to coexist in the context of 3GPP 5G systems.

A second part of this section focuses on the different approaches taken by standardisation bodies such as 3GPP to consider the interoperability of 5G systems with UTM. As is explained in 3.2, 5G systems must meet the connectivity needs of unmanned aerial systems for the safe operation of UAVs. In addition, this insertion of UAVs in 5G networks must not be detrimental to the experience of the existing users. Therefore, both aspects are addressed by standardisation groups, in particular within 3GPP since Release 15.

Finally, section 3 gives a description of the potential interrelations between the 5G!Drones architecture with relevant projects from the 5G Infrastructure Public Private Partnership (5G PPP) and concludes with part 3.3.2, outlining the further enhancements to expect within 3GPP, mainly in the context of Release 17 and beyond.

3.1. Relevant 5G Features

3.1.1. NG-RAN, 5G Core

The 5G NG-RAN (Next Generation - Radio Access Network) key element is a Base Transceiver Station (BTS), which provides means for data transfer from the User Equipment (UE) to the 5G Core and Internet. More precisely, 3GPP defines a BTS as a RAN network element responsible for radio transmission and reception in one or more cells to or from the user equipment. A BTS may have an integrated antenna or be connected to an antenna by feeder cables [47]. Moreover, The NG-RAN architecture is described in [48], while the BTS for radio transmission and reception is defined by 3GPP in [49].

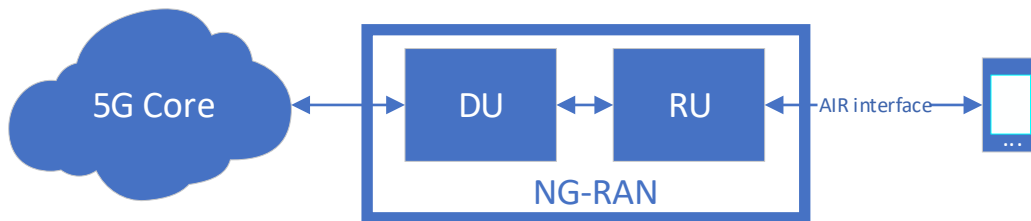


Figure 5 - 5G NG-RAN

NG-RAN, as depicted in Figure 5, consists of i) radio Digital Unit (DU), which itself encompasses a base band and functionality for controlling radio unit and ii) Radio Unit (RU), which contains transmitter(s) and receiver(s). The BTS hosts several functions like UE connection setup and release, routing of user plane data, radio resource management (including Radio Bearer Control, Radio Admission Control, Dynamic allocation of resources to UEs in both uplink and downlink, and so on).

NG-RAN typical installations may adopt the following implementation choices:

- Classical installations, in which all the radio network processing is done close to the antenna and Radiofrequency (RF). In addition, some options allow performing all the baseband processing in the centralised location or split functions to lower and higher layers. Delay critical functionalities are in the RF unit (low layer) and less delay critical functions in the edge cloud unit (high layer). This type of split is referred to as Centralised Unit – Distributed Unit (CU-DU) split.
- Most implementations include CU-DU split, with some going further to also include exposure of Common Public Radio Interface (CPRI) creating a split in the radio equipment between a Remote Unit (RU), Distributed Unit (DU) and Centralised Unit (CU) [10].

Furthermore, 5G Network deployment types in 3GPP Release 15 include different options [78] either with the evolved packet core (EPC) or with the 5G Core network (5GC) [50]. The 5G system, which involves a 4G element, is called a Non-Standalone solution (NSA) and system without the 4G element is referred to as Standalone (SA). In the SA solution, both user plane and control plane use the 5G Core. The SA network allows lower latency and faster setup time, plus new end-to-end services. In general, the NSA solution with dual connectivity to the LTE elements (as depicted in option #3 in Figure 6) seems to be a favoured option when starting a 5G network deployment, as it provides 5G data rates for enhanced mobile broadband. In addition, it allows operators to reuse existing investments for the EPC.

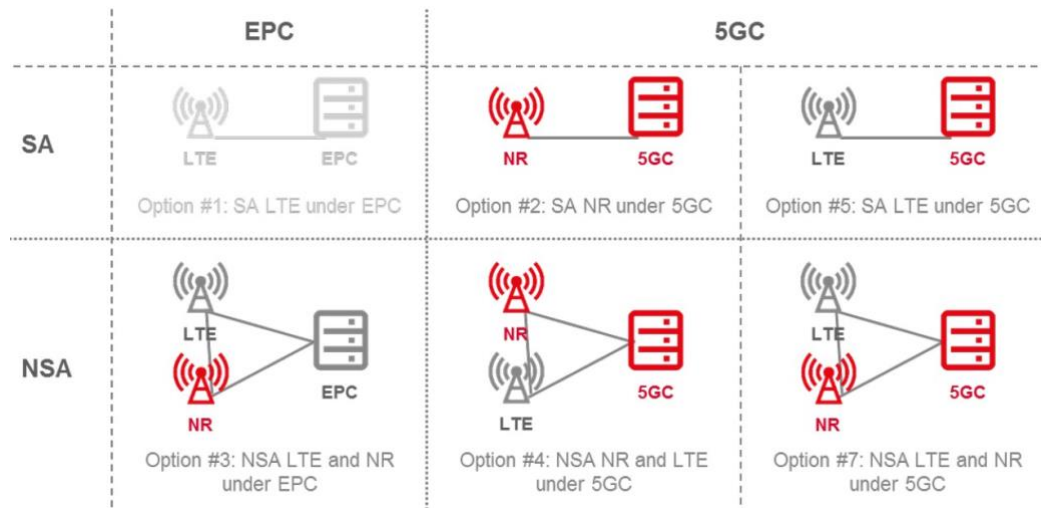


Figure 6 - 4G and 5G deployment options [78]

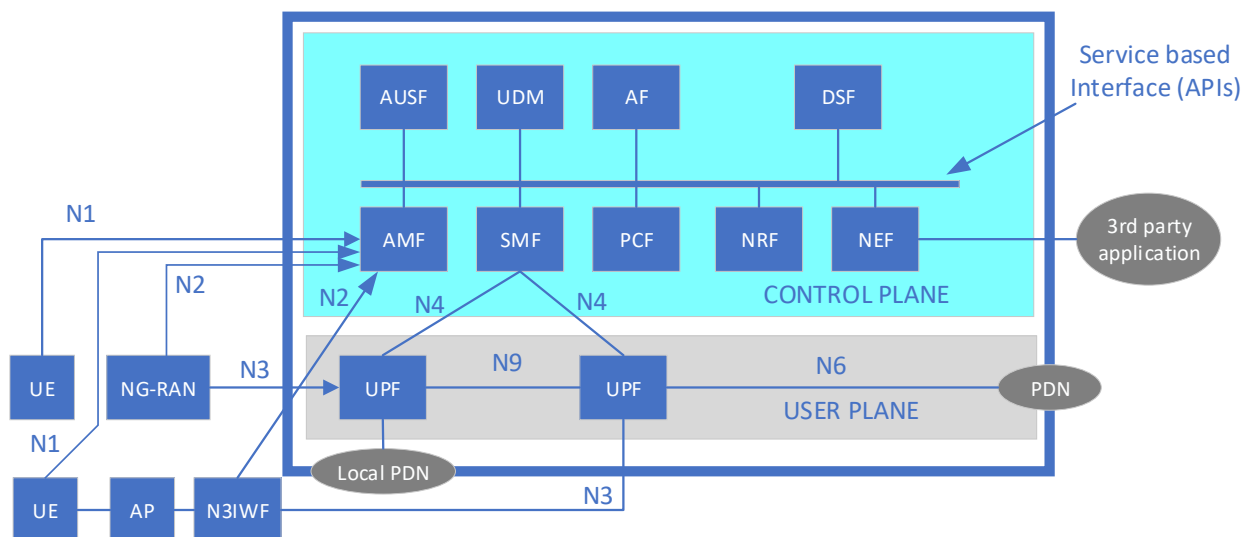


Figure 7 - 5G Core Services Based Architecture

5GC brings the concept of Services-Based Architecture (SBA). In the SBA representation, the NG-RAN is connected to 5GC via NG-C to the Access and Mobility Management Function (AMF) and NG-U to the User Plane Function (UPF). A brief description of the prominent 5GC basic elements, depicted in Figure 7 can be given as follows:

- A user plane, which takes care of the actual data flow:
 - UPF takes care of user data and supports flow-based QoS;
 - N3IWF (Non-3GPP Interworking Function) is a core network function for the integration of the stand-alone untrusted non-3GPP access to core.
- A control plane, which takes care of following functions:
 - AMF (Access and Mobility Management Function) to manage access control and mobility;
 - AUSF (Authentication Server Function) facilitates an authentication framework;

- UDM (Unified Data Management) stores subscriber data and profiles;
- SMF (Session Management Function) is the only function which establishes and manages sessions for all access types according to the network policy;
- AF (Application Function) for applications;
- PCF (Policy Control Function) takes care of QoS. Moreover, it supports network slicing, roaming and mobility policies;
- NRF (Network Repository Function) provides registration and discovery functionality;
- DSF (Data Storage Function) for data storage;
- NEF (Network Exposure Function) is an extension of the Service Capability Exposure Function in 4G networks. It is worth noting that from the UAV Vertical viewpoint, the NEF service is the contact point to 5G, as the NEF exposes 5GC functionalities to third parties.

3.1.2. Principles of SDN/NFV

This section builds on-top of the 5GENESIS work on NFV and SDN [79], with adaptations towards the specific context of 5G!Drones.

3.1.2.1. Network Function Virtualisation (NFV)

NFV technology was initiated in 2012 by the European Telecommunications Standards Institute (ETSI) NFV Industry Specification Group (NFV ISG), to allow customers to transfer the networking functions from vendor-specific and proprietary hardware appliances to software hosted on Commercial Off-The-Shelf (COTS) platforms [19]. The main idea is to provide the network services in virtual machines (VMs) working in Cloud infrastructures, where each VM can perform different network operations (e.g. firewall, intrusion detection, deep packet inspection, load balancing) [20]. The main benefits of deploying network services as virtual functions are: (1) flexibility in the allocation of network functions in general-purpose hardware; (2) rapid implementation and deployment of new network services; (3) support of multiple versions of service and multi-tenancy scenarios; (4) reduction in capital expenditure (CAPEX) by managing energy usage efficiently; (5) automation of the operational processes, thus improving efficiency and reducing operational expenditure (OPEX) costs.

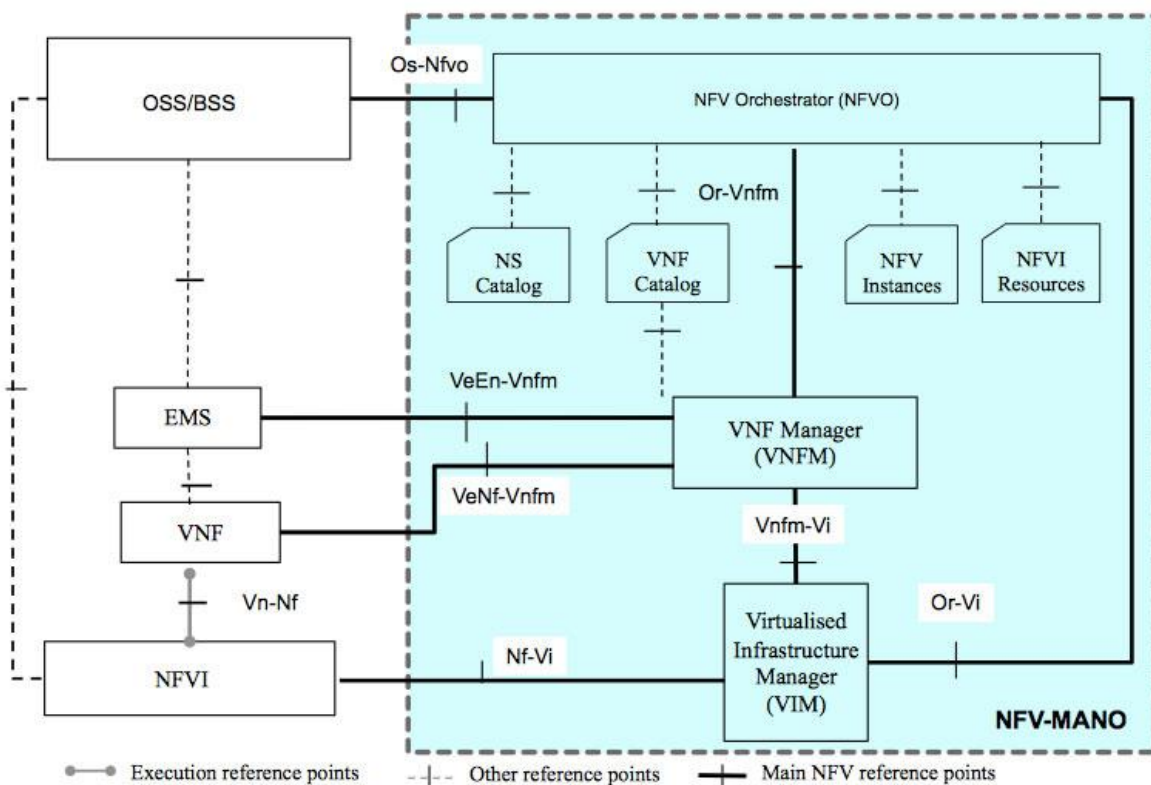


Figure 8 - NFV MANO Architecture [79]

The NFV Architecture depicted in Figure 8 is comprised of four main functional elements [21]:

- **The Virtual Network Function (VNF)** layer virtualises a certain NF, that operates independently of others. A particular VNF can run on one or more VMs and it can be divided into several sub-functions called VNF Components (VNFCs). VNFCs monitoring is performed using Elemental Management Systems (EMSs). Automation of the operational processes is feasible and results in improvement of the efficiency and reduction of the OPEX costs.
- **The NFV Infrastructure (NFVI)** is comprised of all the hardware and software required to deploy, operate, and monitor the VNFs. Particularly, NFVI includes a virtualisation layer necessary for abstracting the hardware resources (processing, storage, and network connectivity) to ensure independence of the VNF software from the physical resources. The virtualisation layer is usually composed of virtual server (e.g. Xen [22], Linux-KVM [23], Dell-VMware [24], etc.) and network (e.g. VXLANs [25], NVGRE [26], OpenFlow, etc.) hypervisors. The NFVI Point of Presence (NFVI-PoP) defines a location for network function deployments as one or many VNFs.
- **NFV management and orchestration (MANO)** is comprised of three components:
 - *The Virtualised Infrastructure Manager (VIM)*, which manages and controls the interaction of VNFs with physical resources under its supervision (e.g. resource allocation, deallocation, and inventory),
 - *The VNF Manager (VNFM)*, which is responsible for managing the VNF life-cycle (e.g. link initialisation, suspension, and termination),

- *The NFV Orchestrator (NFVO)*, which is responsible for realising network services on NFVI. Also, NFVO performs monitoring operations of the NFVI to collect information regarding operations and performance management.
- **Operations support systems and business support systems (OSS/BSS)** element comprises the legacy management systems and assists MANO in the execution of network policies. The two systems (OSS and BSS) can be operated together by telecommunications service providers or operators, either automatically or manually to support a range of telecommunication services.

3.1.2.2. Software Defined Networking (SDN)

The basic architecture of SDN uses modularity-based abstractions, similar to formal software engineering methods. A key abstraction of the SDN paradigm is the separation of the network control and forwarding planes. Conceptually, in SDN networks, resources are treated as a dynamic collection of arbitrarily connected forwarding devices with minimal intelligence. A typical SDN architecture divides processes such as configuration, resource allocation, traffic prioritisation, and traffic forwarding in the underlying hardware, using a 3-tier structure consisting of application, control, and data planes as highlighted below and depicted in Figure 9.

- **Tier 1 - Data (forwarding) plane:** The Data plane is the set of network physical components (switches, routers, virtual networking equipment, firewalls, middle box appliances, etc.), almost the same as in conventional networks. It aims at efficiently forwarding the network traffic based on a certain set of rules as instructed by Tier 2 - Control plane. That way, SDN technology makes the hardware (physical) infrastructure of the network rather flexible, by removing intelligence and isolated configuration per network element, and moving these functionalities to the control plane.
- **Tier 2 - Control plane:** The Control plane contains the logic to decide on how traffic can be routed through the network from one node to another based on end user application requirements. Such control logic is incorporated into external software application elements called SDN controllers. An SDN controller handles all Tier-1 forwarding devices by translating individual application requirements and business objectives (e.g. traffic prioritizing, access control, bandwidth management, QoS) into relevant programmable rules and announcing them to the data plane. By introducing programmability through these rules, flow tables can be manipulated in individual elements in real time, based on network performance and service requirements.
- **Tier 3 - Application plane:** The Application plane is the layer to include all applications and services of the network. Conceptually, the application plane is situated above the control plane to enable applications communicating with data plane through requesting network functions from control plane, while performing network related tasks. The Application plane uses APIs to capture the individual application parameters (delay, throughput, latency, etc.), based on which the SDN controller configures the individual network elements in the data plane for efficient traffic forwarding [27], [28].

The SDN controllers represent the focal point in the SDN system to oversee and manage the flow of traffic among southbound switches/routers (network-wise) by using APIs according to each application requirements. In order for an SDN controller to perform such tasks, it requires information regarding the state of the underlying network provided by collections of pluggable modules, which perform different information gathering procedures about the data link layer devices, providing full inventory of the network below, as well as devices capabilities. In addition, when the SDN controller has full view of the network, it adds extensions and bundles to improve the controller capabilities and provide customised

forwarding rules created using algorithms that analysed information and statistics gathered from the network.

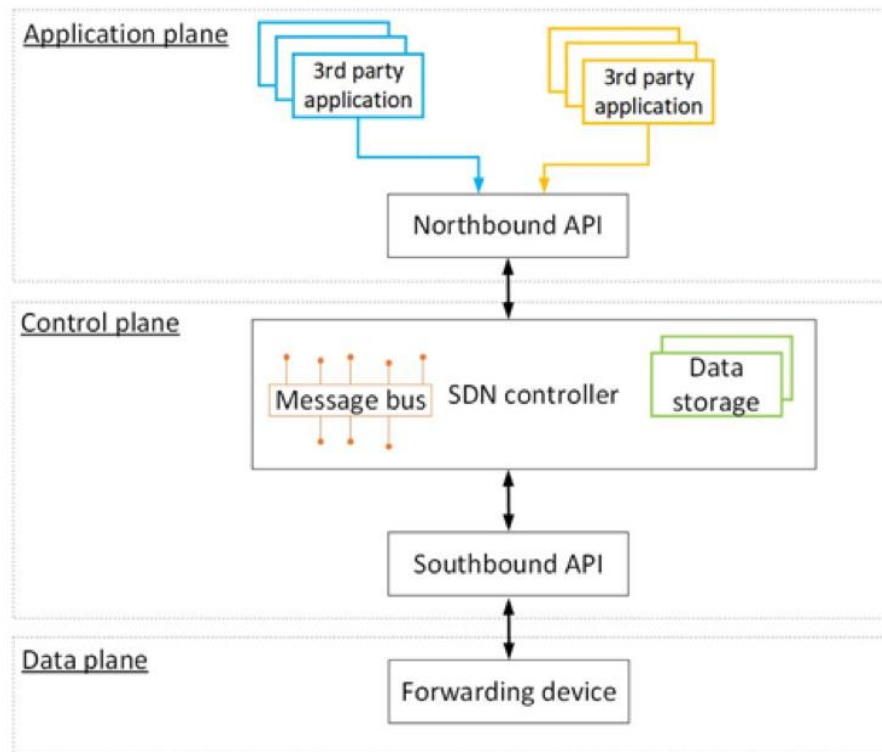


Figure 9 - Three-tier structure of a typical SDN controller [79]

There are two different approaches to reach the logical centralisation of the SDN Control Layer - Single and Distributed controller [29]:

- **Single Controller:** In single controller implementation, only one instance of an SDN controller exists in the network. All the switches are connected and controlled by that single machine in a centralised manner. Many early SDN adopters are using this solution.
- **Distributed Controller:** The distributed controller addresses the two principal issues that appear in the single controller approach: (a) Scalability, when the SDN controller has to handle multiple forwarding path requests from switches, and (b) Robustness, when, in case of a controller failure, switches are not able to forward new packets and eventually the entire network collapses. In the distributed controller approach, the SDN control plane consists of multiple SDN Controllers, which can share the load in the network equally. Furthermore, one controller can take over another controller when it crashes, thus fixing both issues that exist in the single SDN controller.

3.1.3. Slicing Mechanisms

Network slicing is relatively a new concept that allows for the creation of multiple network instances over a shared infrastructure. The NGMN [30] has proposed the widely used description of network slicing. In general, network slices are dynamic, virtual network instances, mutually isolated and typically built on a distributed cloud infrastructure, in which the slice is implemented as a set of interconnected, softwareised network functions. The main enabler of network slicing ETSI NFV MANO [2] framework that is used for slice orchestration and management. The MANO is responsible for converting the abstracted description of a slice into a set of network functions providing their optimal placement within

the infrastructure during the slice deployment phase and dynamically allocates resources to slices during their runtime. There are multiple benefits of network slicing:

- Each network slice can be properly customised to its service(s);
- Slices can be deployed on-demand;
- Slices are inherently isolated;
- Slice tenant does not need to own any infrastructure;
- A possibility of delegation of slice management (partially or fully) to slice tenants.

The economic aspect of infrastructure mutualisation and multi-tenancy is also positive because the capital expenses associated with the creation of a single network slice and further operational costs will be lower in comparison to the classical case. Due to the mentioned features, the network slicing technology will revolutionise the way in which networks and services are built and operated. The slicing concept is also seen as a key enabler of 5G. At present most researchers use the centralised management and orchestration for network slicing as defined by ETSI NFV MANO [31] where the network slice is treated just as a MANO Network Service (NS).

The works of 3GPP on 5G network slicing follow the NGMN concept. According to 3GPP, the universal, all-services network (like LTE so far) will be sliced into parallel separate networks specifically tuned to support specific classes of services with distinct characteristics. The 5G RAN (NR) is treated separately from 5G Core (5GC). Moreover, the independent slicing of system planes (user/control) and a further split of control plane functions into common and slice-specific ones is described in [32]. The common control plane functions include slice selection, authentication and mobility management. One of the benefits of such an approach is the effective handling of the handover of UEs that are simultaneously attached to several slices. The 3GPP reports [33], [34], [35] and [36] describe generic and network slice-specific management and orchestration of softwarised networks. The already published 3GPP standards concern topics related to slice management [37], provisioning [38], [39], selection [40] and security [41]. The approach of 3GPP is suited for mobile networks and tightly coupled with the 3GPP network architecture defined in Releases 15 and 16. It does not go into details of underlying network slicing technology, referring rather to ETSI NFV framework mechanisms, except for the slice selection mechanisms. The 3GPP defines a Communication Service that uses a Network Slice (NS). The network Slice is typically composed of multiple Network Slice Subnets (NSS) which in turn are composed of Network Functions (NF).

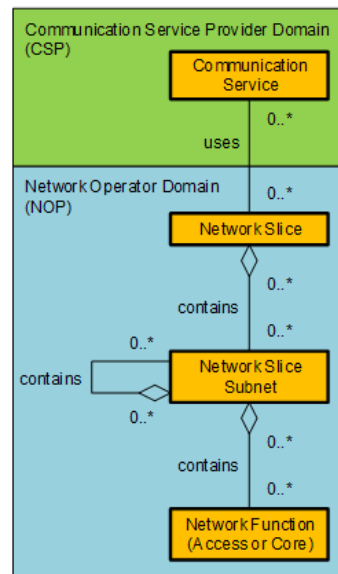


Figure 10 - Network Slice Subnets, Network Slice and Communication dependencies (based on [34])

The 5G System (5GS) allows for instantiation of multiple Network Slice Instances (NSI) or Network Slice Subnet Instances (NSSI) as shown in Figure 10. Several NSIs may share the same NSSI (as shown in Figure 11). Each NSSI or NSI has its unique identifier.

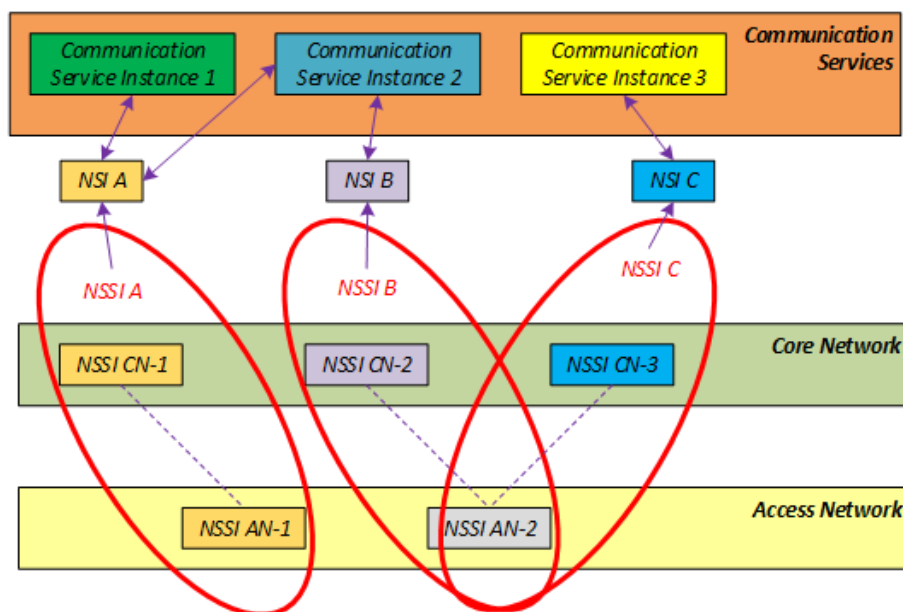


Figure 11 - Creation of end-to-end 3GPP compliant slices (based on [37])

The network slicing support by NR is defined in [42]. According to this document NR is aware of the existence of slices, traffic for each slice is handled by different PDU sessions. In opposite to generic slicing, the NR slicing is not using MANO but is based on Resource Blocks scheduling or L1/L2 configurations. For slice selection, the Single Network Slice Selection Assistance Information (S-NSSAI) issued by UE or 5GC is used. In NR there is slice-aware admission and congestion control – in case of overloading of a requested slice, the UE may be attached to default one. The slice coverage may

be limited to selected areas only, and outside them the UE may be also attached to some default general NSI.

The 5GS in SA implementation is needed in order to support network slicing. The architecture of 5GC with marked red components involved (supporting) in network slicing is shown in Figure 12.

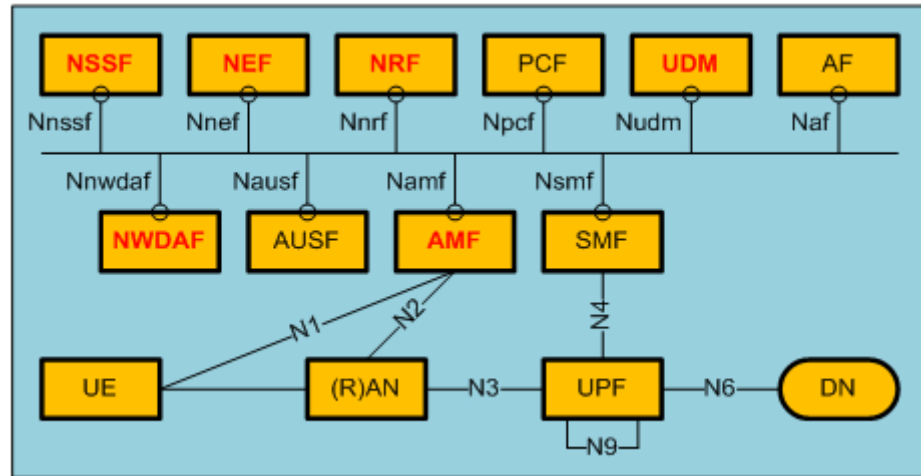


Figure 12 - 5GC support for network slicing (based on [7])

The role of the control plane functions in network slicing is the following [7]:

- Access and Mobility Management Function (AMF) – is a common function for all slices to which the UE is attached;
- Network Slice Selection Function (NSSF) plays a key role in network slicing. It is used for slice selection;
- Network Exposure Function (NEF) can be attached to each NSI/NSSI;
- Network Functions Repository Function (NRF) keeps information about functions allocated to a slice;
- Network Data Analytics Function (NWDAF) allows for data analytics on a per slice level;
- Unified Data Management (UDM) keeps information about users' subscriptions to slices (access rights, etc.).

The UE can be attached up to 8 slices of the same network operator using one signalling connection for all of them. The multi-operator attaching is not considered. In case of such requirement, the dual/multi-SIM UE has to be used. The following Slice/Service Types (SSTs) are currently defined:

- eMBB – enhanced Mobile Broadband;
- mMTC – Massive Machine Type Communication;
- URLLC – Ultra Reliable Low Latency Communication;
- V2X – Vehicle to X slice type used for car communications.

The first three ones are the classes defined by ITU-R [43] and further commonly followed by different bodies and organisations. The last one has been recently added by 3GPP in R16. Other SSTs (e.g. for UAVs C2 transmission) may be added in the future.

There are four categories of network slice management operations. The first one is related to slice preparation, the second one to slice installation, configuration and activation, the third one is related to slice run-time management, and the fourth one deals with slice instance decommissioning (see Figure 13).

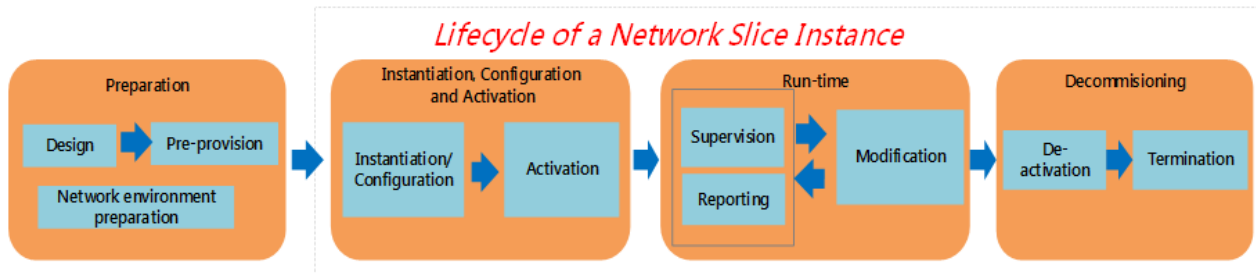


Figure 13 - Network slice instance management phases [34]

The general information used to describe a network slice instance may include:

- Resource model information: describes the static parameters and functional components of network slice, network slice type (e.g. eMBB), priority, etc.;
- Management model information: describes the information model used for network slice lifecycle management;
- Capability model information: describes the capability (e.g. service type, UE mobility level, density of users, traffic density), QoS attributes (e.g. bandwidth, latency, throughput) and capacity (e.g. maximum number of UEs).

The slice tenant, according to [38] has the following management rights related to its slice instances:

- Exposure of network slice management data: enable the network slice management service consumer to obtain network slice management data (e.g. performance and fault management data);
- Exposure of network slice management capability: enable authorised network slice management service consumer to obtain certain management capability to manage the network slice instance (e.g. provisioning) through the exposure interface;
- Creation of a 3GPP NF: to enable the authorised consumer to request creation of an instance of 3GPP NF (VNF);
- Configuration of a 3GPP NF instance: to enable the authorised consumer to request configuration of a 3GPP NF instance;
- Network slice resource capacity planning: to calculate the capacity of network slice instances and network slice subnet instances;
- Network slice subnet management with assigned priority: to assign priority on the existing network slice subnet instance(s).

The work on network slicing is still in progress. Yet, there is no commercial 5G network deployment yet with support of network slicing.

3.1.4. Multi-Access Edge Computing

Multi-access edge computing (MEC) is an Industry Specification Group (ISG) within ETSI aiming to leverage IT and cloud-computing capabilities within the mobile telecommunications networks [6]. Ultra-low latency and high-bandwidth along with real-time access to radio network information that can be utilised by applications are some of the characteristics of the edge environment created by the ETSI MEC standard. On the 3GPP domain, a set of enablers to support edge computing are given in the 3GPP TS 23.501 system architecture specification [7]. In addition, it is mentioned that the NGC may expose network information and capabilities to an Edge Computing Application Function. The idea is to handle MEC as a 5G-application function via these enablers.

Multi-access edge computing (MEC) provides a new ecosystem and value chain. Operators can open their RAN edge to authorised third-parties, allowing them to flexibly and rapidly deploy innovative applications and services towards mobile subscribers, enterprises and vertical segments [1].

MEC implements:

- A MEC platform, and an Edge Cloud to run applications that control drones;
- Cloud resources to run VNFs;
- Service elasticity: capacity to increase/decrease resources used by the UAV slices.

Edge computing comes with the promise of low latency, and this is critical for the delay-sensitive components that many of the 5G!Drones use case scenarios involve. Moreover, edge computing is acknowledged as one of the key pillars for meeting the demanding KPIs of 5G, especially as far as low latency and bandwidth efficiency are concerned [1].

5G networks based on the 3GPP 5G specifications are a key future target environment for MEC deployments. The 5G system specification and its Service-Based Architecture (SBA) leverage the service-based interactions between different network functions, aligning system operations with the network virtualisation and SDN paradigms [1] as illustrated in Figure 14.

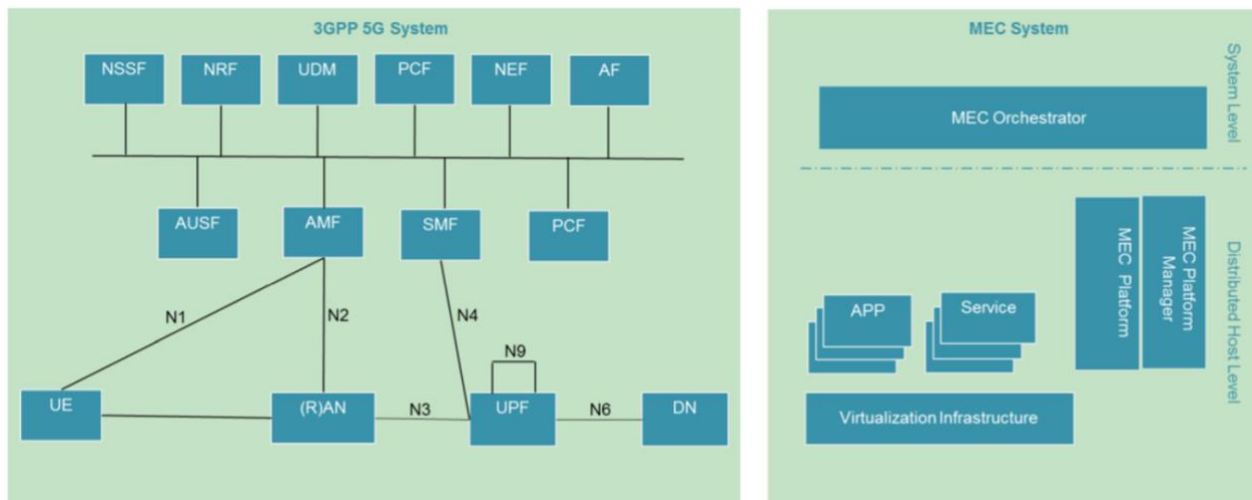


Figure 14 – 5G Service Architecture and a generic MEC system architecture [1]

With 5G, the starting point is different, as edge computing is identified as one of the key technologies required to support low latency together with mission critical and future IoT services. This was considered in the initial requirements. The system was designed from the beginning to provide efficient and flexible support for edge computing to enable superior performance and QoE [1], [2]. Besides, although all ETSI MEC specifications are defined with the intent of enabling a self-contained MEC cloud able to exist in different cloud environments, in most telco environment the need is to extend NFV into the MEC realm. To that end, ETSI MEC has defined a MEC-in-NFV reference architecture in [3] and illustrated in Figure 15.

Generic reference architecture

This reference architecture shows the functional elements that comprise the multi-access edge system and the reference points between them. There are three groups of reference points defined between the system entities:

- Reference points regarding the MEC platform functionality (Mp);
- Management reference points (Mm);
- And reference points connecting to external entities (Mx).

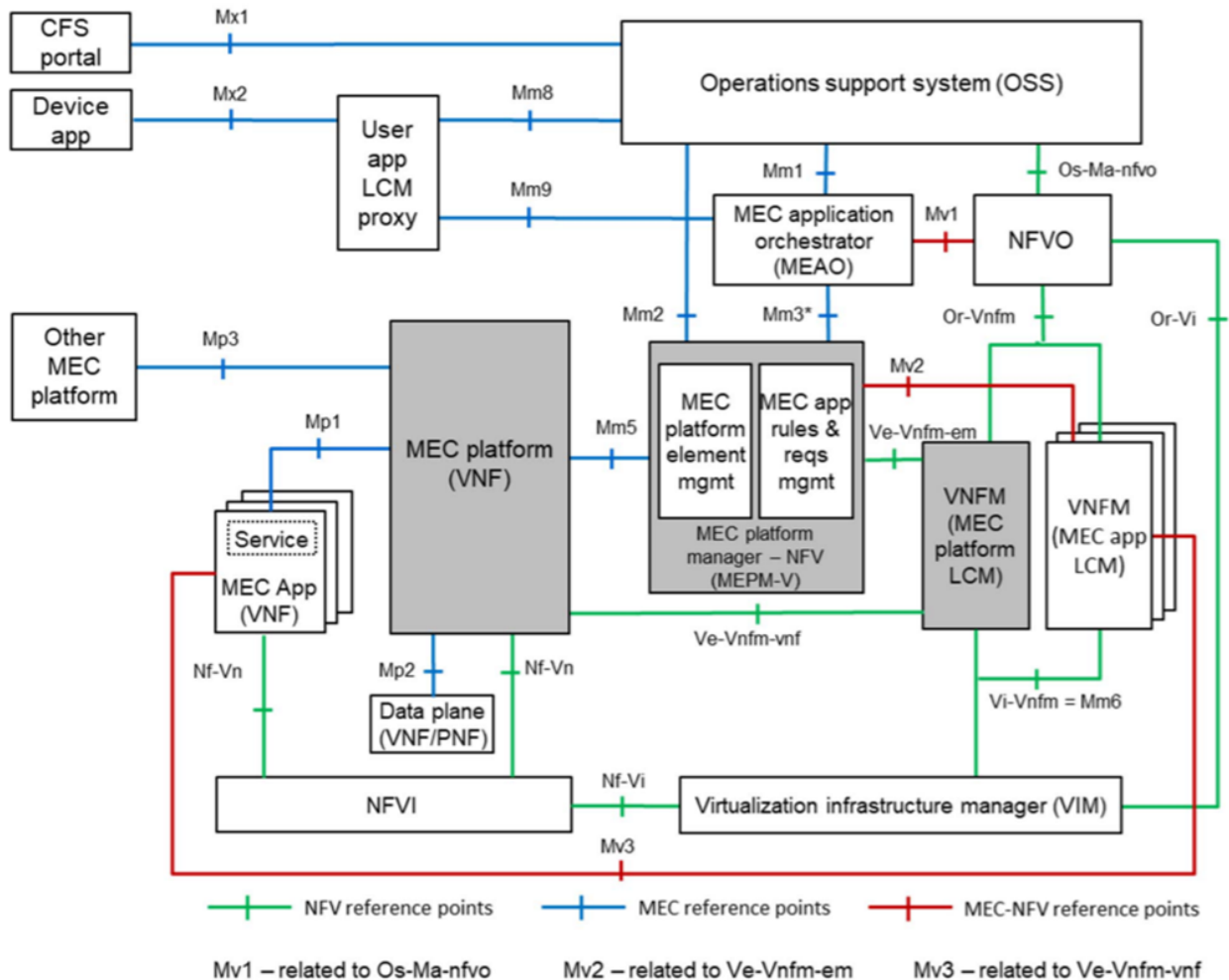


Figure 15 – Multi-access edge system reference architecture variant for MEC in NFV [3]

The multi-access edge system consists of the MEC hosts and the MEC management necessary to run MEC applications within an operator network or a subset of an operator network. The MEC host is an entity that contains a MEC platform and a virtualisation infrastructure which provides compute, storage, and network resources, for the purpose of running MEC applications. The MEC platform is the collection of essential functionality required to run MEC applications on a particular virtualisation infrastructure and enable them to provide and consume MEC services. The MEC platform can also provide services. MEC applications are instantiated on the virtualisation infrastructure of the MEC host based on configuration or requests validated by the MEC management.

The MEC management comprises the MEC system level management and the MEC host level management. The MEC system level management includes the Multi-access edge orchestrator as its core component. The MEC host level management comprises the MEC platform manager and the virtualisation infrastructure manager, and handles the management of the MEC specific functionality of a particular MEC host and the applications running on it.

The MEC host is an entity that contains the MEC platform and a virtualisation infrastructure which provides compute, storage, and network resources for the MEC applications. The virtualisation infrastructure includes a data plane that executes the traffic rules received by the MEC platform, and routes the traffic among applications, services, DNS server/proxy, 3GPP network, other access networks, local networks and external networks.

Figure 16 shows the ability to offer an environment where the MEC applications can discover, advertise, consume and offer MEC services, including, when supported, MEC services available via other platforms (that may be in the same or a different MEC system) [4].

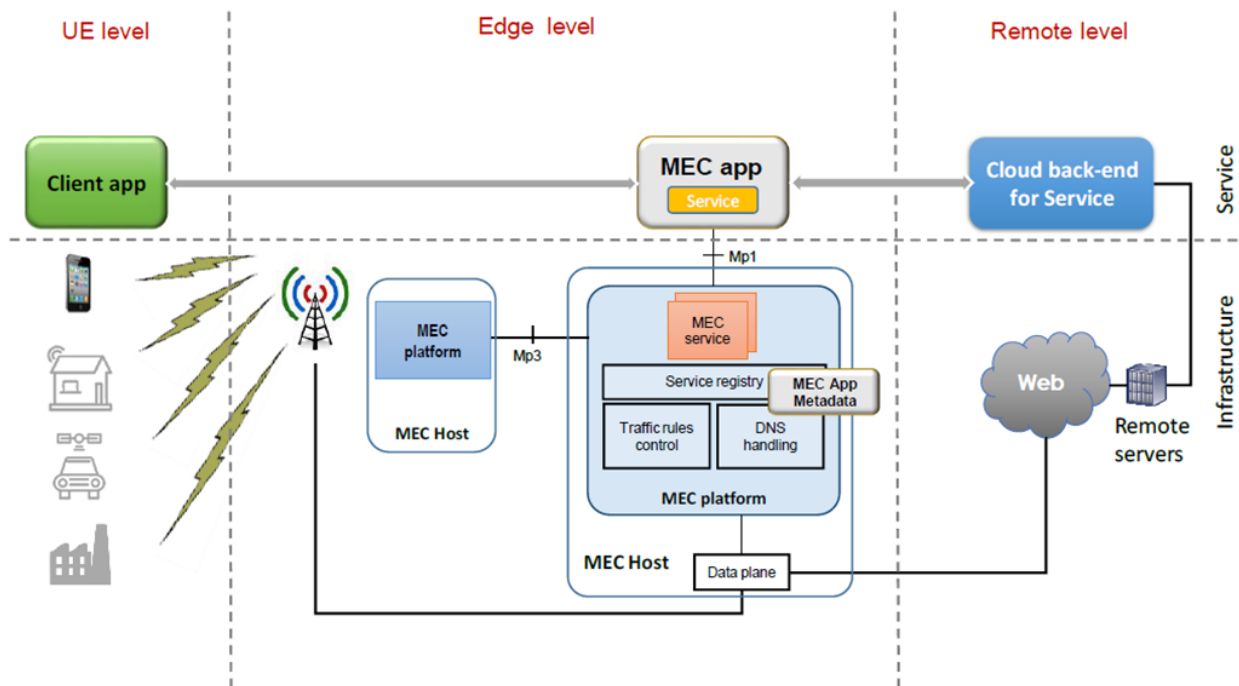


Figure 16 – New application development paradigm introduced by MEC [4]

MEC enables the implementation of MEC applications as software-only entities that run on top of a virtualisation infrastructure, which is located in or close to the network edge. The MEC framework shows the general entities involved. These can be grouped into system level, host level and network level entities, as depicted in Figure 17.

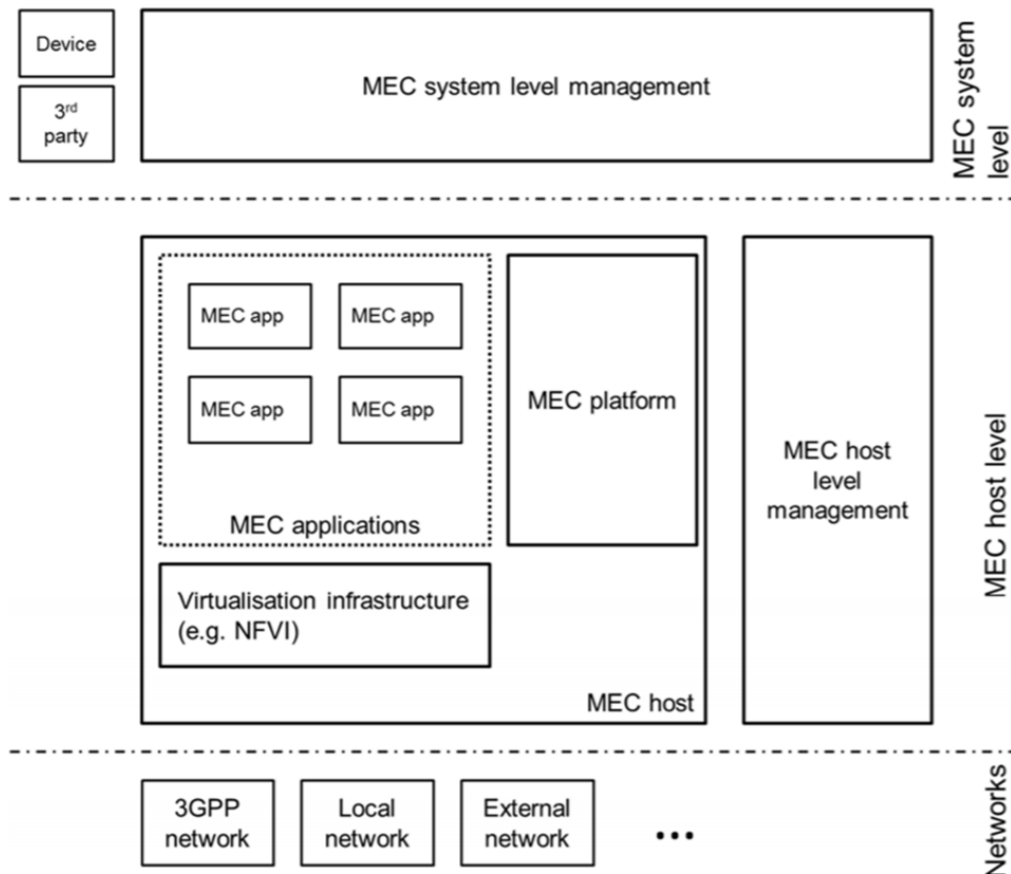


Figure 17 - Multi-access edge computing framework [3]

Furthermore, with respect to network challenges, [8] summarises the most salient issues in deploying MEC in 4G networks, thereby preparing for the evolution towards 5G.

For the 5G NSA deployments the resulting MEC deployment options are summarised below:

- **Bump in the Wire:** In this scenario, the MEC platform sits on the S1 interface of the system architecture and the MEC host's data plane has to process user traffic encapsulated in GTP-U packets. Apart from the requirement on the MEC server to handle GTP tunnels, this scenario poses challenges to operations such as lawful interception and charging possibly mandating a dedicated solution such as a MEC GW to be implemented. Low latency is supported by installing the MEC platform all the way down to the eNodeB.
- **Distributed EPC:** In this scenario, the MEC data plane sits on the SGi interface. The MEC applications can be co-located with the evolved packet core (EPC) functions in the same MEC host. In this case, the Home Subscriber Server (HSS) is co-located with the EPC as well, and there is no need for a working backhaul to keep the local service running. This type of deployment is typically used by first responders, public safety, and mission critical industrial sites. This scenario requires fewer changes to the operator's network and leverages standard 3GPP entities for session management and charging operations.
- **Distributed S/PGW:** This scenario is similarly to the Distributed EPC except that only SGW and PGW entities are deployed at the edge site, whereas the control plane functions such as the Mobility Management Entity (MME) and HSS are located at the operator's core site.

- **Distributed SGW with Local Breakout (SGW-LBO):** Local breakout at the SGWs is a new architecture for MEC to achieve a greater control on the granularity of the traffic that needs to be steered such as to allow the users to reach both the MEC applications and the operator's core site application in a selective manner over the same APN.

The deployment options above which distribute the EPC gateways at the edge, either co-located with or within the MEC host, can also be built using the CUPS paradigm standardised in 3GPP Release 14 and have the new User Plane built in the MEC host allowing the traffic to be locally steered.

Among the challenges identified to support the various MEC deployment options, such as Session Management, Lawful Interception, Charging, Security and MEC platform subscribers' identification, the Mobility Management is specifically critical as it affects, depending on the management option implemented, the Service Continuity and mandating MEC handover capabilities: Two scenarios are perceived:

- **Intra-MEC mobility:** The UE moves from one eNodeB to another, but is still in the coverage of the same serving MEC host. The MEC system should be able to route the traffic to the UE via the correct eNodeB and tunnel.
- **Inter-MEC mobility/MEC hand-over:** The UE moves out of the coverage area of the source MEC host to enter the coverage area of target MEC. In order to provide service continuity to the UE, the MEC system needs to relocate the service to the UE from the source to the target MEC. In the EPC MEC, SGW + PGW MEC, and CUPS MEC, SGW-LBO MEC, the MEC handover is supported using 3GPP standard S1 Handover with SGW relocation by maintaining the original PGW as anchor. Nevertheless, it is the MEC application's responsibility to synchronise at application level and maintain the session in the case of a stateful application.

In the evolution towards 3GPP Option 2 and SBA Architecture, there exist clear migration patterns for the MEC deployments above, as documented in [7], [8]. In the long term, 5G deployments will increasingly integrate fixed mobile networks infrastructures with cloud computing and MEC. Orchestration capabilities, which are already a key element for exploiting cloud computing capabilities, shall become an essential part of the operation of future 5G infrastructure. Virtualisation, Network Management and Orchestration, Network Function Virtualisation (NFV), 3rd Party Support and MEC Application Management are critical capabilities for successful deployments.

3.1.5. Beamforming

Beamforming in 5G allows providing better capacity, spectral efficiency and coverage, especially at high frequencies. In that regard, 3GPP R15 brought to 5G NR enhanced Massive MIMO, a Multiple Input Multiple Output multi-antenna transmission and reception technique, as well as beamforming capabilities for all new devices. Besides, 5G supports more transmission branches than LTE: in effect, 5G will support initially at least 64 transmit antennas while LTE supports up to 32 in R14. The horizontal beamforming works when the same signal from all antennas is sent with different phase-shifts at azimuth plane. The vertical beamforming works when the signal is modified at elevation plane. For further information on beamforming mechanisms, the reader may refer to the 3GPP RAN-level beamforming specifications [51].

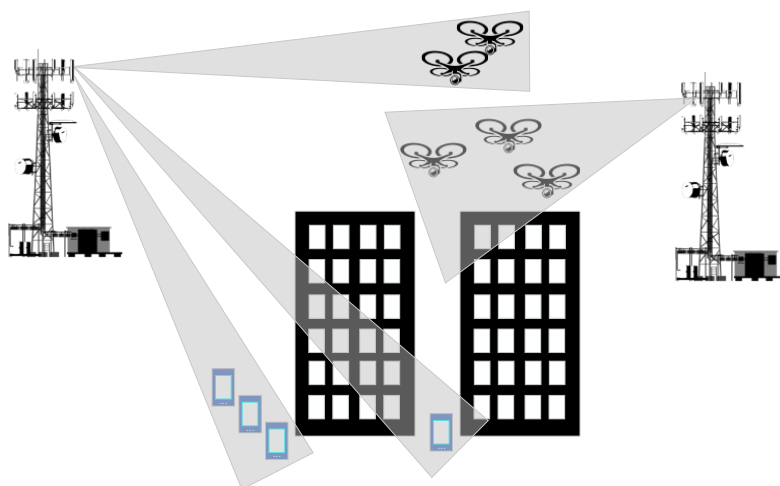


Figure 18 - 5G Beamforming benefits for UAVs

In the context of 5G!Drones, the expected basic benefit of beamforming is related to the efficient support of UAV UE connectivity. In effect, each UAV may benefit from a faster and more reliable wireless connection, as UAVs may depend on dedicated beams, as illustrated in Figure 18. In this type of 5G deployment, beamforming improves signal quality, in particular in indoor environments and at the edge of cells. To this end, beamforming requires more receiver and transmitting antennas both in the RAN and UAVs. Moreover, a key enabler for the efficient support of beamforming is the use of high frequency bands. When all conditions are met, 5G network is then able to provide more gain for UAV signals at horizontal and vertical separation and reduce inter-UAV interference, thereby providing additional gain for UAV signals at horizontal and vertical separation.






3.1.6. Spectrum and Spectrum Efficiency

As a general rule, radio spectrum must be considered as a finite physical resource. It is globally coordinated by ITU-R, the radio communication sector of the International Telecommunication Union (ITU) and within this organisation, spectrum license management is based on geographical areas: according to this principle, each country controls its spectrum licenses. In Europe, spectrum roadmap coordination is done by the Radio Spectrum Policy Programme (RSPP) [52]. In this regard, Table 1 gives a rough classification of the typical spectrum for respectively 4G and 5G.

Table 1 - High-level classification of the 4G and 5G radio frequency spectrum

Frequency area	4G	5G
Sub-6GHz	✓	✓
6GHz - 52.6 GHz	-	R15
Above 52.6 GHz	-	R16 and R17

Moreover, in 3GPP R15, multiple bands are defined for 5G, from 617 MHz to 40 GHz [80]. In later 3GPP R17, the aim is to expand to higher frequencies, in practice up to 114 GHz [81]. There are also research projects investigating even higher frequencies, such as ARIADNE for D-Band (100-170 GHz) [82]. In brief, the frequencies above 30 GHz are called millimetre waves, as the wavelength for this frequency is below 10 mm. The commercial 4G installations are focused to sub-6 GHz areas, see Figure 19 below.

	RAT/Band	Illustrative coverage comparison	Scenario
> 6 GHz	NR mmWave		Local coverage Peak data rate: 10Gbps
< 6 GHz	NR 3.5GHz mMIMO LTE 1800	 	Reuse of 1800 grid possible for Downlink Peak data rate: 1Gbps
< 1 GHz	NR 700MHz LTE 800 MHz	 	Deep indoor penetration Peak data rate: 100Mbps



 NR gNodeB
  LTE eNodeB

Figure 19 - Coverage and spectrum usage comparison between 4G and 5G [83]

The typical 4G system bandwidth ranges from 1.4 MHz up to 20 MHz. In contrast, the 5G system can be used to provide better eMBB service level for UAV by utilising millimetre waves in a specific area, as the bandwidth for the higher frequency range can reach up to 400 MHz. For 5G bands in the lower frequency range however, the maximum bandwidth will not exceed 100 MHz. It is also important to note that in the context of higher frequencies like 28 GHz or 39 GHz, the rain attenuation may strongly affect the signal quality; the 5G NR radio coverage values are therefore limited in this case, as Figure 20 illustrates. Consequently, networks operated with millimetre bands should be planned to areas where UAVs needs the best 5G eMBB service, like public crowded events at stadium or for temporary public safety applications. Centimetre waves can be utilised for providing URLLC services to UAVs in a wider geographical location, thereby offering more reliable, longer range drone communication channels in the sky. In a radio network planning, Mobile Network Operators (MNOs) seek to optimise available radio spectrum bandwidth based on data consumption. As currently, most MNO customers are located at ground level, the existing radio network plans do not particularly target the case of UAV evolving at higher altitudes.

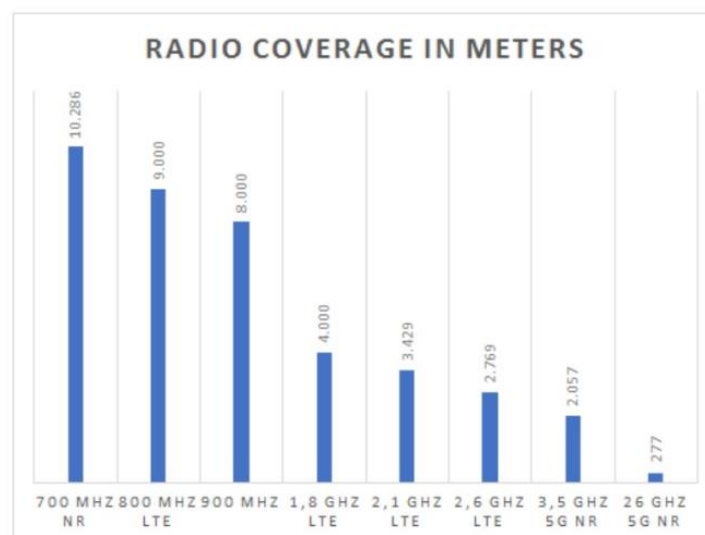


Figure 20 - Estimation of radio coverage for several 5G NR frequencies [10]

As shown in Figure 20, radio coverage significantly varies with the considered 5G NR frequency. This naturally has a strong impact on UAV communication support in 5G systems, in which NR-to-UAV, UAV-to-UAV and NR-to-regular-UE links may rely on different spectrum to avoid interference and optimise CSPs spectrum usage [10].

3.1.7. Focus on mMTC

As delineated in subsection 2.4.1, and presented in more details in deliverable D1.1, 5G!Drones investigates four (4) scenarios for which IoT-based sensors represent an important part of the trials: UC 1/Scenario 3 (“UAV Logistics”), UC 2/Scenario 1 (“Monitoring a wildfire”), UC 2/Scenario 3 (“Police, incl. Counter-UAS”) and UC 3/Scenario 2 (“UAV-based IoT data collection”). Moreover, the different 5G mechanisms presented in the previous paragraphs of Section 3, which largely address eMBB and URLLC requirements, are less relevant in this context. This subsection therefore outlines the principles of Massive Machine-Type Communications (mMTC), also referred to as massive Internet of Things (mIoT), as one of the main improvements offered by 5G. The rest of this subsection presents LTE-M and NB-IoT, which are the main 5G technologies for mMTC. For 5G, there are two standards that support mMTC: NB-IOT and LTE-M CatM1/2. Mobile IoT networks, using LTE-M or NB-IoT cellular technology, continue to gain traction for applications that require low power wide area (LPWA) connectivity. The LTE-M and NB-IoT networks will continue to evolve and will operate seamlessly both with existing networks and 5G NR (New Radio) connectivity. From the core network perspective, both the existing LTE Core (Enhanced Packet Core/EPC) and the new 5G core (5GC) will continue to support the evolution of Mobile IoT into the future [88].

NB-IoT is a narrowband radio technology developed for IoT. It is categorised as one of the licensed Low-Power Wide-Area Networks cellular technologies, which is especially suited for mMTC applications with low data rate that require low module cost, long battery lifetime and increased coverage. In its LTE R13, 3GPP has standardised NB-IoT and addressed different objectives such as indoor coverage, support of massive number of low throughput devices, delay sensitivity and low-power consumption. Further standardisation of NB-IoT was addressed by 3GPP R14 with respect to several topics including improved positioning support, multicast downlink transmission, etc. NB-IoT is naturally intended to support cellular networks and especially mMTC applications, which reflects one of the service categories of 5G.

LTE-M has two standards, specified by 3GPP as Cat-M1 and Cat-M2. This low power technology supports mobility, roaming, moderate data rates, real-time connectivity and voice support. LTE-M supports relatively high data rates and low latencies, as Table 2 summarises. This standard is therefore particularly effective for transferring photos and video clips from IoT cameras.

Table 2 - LTE Cat-M1, LTE Cat-M2, NB-IoT comparison [87]

	LTE Cat-M1	LTE Cat-M2	NB-IOT
Uplink	1 Mbit/s	7 Mbit/s	159 kbit/s
Latency	10 -15 ms	10 -15 ms	1.6 -10 sec
Bandwidth	1.4 MHz	5 MHz	180 -700 KHz

LTE-M was initially limited to a bandwidth of 1.4 MHz (Cat M1) in 3GPP R13 and some coverage enhancement features like frequency hopping and sub-frame repetitions. Then, Cat-M2 introduced the optional use of 5 MHz bandwidth and voice enhancement in 3GPP R14. 3GPP R15, in 2019, describes

Wake Up Signal (WUS) in the idle mode, early data transmission and latency optimisation. 3GPP R16, which will be finalised in June 2020, will describe coexistence between 5G NR and standalone LTE-M.

Compared to NB-IoT, the higher data rates provided by Cat-M1 means that more data can be sent through the network in a given timeframe. This is intended to benefit to applications that rely on speed of transmission, for example security or mission-critical reporting. Cat-M1 also has the advantage of being able to support voice transmissions, unlike NB-IoT, enabling support for a wider range of use cases. It is worth noting that on the other hand, LTE-M consumes in average slightly more energy than NB-IoT. Therefore, this complementarity explains that many operators are expected to support both CAT-M1 and NB-IoT in the short future [65], [66].

3.1.8. Multimedia Mission Critical Services

Among the scenarios identified by 5G!Drones, a subset specifically targets the context of public safety, as previously described in subsection 2.4.1. More precisely, Use Case 2 scenarios were identified with the aim to demonstrate the need for 5G-enabled UAV applications to provide emergency response in public safety situations. In the 3GPP context, a relevant standard is therefore related to Multimedia Mission Critical Services (MCS) [94]. MCS has been standardised by 3GPP since Release 13, which was completed in 2016. Mission Critical Push-To-Talk (MCPTT) [91] was first standardised to provide voice communication and was a first step in a series of other MCS functionalities demanded by the market. During 3GPP Release 14, which was completed in 2017, 3GPP added additional Mission Critical Services which are the Enhancements to MCPTT, Mission Critical Data (MCData) [93] and Mission Critical Video (MCVideo) [92].

With 3GPP Release 15, the Mission Critical Services are currently further evolved, mainly for the interconnection between Mission Critical Systems and MBMS APIs for MCS.

The MCS solution allows public safety users to access professional communication in groups and in private calls. The following services are enabled by this solution:

- Group and individual calls;
- Group and individual messaging;
- Group and individual multimedia messaging;
- Group and individual video calls;
- Emergency calls;
- Location and map services.

3.2. UTM Integration into Standardised 5G Systems

To ensure that the 5G systems can meet the connectivity needs of unmanned aerial systems for the safe operation of UAVs, as well as guarantee that other users of the network do not experience a loss of service due to their proximity to UAS, significant 3GPP Working Groups activities are taking place, and are presented in brief in [53].

In Release 15 [58], 3GPP addressed the implications of serving low altitude UAVs using LTE radio, that led to the report 36.777 (Enhanced LTE Support for Aerial Vehicles [56]), approved in January 2018. This activity had main focus on radio aspects for the support of UAVs in order to provide the coverage necessary for a growing population of low altitude UAVs in all types of environments - considering that most perceived problems are due to interference caused by the UAVs operating above the normal height

of UEs. In this respect, there were enhancements to TS 36.331 (Section 5.5.4 - Measurement report triggering) to address the issue of aerial UE interference to the base station (eNodeB), addressing above and below UE height thresholds to help the eNodeB to see the UAV and to deal with any potential interference. Other measures for signalling and to reduce interference by the UAV were also added. Notably, NR is expected to make greater use of beamforming antennas to reduce this interference but these additions could introduce new problems. UAVs may also experience “coverage holes in the air” as network planning and design is directed to ground-based users. Work reported in TR 38.811 [58], in the larger context of Non Terrestrial Networks (NTN), addressed the support for High Altitude Platforms (HAP) operating at altitudes between 8 km and 50 km, to provide services to either fixed very narrow aperture receivers or to portable hand-held receivers.

In Release 16, work on HAP is continued, and system and application layer aspects are put in perspective, through an initial study of service requirements for UAV identification leading to the approved 22.825 report on “Study on Remote Identification of Unmanned Aerial Systems” [59]. As noted in [54], the focus of R16 UAV study and normative work has been the concept of UAV identification by control data that can be transmitted via the 3GPP network between a UAV or UAV controller and a centralised network-based UTM function. The direct communication between UAVs, and UAVs and ground-based personnel (especially law enforcement) has also been considered to support collision avoidance use cases.

3GPP Release 17 extends the work through a study item on enhanced requirements for UAV services including specific KPIs relevant to UAVs. In TS22.125 [61], the term UxNB is introduced referring to the radio access node on-board UAV, defined to be the radio access node providing connectivity to UEs, which is carried in the air by an Unmanned Aerial Vehicle (UAV). The UxNB can also connect to the 3GPP core network like a normal ground Base Station [60].

The dedicated 3GPP SA6 group is studying the use cases and requirements regarding UAS identification and tracking in particular the application support/enabler functionalities for UTM and the service interactions between UAS and the UTM (e.g. flight route authorisation, location management, and group communication support). Furthermore, in 3GPP TS22.261, KPIs based on communication service are addressed such as KPIs for C2 traffic, UxNB, service restriction for UAV, and network exposure for the UAV. In TS22.125, the UAS reference model is included, as shown in Figure 21:

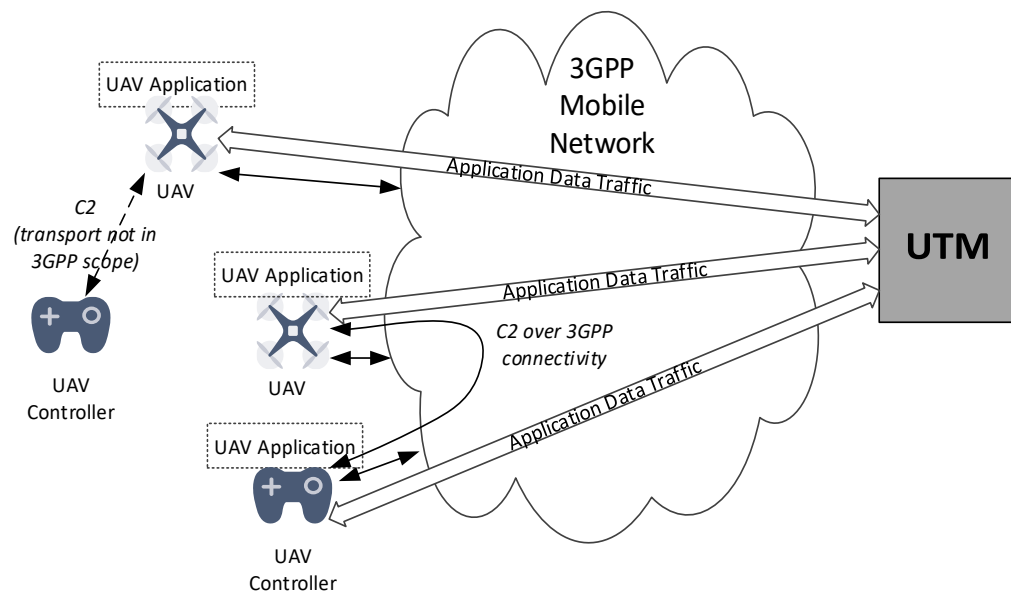


Figure 21 - UAS reference model in 3GPP ecosystem TS22.125 [61]

Moreover, in 3GPP Release 17, through TS22.125 [61] and TR22.829 [60], the communication model for C2 is analysed, as depicted in Figure 22:

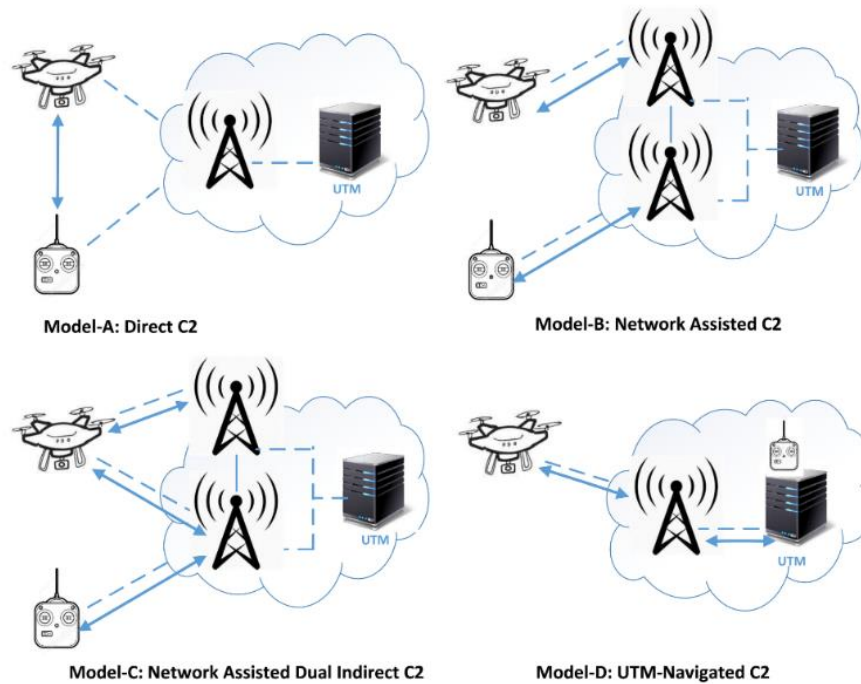


Figure 22 - C2 communication models (blue arrows show C2 communication links) [60]

3.3. Extended scope and opportunities

3.3.1. Interrelated 5G PPP Architectures

The 5G Infrastructure Public Private Partnership (5G PPP) is a joint initiative between the European Commission and European ICT industry, that notably includes ICT manufacturers, telecommunications operators, service providers, SMEs and researcher institutions. The 5G PPP is now in its third phase, initiated in Brussels in June 2018 via the launch of several prominent projects. The 5G PPP intends to deliver solutions, architectures, technologies and standards for the ubiquitous next generation communication infrastructures of the coming decade [68]. It is also worth highlighting that the Phase 2 and Phase 3 5G PPP projects launched in 2018 and 2019 are consistent with the 3GPP R15 and R16 timetables, as illustrated by Figure 23.

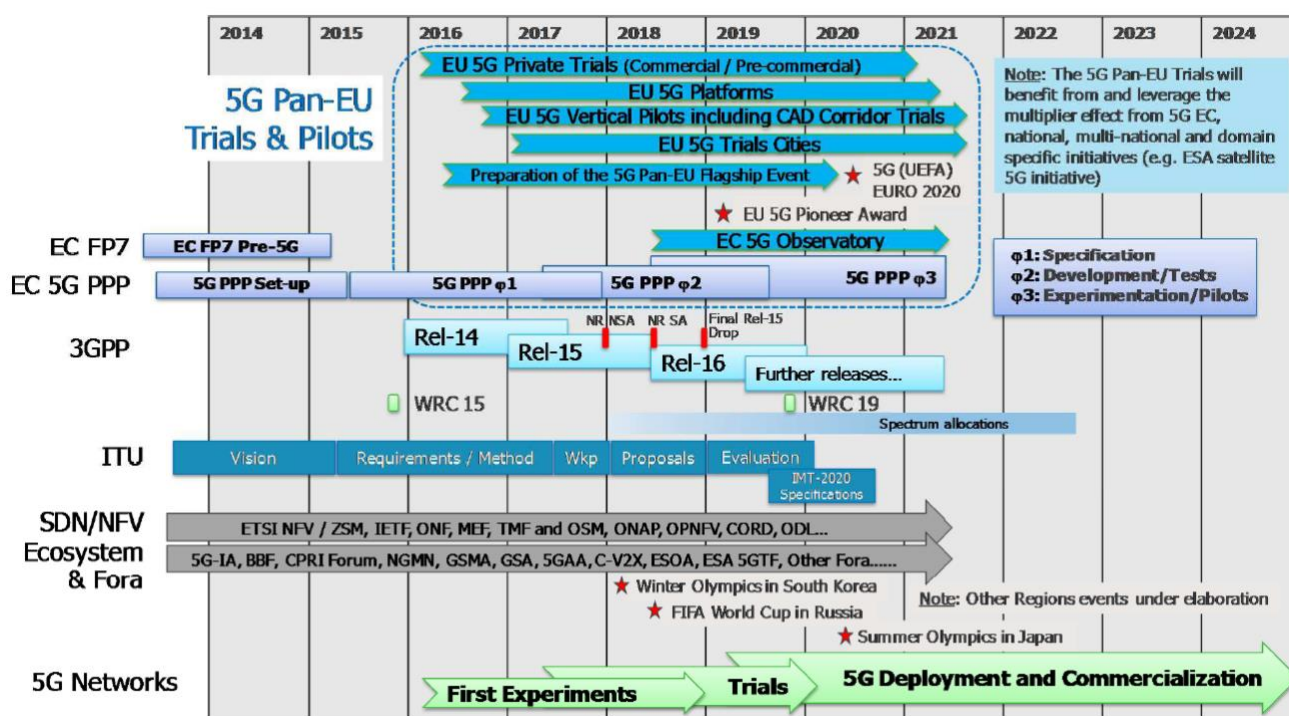


Figure 23 - 5G Pan-EU Trials Roadmap – Time Plan [69].

For 5G!Drones, the overall project architecture is directly impacted by 5G ICT-17 projects, because the 5G!Drones trials are meant to be conducted in part in ICT-17 Facilities (5GEVE and 5GENESIS, as presented in section 5 and detailed in deliverable D1.2).

Moreover, In the context of 5GENESIS, the project technical board has initiated an activity to propose a common experimentation methodology for all ICT-19 projects. Currently, two relevant ICT-17 projects, 5GENESIS and 5G-VINNI, have used the Open-Source OpenTAP software [70] as a starting point to design and build their trial engines. In this regard, 5G!Drones may adopt this trial toolset as a part of its own approaches, in order to be aligned with the testing methodology of the 5GENESIS and 5G-VINNI projects. The final version of this deliverable, D1.6, will provide an update of this initiative, and if applicable, of the steps taken by the 5G!Drones project to support the initiative.

3.3.2. Further enhancements with next 3GPP Releases

Most of Section 3 primarily focuses on the available and short-term 5G activity in the span of R15 and R16, with the notable exception of subsection 3.2, for which R17 already contains several important study items that plan to extend the existing work on UAS/UTM integration in 5G networks. In this context, the objective of this subsection is to provide an early outline of the next 5G normative steps which are materialised, in the 3GPP timeline, as R17 and beyond.

On 14th December, 2019 3GPP released Overall RAN timeline (in Figure 24) which describes next actions related R16, R17 and preparations for R18 [71].

Overall RAN timeline

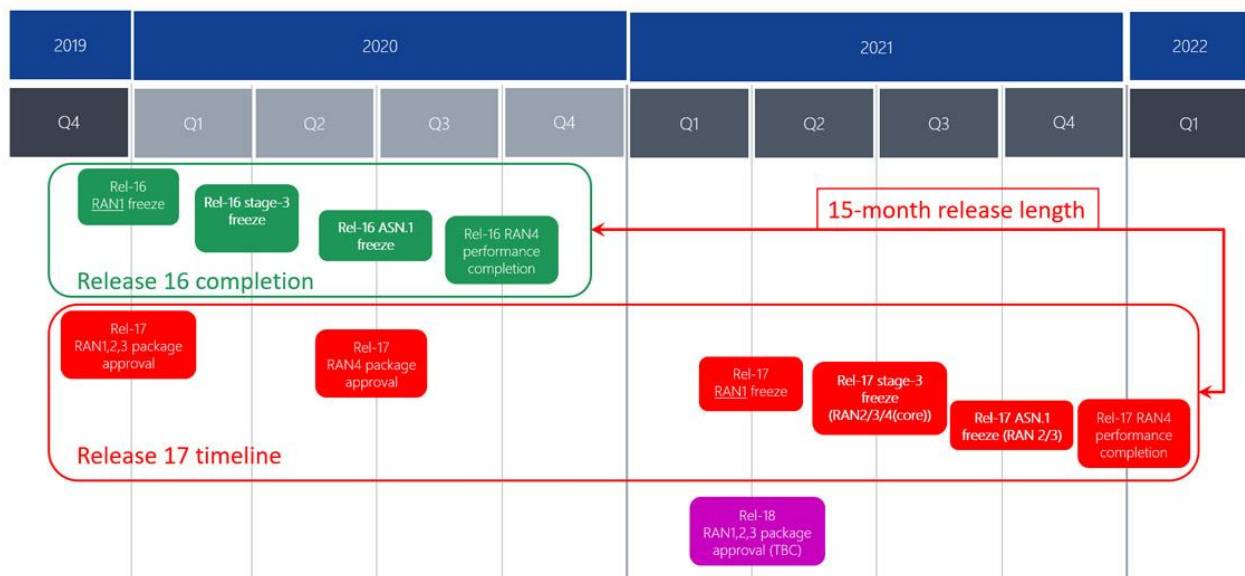


Figure 24 - Overall RAN timeline. 5G in Release 17 – strong radio evolution [71].

Release 17

Release 17 is planned for delivery in September 2021, with its stage-3 freeze, as can be seen in Figure 24. Moreover, among the various 5G system enhancements which are scheduled within the R17 timeline [89], some prioritised areas are particularly relevant for 5G!Drones. These topics mainly relate to UAV and UTM integration into 3GPP systems:

- Aerial UE-specific reporting, such as height, location and flight path reporting. On that note, the prioritised work “NR positioning enhancements” is relevant to the support of additional location mechanisms for aerial UE positioning;
- Remote identification, including UAV-UAV, UAV-ground identification and tracking;
- UAV connectivity requirements and enhancements;
- UAV restrictions.

The already identified work has been described in more details in subsection 3.2. In addition, other areas are relevant to the future evolution of the 5G!Drones architecture:

- Network slicing phase 2 (in relation with subsection 3.1.3);
- Edge computing in 5GC (in relation with subsection 3.1.4);
- NR MIMO and NR sidelink enhancements (in relation with subsection 3.1.5);
- 52.6 - 71 GHz with existing waveform and dynamic spectrum sharing (DSS) enhancements (in relation with subsection 3.1.6);
- Industrial IoT / URLLC enhancements, NB-IoT and LTE-MTC enhancements (in relation with subsection 3.1.7).

Furthermore, the area of NTN is not directly related with the 5G!Drones architecture, since it primarily covers satellites, HAPs and UAVs flying above 8 km. Yet, as previously mentioned in subsection 3.2, the work conducted at 3GPP, notably in the context of R17, may shed light on specific mechanisms. That is notably the case for the following topics, which were prioritised with R17:

- IoT over Non-Terrestrial Networks (NTN);
- NR over Non-Terrestrial Networks (NTN).

Release 18

At the time of finalising this deliverable, the information and timetable for R18 is still scarce. Discussions about R18 stage-1 initial inputs started by end-2019, notably in the context of the SA1 3GPP group. Although no official decision was already made on the R18 timeline, it can be expected that R18 will have an 18-month release length, with stage-1, stage-2 and stage-3 freeze between early 2021 and end-2022. The next version of this deliverable, D1.6, which is due at month 18 of the 5G!Drones lifecycle, will detail this timeline and provide the areas of interest for 5G!Drones, where applicable.

4. OVERALL ARCHITECTURE DESIGN

The objective of this section is to provide the overall architecture design of 5G!Drones. The approach is actually twofold. First, this architecture is intended to support the selected use cases, as summarised in subsection 2.4, over a federated, multi-domain 5G infrastructure. Then, the identified architecture design shall also effectively manage the execution of large-scale UAV trials. The rest of this section is therefore dedicated to the identification and design, at a high level, of the architecture components required to provide the necessary infrastructure support to the 5G!Drones system, in both aforementioned cases.

4.1. High-level Overview

An overview of the 5G!Drones architecture is illustrated by Figure 25. According to this representation, the architecture is broken down into boxes, each embodying a 5G!Drones architecture component. In addition, the potential interactions between the components are assessed, together with their directionality, represented by the arrows. It is worth noting that, at this point in the 5G!Drones project lifetime, these arrows must be considered rather as an early identification of the way components communicate, which is intended to support the subsequent work in the 5G!Drones work packages WP2 and WP3, thereby leading to the definition of the project interfaces. In that regard, the current arrow representation may be assimilated as a type of Integration Reference Point (IRP), as defined by 3GPP [77].

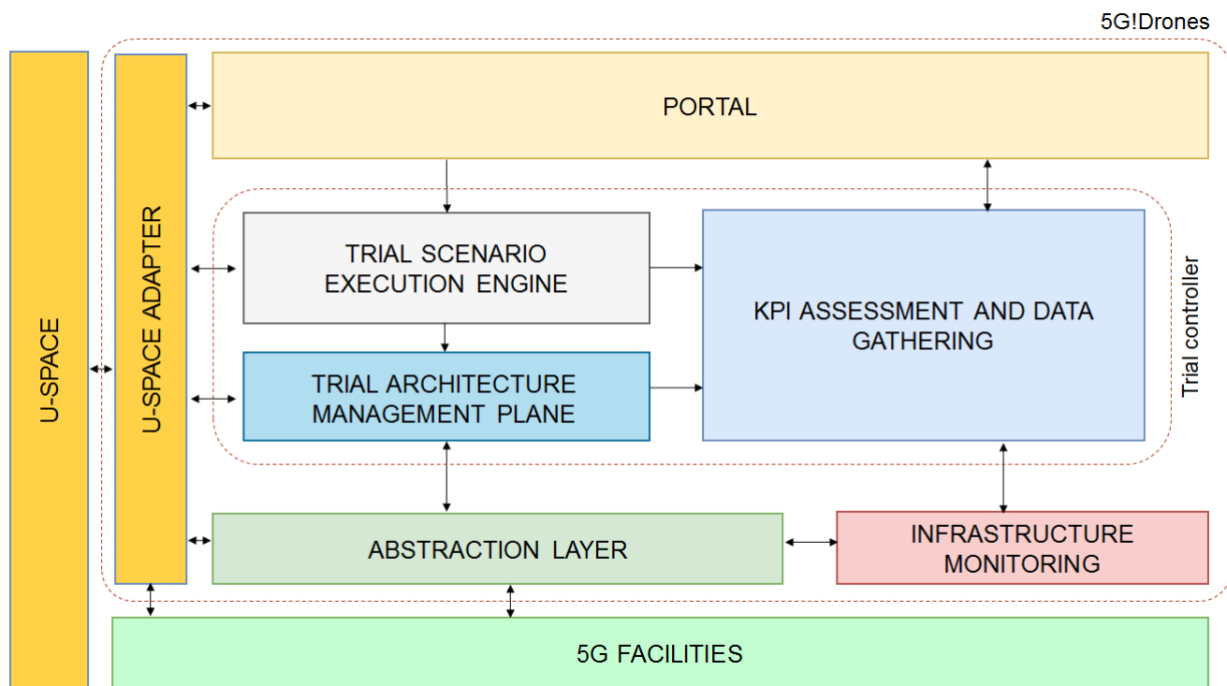


Figure 25 - High-level overview of the 5G!Drones architecture

4.2. Architectural Breakdown into Components

Furthermore, the high-level architecture shown in Figure 24 can be broken down into several entities, each representing a component or encompassing several components: the Portal, the Trial Controller, the Abstraction Layer, the 5G Facility Infrastructure Monitoring, the U-Space entity and the U-Space Adapter.

4.2.1. Portal

The Web Portal is the component in charge of the interaction with the UAV Verticals. The Web Portal allows a UAV Vertical to describe the desired trial scenarios and to indicate the (5G and UAV) KPIs to measure for the considered scenario to trial. In the execution of the trial scenario, the Web Portal is also in charge to display the results obtained from the trial.

The UAV Verticals can request more resources from the 5G Facilities (i.e. in terms of CPU and RAM) or adapted configuration of the slices, for instance. These requests will be passed via the Portal.

4.2.2. Trial Controller

The 5G!Drones Trial Controller represents the entity of the 5G!Drones trial architecture designed to support the execution of large-scale UAV trials. It encompasses several components: those are the Trial Scenario Execution Engine, the Trial Architecture Management Plane and the KPI Assessment and Data Gathering:

- **The Trial Scenario Execution Engine** takes as input from the Web Portal the scenario defined by the UAV Vertical. It is in charge of instantiating virtual and physical functions according to this trial scenario. In addition, it implements the lifecycle management of the trial.
- **The Trial Architecture Management Plane** component is in charge of enforcing the trial scenario elements forwarded by the Trial Scenario Execution Engine. To this purpose, it interacts with the 5G Facility resources via a dedicated IRP. Furthermore, this component is in charge of:
 - Instantiating the network slices needed to run the trial;
 - Onboarding the required UAV service components, under the form of VNFs. Examples of such components are UTM functions and other UAV-related applications which need to be executed on top of the 5G Facility resources to enforce the requested trial scenario. It is worth noting that, the analyses carried out in section 5 take into account both the specific requirements of the target scenarios to be trialled and the features of the four 5G Facilities where the 5G!Drones Trial Controller shall be deployed. On this basis, a set of UAV service components can be found in section 6;
 - Configuring the embedded slice manager elements to gather service-level KPIs;
 - Configuring the monitoring information regarding the 5G KPIs made available by the 5G Facility and the virtualised resources used by the network slices;
 - Returning to the Trial Scenario Execution Engine, once the aforementioned steps are completed, the interfaces needed to connect to the slice manager and to retrieve monitoring information from the 5G Facility.
- **The KPI Assessment and Data Gathering** component is in charge to monitor the KPIs defined by the trial scenario, and requested by the Trial Scenario Execution Engine. To that end, the KPI Assessment and Data Gathering component receives from the Trial Scenario Execution Engine the relevant interface information needed to connect to the slice manager and to retrieve monitoring information from the 5G Facility Testbed Infrastructure Monitoring. To enable harmonised analysis on potential inhomogeneous data from different components in the large system of systems that will be realised in WP4, it is envisioned to provide a simple catalogue / categorisation / mapping of KPIs in the KPI Assessment and Data Gathering component, to e.g. know which measurements provide latency data. For end-to-end monitoring, means to relate measurements to each other should be considered in all components of the system (e.g. by having

a unique identifier on a request, which is made available in every measurement, no matter which component reports). Leveraging existing work, currently available products will be analysed and compared focusing on their suitability for the tasks at hand in 5G!Drones (based on use cases and requirements defined in D1.2).

4.2.3. Abstraction Layer

5G!Drones will run several use cases over different Facilities. This includes two ICT-17 Facilities (the Greece trial site of 5Genesis and the French trial site of 5G EVE) in addition to two complementary trial sites (5GTN of University of Oulu and X-Network of Aalto University). This diversity results in heterogeneity in terms of the supported capabilities and offered interfaces. In this regard, **the Abstraction Layer** is a key component which abstracts the underlying heterogeneity, thereby exposing unified interfaces to the upper layer, as Figure 26 illustrates. Therefore, the Abstraction Layer will allow the Trial Controller to be agnostic of the Facility specificity.

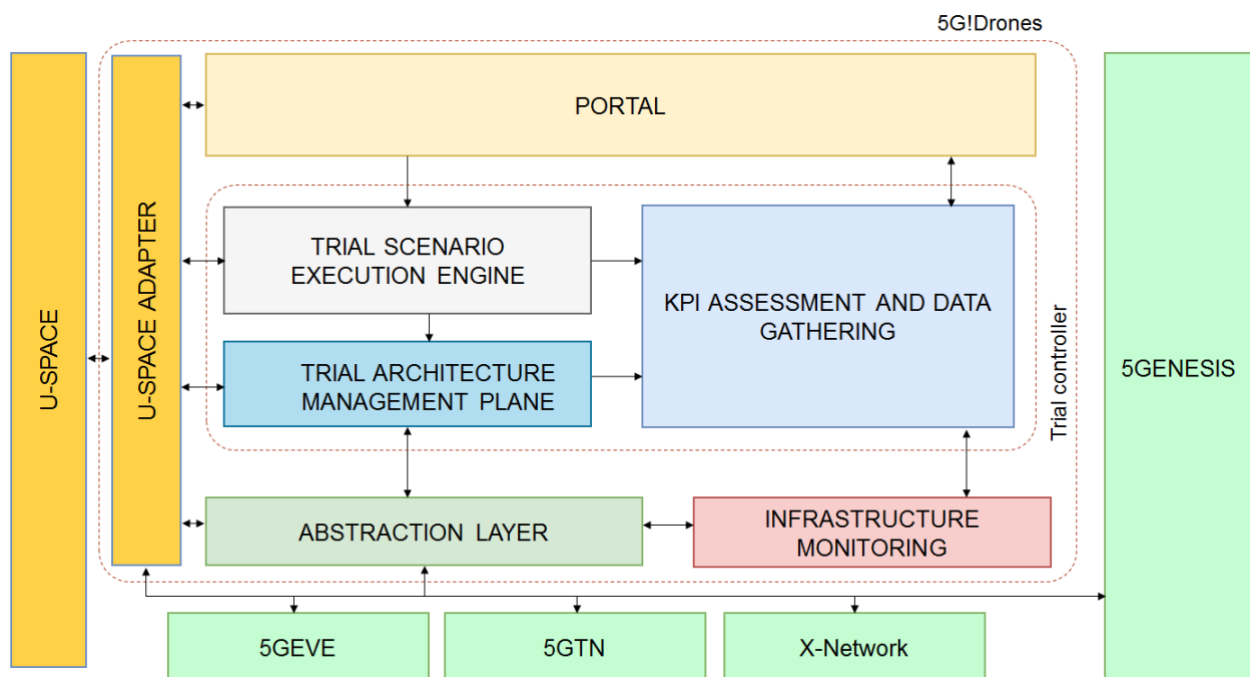


Figure 26 - The Abstraction Layer handles the 5G Facilities diversity (5GEVE, 5GTN, X-Network and 5GENESIS)

4.2.4. 5G Facility Infrastructure Monitoring

The 5G Facility Infrastructure Monitoring is in charge of enforcing the monitoring of the 5G Facilities. This component receives from the KPI Assessment and Data Gathering component the relevant information to monitor the 5G KPIs defined by the considered use case.

4.2.5. U-Space

The U-Space entity is a set of services and specific procedures designed to support the safe, efficient and secure access to airspace for large numbers of drones, as previously described in subsection 2.3. In practice, it will consist of a suite of tools, including a UTM, designed and developed outside 5G!Drones. This later component is likely to be deployed along with the 5G!Drones trials.

4.2.6. U-Space Adapter

The **U-space Adapter** is a component which allows the integration of the 5G!Drones architecture with UTM and more generally the U-Space entity. To allow this integration, several IRPs are identified, thereby defining interaction points with the U-Space, Portal, Trial Scenario Execution Engine, Trial Architecture Management Plane and the 5G!Drones UAV Enablers:

- **IRP with the Portal:** Drone operators and service providers are likely to expose U-Space APIs and potentially UIs in the portal in order to reuse existing work, to the extent possible. Nevertheless, some adaptation work will nevertheless be required on several existing and possibly new mission planners, and that should subsequently foster the open market;
- **IRP with the Trial Scenario Execution Engine:** One of the prerogatives of the Trial Scenario Execution Engine is the validation that the trial can be performed. One precondition is the approval from traffic management, either proxied to an operational UTM, or handled by the UTM deployed for the 5G!Drones trials;
- **IRP with the Trial Architecture Management Plane:** U-Space services are expected to require information from the management plane, e.g. to ensure safety for high risk areas. This includes receiving information by the 5G network for capabilities of the network(s) that are not available, as well as issuing requests to setup high priority slices for emergency situations, and enforcing immediate orders to all airspace users;
- **IRP with the Abstraction Layer and with the 5G Facilities:** These IRPs allow retrieving up-to-date information. This IRP can be considered as belonging to the Data Plane. A use of this IRP is for instance the transmission of UAV telemetry to the U-Space.

5. GAP ANALYSIS

This section conducts a gap analysis, in the context of the X-Network, 5GEVE, 5GTN and 5Genesis Facilities respectively. The objective is to recognise the UAV service requirements that can be met by the existing 5G architectures, and identify the specific components that must be further developed within the context of each Facility.

5.1. Per Site Gap Analysis

5.1.1. X-Network

As presented in D1.2, the current setup of Aalto University's X-Network includes different component at the infrastructure layer level (eNB/gNB, 4G/5G core network, MEC and datacenter, SDN-based backhaul). Some limitations have been identified especially at the management layer.

Aalto University is building an orchestration solution for its Facility considering different levels (cloud, RAN and transport). MANO is a key element for the NFV architecture. It allows manage network resources for cloud-based applications and life cycle management of virtual network functions and network services. OSM (Open Source MANO) or Open Baton are some tools that can be considered for building the orchestration solution.

The current gNB is deployed in NSA mode; it uses another eNB as anchor node. The eNB communicates with the CN for signalling, then after the UE attaches it uses the gNB for user plane. The upgrade of the gNB to SA mode is planned for 2020.

The gNB can be configured, in the current setup, only manually and on the site. Although this can be used to accommodate the different use cases by configuring the RAN as per the target scenario, remote configuration of the RAN would enable advanced services that can be requested on demand. Aalto University is in the process of acquiring a RAN manager software which can be used for remote configuration and monitoring. This tool shall be integrated in the orchestration solution to enable end-to-end network slicing.

The following table summarises different available features and the potential evolution of the trial site of Aalto University.

Table 3: AALTO Evolution Analysis

	Availability at Aalto's trial site	Evolution	Alternative
Trial Descriptor	Non-available	To be developed by 5G!Drones (WP2)	X
Trial Engine	Non-available	To be developed by 5G!Drones (WP2)	X
Facility Resources Access API	Non-available	Aalto University is building and orchestration solution for its Facility. The solution shall provide the interfaces to the upper layers.	

	Availability at Aalto's trial site	Evolution	Alternative
UTM connection	Non-available	To be developed in WP2 or added by UAV partner in 5G!Drones	
UAV Deployment	The trials can be performed in the campus of the university.		
UAV Devices	Two models of drones are available. The drones are equipped with different IoT devices.		
Orchestration and Management	Non-available	Aalto University is building and orchestration solution for its Facility (WP3 work can be considered).	X
Virtualisation Infrastructure Manager (VIM)	OpenStack services	X	X
Multi-access Edge Computing (MEC) - ETSI	<ul style="list-style-type: none"> Nokia's MEC platform is deployed Another MEC platform is available which is open MEC platform. 	WP3 work can be considered for MEC service relocation	
5G Core components	A 4G/5G core is available where different 3GPP network functions are available (AMF, SMF, NSSF, UPF, NRF).	X	X
Radio Access Network	<ul style="list-style-type: none"> Several eNBs (FDD 2.6 GHz) One NB-IoT eNB (FDD 700 MHz) Two gNBs <p>The RAN can be (re)configured only manually and on the site.</p>	<p>The gNB is operating in NSA mode. The upgrade to SA mode is planned for 2020.</p> <p>RAN manager software to be acquired.</p>	X
Frequencies	Aalto University has been granted from TRAFICOM (Finnish Transport and Regulation Agency) the license to 3.5 GHz for 5G test networks.	X	X

	Availability at Aalto's trial site	Evolution	Alternative
Network Slicing	The core network is virtualised and is implemented to enable slicing in the CN. Slicing in the transport is based on SDN solution (backhaul orchestrator).	Aalto University is building an orchestration solution to enable end-to-end network slicing.	X
Mobility Management	Non-available	No further deployment	X
5G Devices	Non-available	To be acquired	X

5.1.2. 5GEVE

The 5GEVE Sophia-Antipolis site is built on top of OAI gNB and eNB. It offers NSA 5G connection, using an OAI EPC. The gNB can operate on both sub-6GHz and Millimetre waves. The platform supports Network Slicing using a home-made Slice Orchestration, which controls a home-made NFVO orchestrator on top of Kubernetes. The RAN is configurable and controlled via the FlexRAN framework. The platform is providing a MEC ETSI Edge computing system. The limitation of the platform concerns mainly the non-availability of the 5G Core elements. However, the platform will include, by the end of 2020, beginning 2021, an OAI 5G CN, enabling SA 5G deployment.

Table 4: 5GEVE EURECOM Site Evolution Analysis

	Availability at 5GEVE EURECOM Site	Evolution	Alternative
Trial Descriptor	Non-available	To be developed by 5G!Drones (WP2)	X
Trial Engine	Non-available	To be developed by 5G!Drones (WP2)	X
Facility Resources Access API	Non-available	To be provided by 5GEVE consortium.	EURECOM will develop the needed API to access its Facility
UTM Connection	Non-available	To be developed in WP2 or added by UAV partner in 5G!Drones	EURECOM will simulate UTM component
UAV Deployment	A corridor of 200 m maximum, No more than 15 m of height	Constraints imposed by the geographical location of EURECOM site, and location regulation.	X

	Availability at 5GEVE EURECOM Site	Evolution	Alternative
UAV Devices	Non-available	X	EURECOM has one flying drones for the tests
Orchestration and Management	<p>A home-made orchestrator that handles Life Cycle Management (LCM) of VNF/CNF or MEC applications,</p> <p>Support:</p> <ul style="list-style-type: none"> • Network Service Descriptor (NSD), • Application Descriptor (AppD), • On-boarding and instantiation of AppD on top of cloud infrastructure, including Edge, • Monitoring of the usage of virtualisation resources. 	To be improved in WP3 to handle UAV applications described by an AppD or VNFD.	X
Virtualisation Infrastructure Manager (VIM)	Container-based virtualisation (LXC/LXD and Kubernetes)	X	X
Multi-access Edge Computing (MEC) - ETSI	<p>MEC Edge Platform (MEP) compliant with ETSI model.</p> <p>Support:</p> <ul style="list-style-type: none"> • mp1 interface: RNIS, Location, DNS, traffic redirection • mp2 interface: connecting to OpenAirInterface (SGW-U/SGW-C Split), and LORA IOT network 	To be improved in WP3 to support Slicing	
5G Core Components	Non-available	Expected to be deployed by 5GEVE, end of 2020	X
Radio Access Network	<p>OpenAirInterface:</p> <ul style="list-style-type: none"> • 4G and 5G connectivity (Non-Standalone) 	5G connectivity will be available by the first semester of 2020.	

	Availability at 5GEVE EURECOM Site	Evolution	Alternative
	<ul style="list-style-type: none"> NB-IOT Functional split: CU, DU and RRU FlexRAN to enable RAN programmability (only for 4G) LORA/LORAWAN: <ul style="list-style-type: none"> LoraServer and Gateways. 		
Frequencies	3600-3680 MHz TDD (61 dBm EIRP, NR band 78) => 5G eMBB/URLLC, 2580-2610 MHz TDD (61 dBm EIRP, LTE band 38) => 4G, 708 – 718/763 – 773 (57 dBm EIRP, NR band 28) => 5G (Orange license), 698 – 703/753 – 758 MHz FDD (LTE band 68) => IoT / ProSe, 733 – 736/788 – 791 MHz FDD (LTE band 28) => 5G-EN-DC/IoT / ProSe,	No further extensions	X
Network Slicing	Core Network Slicing using S1flex, RAN slicing using FlexRAN, Slice isolation, Slice Orchestrator: <ul style="list-style-type: none"> Slice template Specify the amount of RAN resources to dedicated to a Slice Interact with FlexRAN and EURECOM-orchestrator 	To be developed by 5G!Drones (WP3): <ul style="list-style-type: none"> Interface to monitor the slices to report trial results Extend the Slice template to support UAV, as two slices (URLLC, and eMBB or mMTC) need to be enclosed in the same template. Edge Slicing URLLC improvement (mainly at the eNB scheduler level) In-Slice management 	X

	Availability at 5GEVE EURECOM Site	Evolution	Alternative
Mobility Management	Non-available (only one gNB will be deployed at EURECOM Facility)	No further deployment	X
5G Devices	Non-available	X	EURECOM can provide a 5G NSA phone for the tests

5.1.3. 5GTN

5.1.3.1. Limitations

RAN

No part of 5GTN Radio is implemented in the cloud (Cloud-RAN) at the moment. Currently, 5GTN Radio contains frequency bands 700 MHz, 2.6 GHz and 3.5 GHz, depending on the requirements. Furthermore, most implementation are currently done with the 4G eNBs. The 5G NR at 5GTN is yet to be fully optimised for maximum usage.

Core Network

- 5GTN currently supports LTE EPC thus limiting its core functionalities regarding slicing capability. Particularly regarding the need for the Network Slice Selection Function (NSSF).
- 5GTN supports NSA deployment Option 3A, while several use-case scenarios might need Option 2 Deployment for a full implementation and support.
- 5GTN uses only OSM as the orchestration solution, thus every limitation with the current OSM orchestration affects 5GTN. The current orchestration tool supports only NSSMF and NSMF (i.e. Network service (NS) creation for VNFs and Network slice instance creation from the NS).
- Network slice service definition is not implemented in the current OSM. This is to say, even though in the slice service types such as eMBB, URLLC and mMTC slices are defined in the slice template, the real implementation is not done during the slice creation.
- The current OSM does not support the Communication Service Management Function (CSMF) which determines how a network slice will be transmitted and distributed to end users.
- The current OSM does support slice creation across multiple domains, but it does not support multiple NSIs (i.e. slice services) which might be relevant to one UAV; A feature that is very vital to implement slicing in many use cases. Since many use case scenarios require multiple slice services (e.g. eMBB and URLLC for UTM 2, safety 1, etc.).

5.1.3.2. Enhancements Required

- 5GTN is expecting to get 5G NR for a full deployment of the network.
- New 5G small cells are expected to be deployed to 5GTN.
- 5GTN is envisioned to have the 5G Core by 2020, thus removing the NSA deployment limitations. The 5G Core will contain all 5G functionalities and there is full implementation of the 5G NR (i.e. Option 2 deployment).

- OSM future release should support the implementation of multiple slice services.
- We are currently working on an architecture with techniques to derive a solution to how multiple slices can be distributed and shared.

Table 5: 5GTN Oulu Evolution Analysis

	Availability at 5GTN Oulu Site	Evolution	Alternative
Trial Descriptor	Non-available	To be developed by 5G!Drones (WP2)	X
Trial Engine	Non-available	To be developed by 5G!Drones (WP2)	X
Facility Resources Access API	Available but proprietary to equipment supplier	At the moment, 5GTN's access to interface is propriety to the equipment suppliers.	work is currently being done to allow access from third party Facilities and public partners
UTM Connection	Non-available	To be developed in WP2 or added by UAV partner in 5G!Drones	UTM connection will be performed by simulation in 5GTN Facility
UAV Deployment	Most trial deployments will happen in a corridor within the university. For indoor test Facilities, UO provides a cable drone; i.e. a drone that is not actually flying, but moving in 3D space using cables, similarly to so called Spider Cameras use in for example sport events. This device can be equipped with same sensors as flying drone and the interface for moving it in the test space is the same as for flying drones. The advantage of this type of drone replacements is that it can make test series automatically, periodically, and with high precision without human operator. The infrastructure trials will happen in outdoor testing area.		X
UAV Devices	UO provides 1xDJI Matrice 210 RTK drone, payload up to 1.4 kg https://www.dji.com/ee/matrice-200-series/info For UAVs automated flights, UO provide a ROS interface for the drone and online data provided by the sensors on board.	X	EURECOM has one flying drone for the tests

	Availability at 5GTN Oulu Site	Evolution	Alternative
Orchestration and Management	<p>OSM orchestration is used in 5GTN VNF/PNF management. OSM orchestration supports the following:</p> <ul style="list-style-type: none"> Virtual Network Function Descriptor (NSD), Network Service Descriptor (NSD), Network slice Descriptor (NST) Monitoring and performance of the usage of virtualisation resources. Juju charm is used to implement specific actions or services in VNFs Day1, Day2 and Day3 configuration can be established on VNFs 	<p>OSM orchestrator is expected to be used for MEC application and MEC orchestration</p> <ul style="list-style-type: none"> Application Descriptor (AppD), On-boarding and instantiation of AppD on top of cloud infrastructure, including Edge 	
Virtualisation Infrastructure Manager (VIM)	OpenStack service is used	X	X
Multi-access Edge Computing (MEC) - ETSI	Virtualised MEC server supported by Nokia's MEC platform is deployed	To be improved in WP3 to support Slicing Extension of MEC to support slicing	
5G Core Components	<p>4G core currently available</p> <p>Virtualised open source EPCs are used such as OpenEPC and NextEPC</p>	Expected to be deployed by 5G core in future	X
Radio Access Network	5GTN currently deploy one macro cell and six small cells (eNB). The macro cells are installed outdoors, while the small cells are indoor installed. The eNBs operate in an LTE band 7 (2600 MHz) and are based on the Frequency Division Duplexing (FDD) scheme.	The near future plans are to deploy 3.5 GHz equipment and bring first proof of concept 5G radio equipment to the network.	
Frequencies	<p>LTE 700 MHz</p> <p>LTE 2600 MHz</p> <p>5G 3500 MHz</p>	No further extensions	X
Network Slicing	<ul style="list-style-type: none"> Core Network Slicing is achieved using OSM orchestrator. 	To be developed by 5G!Drones (WP3):	X

	Availability at 5GTN Oulu Site	Evolution	Alternative
	<ul style="list-style-type: none"> Current slicing solution is implemented based on NST instantiated in the OSM. Different slice services can be created. Fully Virtualised NextEPC is used to implement slicing based on OSM where separated Network component are sliced to form a single network Performance analysis is done based on different shared and non-shared instantiated slices across different domain <p>Juju charm is used to implement specific actions or services in VNFs to support instantiated slices.</p> <p>No RAN slicing at the moment FlexRAN, Slice isolation.</p>	<ul style="list-style-type: none"> Interface to monitor the slices to report trial results; Transmission of instantiated NSI as communication service to different UAVs; distribution of multiple NSIs to a single UAV; Achieving slicing across MEC; Actual implementation of defined network slice service based on specific configuration, changes, placement of VNFs etc. 	
Mobility Management	Non-available (only one gNB is used)	No further deployment	X
5G Devices	Huawei 5G mobile and One plus 5G phone currently used for experimentation		

5.1.4. 5GENESIS

5.1.4.1. Limitations

Slice Manager

- Currently, the Slice Manager does not support end-to-end slicing, since RAN is not included in the components that are managed by the slice manager.
- Some basic networking setup is performed during the slice configuration, while further elaboration may be needed in the network creation for more complex scenario.

Core Network

- 5GENESIS, although it has available a fully deployed EPC, does not currently support NSA 5G (Option 3A).
- 5GENESIS uses only OSM as the orchestration solution, thus every limitation with the current OpenStack orchestration affects 5GENESIS.
- The current OSM does not support a tight integration with the management functions of the core network, which determines how a network slice will be transmitted and distributed to end users.

5.1.4.2. Enhancements Required

- New 5G small cells are expected to be deployed to 5GENESIS.
- 5GENESIS is envisioned to have 5G NSA deployment by 2020, thus removing both SA and NSA deployments.

Table 6 - 5GENESIS Evolution Analysis

	Availability at 5GENESIS	Evolution	Alternative
Trial Descriptor	Available. 5GENESIS has defined each own trial and experiment descriptor in order the experimenter to describe the experiment and then to be imported the descriptor file at the 5GENESIS experimentation portal.	To be expanded by 5GENESIS consortium in order to support Drones specific experiments, if the current version does not allow the execution of the experiments and trials.	None
Trial Engine	5GENESIS coordination layer includes the trial engine for the automation and the execution of the experiment, which is based on OpenTAP. The 5GENESIS trial engine will be used for the execution of the 5G!Drones experiments in Athens site.	It will be tested in Drones trials and experiments in order to identify the special needs of these tests and appropriate modifications and enhancements will take place in order to better support the specific vertical.	None
Facility Resources Access API	Available. 5GENESIS has developed an Open-API in order to support the integration and extension of the platform with other systems and/or components.	To be expanded by 5GENESIS consortium if additional calls that currently are not supported are needed for the execution of the Drones trials.	None
UTM Connection	Athens UC4-SC1 will not utilise the UTM component	None	None

	Availability at 5GENESIS	Evolution	Alternative
UAV Deployment	Within the Egaleo Stadium. No more than 50 m of height. Constraints imposed by the geographical location of Egaleo Stadium, and location regulations.	None	In case of restrictions, alternative locations could be also considered, such as the NCSR campus.
UAV Devices	Will be provided by HEPTA and CAFA TECH (2 regular drones + 1 tethered)	Additional partners may also contribute with more drones or drones of different type.	None
Orchestration and Management	OSM is installed at 5GENESIS Athens platforms that handles Life Cycle Management (LCM) of VNF or MEC applications.	None	None
Virtualisation Infrastructure Manager (VIM)	Openstack is already installed in 5GENESIS Athens site.		
Multi-access Edge Computing (MEC) - ETSI	In 5GENESIS Athens site, currently operates an edge computing, based on Openstack.	The currently available edge computing environment will be gradually updated to MEC, upon appropriate upgrade of the Mobile Core Network of the platform.	None
5G Core components	Amarisoft Core (NR R15 compliant)	None	NSA 5G deployment with EPC as core network.

	Availability at 5GENESIS	Evolution	Alternative
Radio Access Network	<p>Option 1: OpenAirInterface (OAI)</p> <p>Available Components:</p> <ul style="list-style-type: none"> 5G (OAI NR UE and OAI gNB): <ul style="list-style-type: none"> i9 laptops USRPs N310 Thunderbolt-to-Ethernet adapters (can support up to 2x2 MIMO configuration, due to latency) 4G: <ul style="list-style-type: none"> OAI eNB server OAI vEPC Interoperability of OAI eNB with Athonet vEPC COTS UEs (dongles, mobile phones) FlexRAN for RAN programmability available (NCSRD member of Mosaic5G, but Mosaic5G not part of 5Genesis) <p>Available OAI deployments:</p> <ul style="list-style-type: none"> no-S1 (non 3GPP compliant, OAI gNB <-> OAI NR UE): initial deployment, downlink only, under development NSA: To be deployed when ECM releases the relevant version <p>Option 2: Amarisoft</p> <p>Available Components</p> <ul style="list-style-type: none"> 4G: <ul style="list-style-type: none"> Amarisoft EPC & eNB PCIe SDR B210 USRP N210 USRP 5G 	5G connectivity will be available by the first semester of 2020.	

	Availability at 5GENESIS	Evolution	Alternative
	<ul style="list-style-type: none"> ○ Amarisoft Core (NR R15 compliant) ○ Amarisoft NR solution ○ PCIe SDR <p>Available Deployments</p> <p>NSA:</p> <ul style="list-style-type: none"> • LTE FDD cell 10MHz bandwidth & NR TDD cell bandwidth 50 MHz 		
Frequencies	<p>3650 MHz TDD, 100 MHz bandwidth</p> <p>3489 MHz TDD, 50 MHz bandwidth</p> <p>28 GHz TDD, 50MHz bandwidth</p>		
Network Slicing	<p>“Katana” Slice Manager responsible for the Lifecycle management of End-to-End Slices is fully operational at 5GENESIS Athens site.</p> <p>Katana interacts with South Bound components that are responsible for different domains, namely VIM, NFVO, WIM and EMS</p> <p>Slice isolation:</p> <ul style="list-style-type: none"> -NFVI: Create a separate Tenant for each Slice - Transport Network: Isolation achieved with the use of VLANS and SDN rules <p>Slice is described in the Generic network Slice Template (GST)</p>		X
Mobility Management	5GENESIS supports hand-over only for 4G network. In 5G Networks hand-over is not supported.		
5G Devices	<ul style="list-style-type: none"> - OAI Interface based UE using Ettus N300/310 SDR cards. - Samsung Galaxy A90 5G 	Additional 5G COTS UEs to be available by Q4 2020	

5.2. Harmonised Analysis, Main Takeaways

All testbeds (5GEVE, UO 5GTN, Aalto X-Network) but 5GENESIS, start from a similar standpoint regarding 5G!Drones project trials. Indeed, the first three testbeds lack components such as a Trial Descriptor, a Trial Engine and APIs. These aspects, notably to establish UTM connections, will be particularly addressed by WP2 during the 5G!Drones project lifecycle.

In contrast, the 5GENESIS Athens platform brings into the 5G!Drones project a functional experimentation Facility, tools and components that are developed within 5GENESIS. The 5GENESIS Athens platform is already equipped with the 5GENESIS Coordination Layer and its experiment lifecycle manager component, as well as the experimenter portal, and so on. 5GENESIS Facility in the framework of the project will integrate and/or deploy the additional and drone specific components that are required for the execution of the drones trials, for example the integration of the UAS, the expansion of the 5GENESIS portal with additional fields, and so on. By involving a fully functional H2020 ICT-17 Facility for the 5G!Drones trials, 5GENESIS Facility shall validate, as a complementary activity to the tests involving the UAV components, the 5G!Drones experimentation process and support the comparison and benchmarking among diverse testbed environments.

Furthermore, some testbeds (5GENESIS, 5GTN and X-Network) have already been used to conduct UAV flights. But 5G technology has not been used in these flights. Additionally, the needs to develop mechanisms to connect to UTM and achieve UAV deployments in accordance to project trial plans, which are detailed in deliverable D1.1 are paramount across all Facilities.

Regarding the functions such as Orchestration and Management, Virtualisation Infrastructure Manager (VIM), MEC and 5G Core components, for the testbeds that are not supporting them yet, there are established plans to get them to work by end-2020 through the developments performed in WP3, and via testbeds as needed.

It is worth highlighting that all four testbeds offer 5G NR solutions and relevant frequencies. Besides, Network slicing is already supported in 5GENESIS, while this feature and Mobility Management will be deployed on the other ICT-17 Facilities mainly by 2021 through developments conducted in WP3 and dedicated testbeds. Moreover, Aalto X-Network and Oulu 5GTN networks have successfully used Huawei and One Plus 5G smartphones. Similarly, 5GENESIS has successfully used Samsung COTS 5G smartphones (5G Galaxy A90), covering by this way a wide range of available 5G COTS smartphones.

The main takeaway is that in order to bring 5G Facilities into compliance with the trial requirements as described in deliverable D1.1, and in order to successfully conduct the 5G!Drones trials in 2021, three essential base elements need to be considered:

1. The specific developments done by the test facility owners;
2. The developments done in the context of 5G!Drones, in particular in WP2 and WP3, as well as potential mutualisation of a subset of the developments (e.g. regarding the Trial Descriptor);
3. A close cooperation between trial leaders and facility owners and early stage tests to develop solutions in an agile way, i.e. pre-trials and iterations from pre-trial results.

6. 5G!DRONES ENABLERS

This section leverages on the aforementioned gap analysis to highlight a set of 5G System Enablers. More precisely, the section provides a high-level architectural description of the 5G system components as well as an early outline of the UAV Enablers which shall be designed in the 5G!Drones project. With this last part, the objective is to support, on the architectural level, the design and development of these components within the project Work Packages WP2 and WP3, as well as their trial in Work Package WP4. Lastly, this section delineates the intended project cybersecurity support, introducing its approach to 5G!Drones security high-level architecture as well as a set of 5G relevant security enablers.

6.1. 5G System Enablers

6.1.1. Slicing for Drone-based Services

Network slicing allows creating multiple isolated networking solutions tailored for specific data traffic categories and supporting programmable data plane. The use of network slicing comes with multiple benefits due to the isolation of specific traffic which can individually be handled in an adapted way. The 3GPP has defined so far four slice types, addressing differentiated service needs that include streaming (eMBB), ultra-reliable, low-delay control (uRLLC), massive IoT traffic (mMTC) and V2X (Vehicle-to-everything) communication. Each of the defined class concerns both Radio Access Network (RAN) data plane properties and 5GC configuration, which has to be adapted to support specific service (slice selection, authentication). Deployment of network slices, according to [73], [74], should be realised with ETSI MANO orchestrator, by using generic templates (blueprints) provisioned by the framework. Each of the blueprints can be instantiated multiple times by a vertical (service operator), thus enabling the creation of parallel service-oriented networks. The same terminal (a drone) can be attached up to eight slices simultaneously.

Network slicing is one of the critical enablers for 5G!Drones. In case of UAV-based services, it is essential to provide transmission links with parameters such as latency or reliability required by UAV flight support. These can include e.g. uRLLC for Command and Control (C2) channel, mMTC for cargo and safety services or eMBB for the high-quality view of 8K or Virtual Reality (VR) cameras mounted on-board of UAVs. The most popular UAV operational scenario requires the establishment of two radio links, one responsible for reliable, low-latency C2 information exchange between the operator and the UAV, and the second one; handling high-speed data stream related to the offered service. In order to meet this requirement, multiple RAN slices for each drone operator should be created. Typically for C2 information exchange, URLLC slice is recommended in order to provide near real-time UAV control to the client. Such an approach is advised even if real-time control is not strictly required due to the high reliability of the transmission of URLLC.

Moreover, low latency gives the processing platform more time to handle control data and therefore to operate more effectively. For service-related data transmission, most cases require high bandwidth. Therefore, using eMBB slice is recommended. The type of the slice, however, is service-dependent and may vary according to specific requirements. In some cases, the service may require combined URLLC and eMBB slices e.g. for drone control with real-time VR camera view of the on-board camera. According to 3GPP, one UE can be currently simultaneously attached to up to 8 slices.

In some use cases (swarms), direct communication between drones is required. Such communication can be used for increasing the reliability of the C2 communications or for keeping the mutual distance between drone members. Such communication does not require slicing of the connections. For intra-swarm communications, the Proximity Services (ProSe) can be used. This concept enables the direct,

low-latency device to device (D2D) communication between the swarm members. However, ProSe technology is currently only standardised for LTE-Advanced Pro [75] and its incorporation into 5G is currently under thorough study [76]. The intra-swarm communications can be also implemented using other networking solutions like WiFi.

6.1.2. MEC Extensions and Architectural Impact of Trial Facilities

As stated earlier, MEC and Network Slicing are two key enablers for 5G!Drones, particularly to empower URLLC services required to control and command remotely drones. So far MEC and Network Slicing are evolving in parallel, and are being defined by two different standardisation groups, ETSI and 3GPP, which limits their integration and their benefits as complementary solutions. Recently, a MEC ETSI group has been constituted to evaluate to what extent MEC can support NS. This group has issued a document [45] describing only some use-cases and requirements to support NS at the MEC level and many points are kept open. First, a new MEC architecture should be devised and aligned with (i) the current 3GPP specifications to fit with the 5G architecture at both the RAN and CN, and (ii) the integration of MEC in NFV [46], while considering the new Network Slicing management framework as introduced by 3GPP. Second, the MEC service model should be revised in order to guarantee security and isolation for network slices. Finally, the registration and discovery of MEC services, provided by third-party MEC applications, need to be adapted to the context of sliced MEC.

5G!Drones will address the aforementioned gaps, by: (i) updating the Network Slicing architecture adopted by each facility to integrate MEC; (ii) leveraging the orchestration/management solutions via enablers, which will be plugged into the Facilities, aiming at allowing the deployment of a MEC platform (MEP) as well as MEC applications in a 5G environment that supports Network Slicing.

Different options will be envisioned and studied by 5G!Drones to position the MEP in a Network Slice. Either by considering MEP as VNF and include it in the Network Slice definition (or template); or consider MEP as a shared VNF or PNF among slices. The former is considered as in-slice deployment of MEP, while the latter corresponds to a multi-tenancy case. For both scenarios, the 5G!Drones MEC enablers will guarantee traffic isolation and security of each Network Slice at the edge, by ensuring that: (i) each Network Slice should share the common infrastructure in a secure way; (ii) each network slice shall not see the traffic of other slices, or have access to information on other running slices.

In ETSI group, report [45] as of November 2019 made consolidated recommendations (CR) which are summarised below:

- [CR-1] It is recommended that the Multi-access Edge Application Orchestrator (MEAO) supports the capability to distinguish operations based on the available NSIs and their different requirements (e.g. bandwidth, latency, security, etc.). To that end, the Mm3 reference point needs to support per-NSI operations.
- [CR-2] It is recommended that a MEP supports the capability to serve a single NSI.
- [CR-3] It is recommended that a MEP supports the capability to serve multiple NSIs.
- [CR-4] It is recommended that a MEC application may be associated to a specific NSI.
- [CR-5] It is recommended that a MEC application may also be associated to multiple NSIs.
- [CR-6] It is recommended that the MEC system supports the capability to collect and expose usage and performance data per NSI. This allows to verify the fulfilment of the Service-Level Agreement (SLA) requirements per NSI and react accordingly.

In addition, this same ETSI group report [45] as of November 2019 made recommendations for future work:

- To capture the consolidated recommendations as normative requirements in ETSI documents;
- To collaborate with ETSI ISG NFV for identifying which NFV procedures may require extension when MEC is deployed in an NFV environment and the network slicing concept is adopted. This may include the scenarios where the MEC components are either shared across multiple Network Slices or dedicated to a single Network Slice;
- To collaborate with 3GPP for identifying which 3GPP procedures may require extension when MEC is deployed in a 5G network. This may include the scenario where the MEP plays the role of a 5G Application Function (AF) towards the 5G core network and a 3GPP NSI is created or terminated;
- To collaborate with ETSI ISG NFV and 3GPP all together for identifying the necessary extensions when MEC is deployed in an NFV environment within a 5G network. This scenario considers both network slicing concepts (i.e. 3GPP and ETSI NFV) being applied simultaneously.

6.1.3. Unified Interfaces over Heterogeneous Facilities

5G!Drones will run several use cases over different Facilities. This includes two ICT-17 Facilities (the Greece trial site of 5Genesis and the French trial site of 5G EVE) in addition to two complementary trial sites (5GTN of University of Oulu and X-Network of Aalto University). This diversity results in a heterogeneity in terms of the supported capabilities and offered interfaces. In order to abstract the underlying heterogeneity, unified interfaces should be developed and exposed to the upper layer. These interfaces expose common APIs enabling to access control, monitoring, management and orchestration services, and translate them to sites-specific APIs. The unified interfaces should be abstract regardless of the technology used by each trial site, allowing the upper layer (the trial controller) to be agnostic of the facility specificity. Therefore, the unified interfaces will rely on the APIs provided by the Facilities.

Each trial site is composed of different element at the infrastructure layer (e.g. RAN, transport, MEC, Cloud, etc.). These elements ensure the connectivity and the provisioning of 5G services by providing the computing, storage and networking resources which are required to run the underlying applications. A set of control tools are deployed on the top of the different segment to allow the configuration of the related resources. This includes the RAN controllers for the radio access technologies segment, the SDN controllers for the transport segment, the VIM for the cloud segment, etc. The control tools considered for the different Facilities can be heterogeneous, and so are the underlying interfaces. In order to enable the upper layer to control and configure the different segment, unified interfaces are necessary to be developed for the control plane.

Furthermore, unified interfaces are also necessary to expose trial sites' capabilities related to the orchestration plane. The latter coordinates network services across the different segments of the same facility. Taking into consideration that the trial sites can deploy different orchestration solutions, the unified interfaces will abstract the heterogeneity of these solutions and provide common interfaces for exposing the orchestration capabilities. Table 7 summarises the target planes for abstracting and unifying the exposed interfaces.

Table 7 - Target planes for abstracting and unified the exposed interfaces

Target plane	Description
Orchestration plane	Providing unified interfaces exposing the orchestration capabilities of the trial site.
Control plane	Providing unified interfaces for accessing and controlling the different segments of the facility (RAN, cloud, transport, etc.)

In order to develop common and unified interfaces exposing the trial sites' capabilities to the upper layer, a projection can be made with the related standards. Indeed, different solutions implement the operations and the data model specified in the standards. This is the case of many orchestration frameworks that are compliant with ETSI NFV MANO. However, while some operations and functionalities are specified in different standards, other extensions may be needed to support the operations which are not defined in the standards (e.g. advertising deployed resources and their capabilities).

6.1.4. Use Case Data Storage and Analysis Services

The data storage and analysis services component needs to accommodate various data sources in a distributed system of systems. Ingesting data follows an Extract, Transform, Load (ETL) approach as shown in Figure 27.

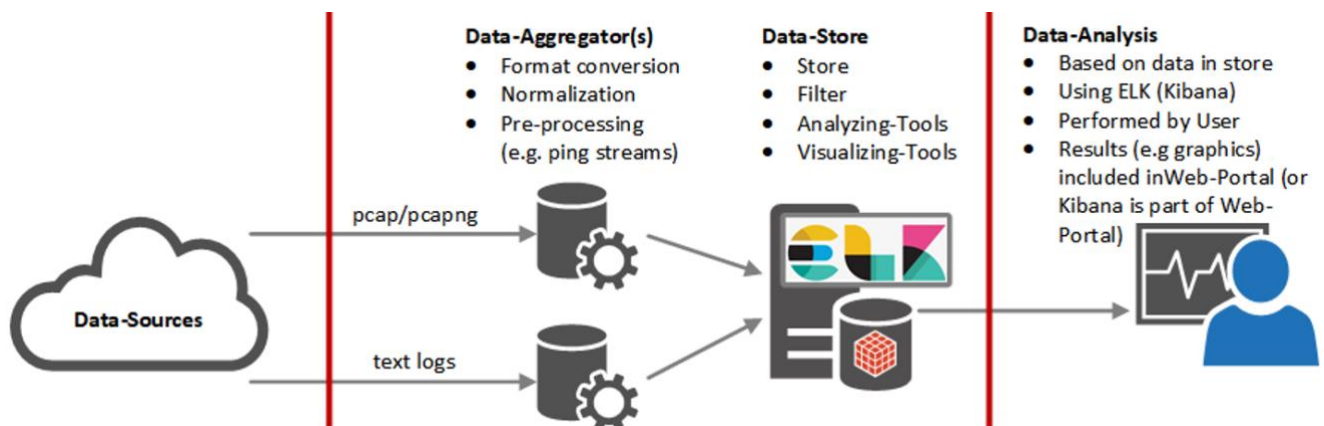


Figure 27 - High Level Architecture Data Storage & Analysis Services

Data is extracted by the originating component. Moreover, via IP network, data is transported to so called data-aggregators which take care of:

- Extracting data;
- Normalising data (where applicable);
- Pre-processing data (where applicable);
- Loading data to the Data-Store.

Data Aggregators might be reused by different originating components; this is likely for components providing logically similar data.

The Data-Store provides built-in means to store, filter/query, analyse and visualise data loaded by the aggregators. A machine-to-machine interface can be used by decoupled analysis components (which are out of scope of the core component). It is currently foreseen to utilise and adopt existing software, the so-called ELK Stack. Depending on a comparison of other, similar solutions, this decision might be revisited in the respective task T2.4 ('Tools for experimenting data analysis and visualisation') of WP2. Regardless of the chosen solution, high level requirements to enable meaningful reporting and analysis will need to be met by components utilising the data storage and analysis service:

- Meta-information on the provided data must be available.
- Data must be timestamped.
- Data originating components must be time synchronised.
- Where KPIs are defined, it must be ensured, that the respective values can be quantified and calculated from the provided trial-data.

After a defined period (or when exceeding a configurable storage size), data can be exported from the storage and will be automatically purged.

6.1.5. MCS Solution

Based on the general description of MCS [94] provided in subsection 3.1.8, the following subsection describes the components and technologies of the Airbus MCS solution, which provide voice services, instant messaging, video communication and emergency calls.

MCS architecture

The following Airbus MCS service components, which have been developed during the H2020 5GENESIS EU-funded project [86], are deployed as part of the Airbus MCS solution:

- *Infrastructure components*
 - **MCS Server:** the MCS Server provides the control and management of voice, video and data communications for both private and group calls.
 - **Identity Management Server (IdMS):** this server manages the MCS users' credentials.
 - **Key Management Server (KMS):** this server stores and distributes the security information such as encryption keys for private and group calls.
 - **Group Management Server (GMS):** this server is used to perform the management of communication groups.
 - **Configuration Management Server (CMS):** this server manages MCS configurations (e.g. user profile, UE configuration, functional aliases and service configuration).
 - **MCS Configuration Server:** it is used by the MCS system administrators for the management of tactical and technical configuration information.
- *Client component:*
 - **MCS Client application:** it runs on the mobile device and implements the MCS protocols, the MCS client entities which are communicating with the servers mentioned above, and the graphical user interface.

These MCS components are further detailed in [86].

MCS APIs

The following application programming interface (API) features could be developed during the course of the project:

- connection in order to receive video streams from an external video source
- sending of a video stream to an external receiver
- interface to integrate the MCS services, i.e. Push-To-Talk (MCPTT), Video (MCVideo) and Data (MCData) communications, into infrastructure and mobile applications

6.2. UAV Service Enablers

To fully support the scenarios to be trialled, different use case Service Enablers are required. These enablers are software functions that are either directly running on the UAV, running remotely (e.g. on edge servers or clouds) or supporting UAV operations. They are responsible for control or application functionalities (e.g. UAV swarm control, 3D mapping algorithm, IoT sensor software ...). By interacting together, they constitute the specific UAV application a scenario wishes to trial.

Each scenario, based on what it aims to achieve, requires a different set of service functions. Part of the functions (e.g. command and control related functions) can be common to different scenarios. The rest of them are specific to the application targeted by a given scenario. These Service Enablers presented in the following subsection will have to be developed within the project (or enhanced/adapted if they already exist) in order to trial the scenarios.

6.2.1. Required Set of Service Enablers per Scenario

The following tables describe each scenario's required set of functions. Those functions are sorted according to where they are running. We can distinguish the following running entities:

- **UAV:** Mainly functions for interfacing the UAV's autopilot and its embedded equipment with 5G (e.g. streaming telemetry, streaming sensor data, C2 Link...);
- **Edge:** UAV management software and application specific functions (e.g. real time data processing) requiring low latencies;
- **Cloud:** Centralised UAV management software or application specific functions requiring more processing power;
- **Operator:** Controlling UAVs, supervision and accessing the mission's outcomes (e.g. processed data such as a 3D map);
- **Delivery Box:** this entity is used in the context of parcel drop-off, in the UAV logistics scenario described in 6.2.2.3;
- **IoT camera:** used in the scenarios described in 6.2.3.1 and 6.2.3.3, this entity hosts functions that allow providing video from crossroads or from other hotspots;
- **First responder:** the corresponding entity hosts functions to allow watching video streams and data from UAVs and from IoT cameras;
- **End user:** the corresponding entity hosts 5G smartphone functions.

6.2.2. Use Case 1: UAV Traffic Management

6.2.2.1. UC1 Scenario 1: UTM command and control application

Table 8: UC1SC1 Service Enablers

Entity	Function	Description
UAV	Interface with autopilot	Interfacing with autopilot for C2 link and telemetry streaming to GCS (CUP or UL-CCP)
	Video streaming interface	Video streaming from UAV's camera to Operator using CAFA Field video solution
Edge	CAFA Tech UGCS based platform (CUP)	CUP for UAV Command and Control
	Unmanned Life Central Command Platform (UL-CCP)	C2 link to UAVs for mission management & swarm control, interfacing with UTM, and forwarding of video data to visualisation functions
	CAFA Field video software incl. Video analyser	Video streaming from UAVs to Operator and Command Centre
Cloud	INVOLI Central Server	Feeding air traffic data to UTM
	CAFA Central server	For data storage and coordination and Big Data analysis
Operator	Video stream reception and visualisation	For video feed CAFA Field.
	Controlling UAV	Controlling UAVs by CUP and UL-CCP

Remark: As UTM will be implemented in all the scenarios, INVOLI's Central Server Solution will systematically be part of the service functions set of every scenario. In order to avoid repetition, this function will only appear here.

6.2.2.2. UC1 Scenario 2: 3D mapping and supporting visualisation/analysis software for UTM

Table 9: UC1SC2 Service Enablers

Entity	Function	Description
UAV	Interface with autopilot	Interfacing with autopilot for C2 link and telemetry streaming to GCS (UL-CCP) through UL-ACE
	Sensor data streaming	From UAV to MEC – Video and other sensor data
Edge	Unmanned Life Central Command Platform (UL-CCP)	Video and IoT sensor data stream forwarding to Operator
		Mission management
		Swarm control
		Interfacing with UTM
	Video Processing	
	3D map processing	

Operator	3D map visualisation	Visualisation of the 3D map results via VR goggles
-----------------	----------------------	--

6.2.2.3. UC1 Scenario 3: UAV logistics

Table 10: UC1SC3 Service Enablers

Entity	Function	Description
UAV	Interface with autopilot	Interfacing with autopilot for C2 link and telemetry streaming to CAFA GCS (CUP)
	Video streaming interface	Video streaming from UAV to Command Centre Operator using CAFA Field video software
Delivery Box IoT sensor	IoT sensor based on NB-IoT or LTE-M Cat1/2 technology	Provides information about Delivery box status and helps parcel drop-off
Edge	CAFA IoT software	Communication between IoT sensor and CAFA CUP and DLN DS
	CAFA Tech UGCS based platform (CUP)	UAV C2 flight management Interfacing with UTM
	CAFA Field Video software	Video streaming from UAV to Command Centre Operator using CAFA Field video software
Cloud	Drone Logistics Network Delivery Software (DLN DS) CAFA Tech server	DLN DS coordinates delivery information between customer delivery box, UAV and logistics centre. CAFA Tech central server stores data and videos and provides Big Data analyse.
Operator	Video stream	Video streaming from UAV to Command Centre Operator using CAFA Field video software
	Controlling UAV	Through CUP

6.2.3. Use Case 2: Public Safety/Saving Lives

6.2.3.1. UC2 Scenario 1: Monitoring a Wildfire

Table 11: UC2SC1 Service Enablers

Entity	Function	Description
UAV	Interface with autopilot	Interfacing with autopilot for C2 link and telemetry streaming to CAFA UGCS platform (CUP)
	UAV video camera streaming	From UAV to Operator through CAFA Field video solution
	MCS client	UAV can embed MCS client application (trade-off between UAV choice/capacity and security using E2E security)
IoT camera	IoT camera based on LTE-M Cat1/2 technology	Provides video from crossroads or from other hotspots

Entity	Function	Description
Edge	Airbus Multimedia Mission Critical Services Platform	Mission critical multimedia collaborative platform implementing 3GPP MCS providing secured services MCPTT, MCVIDEO and MCDATA
	CAFA Tech UGCS based platform (CUP)	Video and IoT sensor data stream forwarding to Operator Flight management Interfacing with UTM
	CAFA Field video analyser	Analysing video feed and photos from UAV and from IoT camera
Cloud	MCS – Web Portal	Airbus critical collaboration platform frontend for system administration (authorisation management, users management, communications management, identity management, encryption keys management, ...) as well as participating in secured communications
	CAFA Field	CAFA Tech central server stores data and videos and provides Big Data analyse.
Operator (Rescue Command Centre)	Video and IoT data stream reception and visualisation	Airbus MCS Web Portal
	Controlling UAVs	Through CAFA CUP and Field system
First responder	5G smartphone	To watch video stream and data from UAVs and from IoT cameras
	MCS application clients	MCS application running on mobile platform.

6.2.3.2. UC2 Scenario 2: Disaster Recovery

Table 12: UC2SC2 Service Enablers

Entity	Function	Description
UAV	Interface with autopilot	Interfacing with autopilot for C2 link and telemetry streaming to GCS (UL-CCP) through UL-ACE
	Sensor data streaming	From UAV to Operator – Video or other IoT Sensor data
Edge	Unmanned Life Central Command Platform (UL-CCP)	Video and IoT sensor data stream forwarding to Operator Mission management Swarm control Interfacing with UTM
Cloud	3020 LifeX solution	Emergency calls management Presenting emergency calls to the control room operator Presenting sensor and drone data to the control room operator

		Interfaces with 3 rd party applications
Operator	Video and IoT data stream reception and visualisation	From video processing functions on the edge
End user	5G Smartphone	

6.2.3.3. UC2 Scenario 3: Police, incl. counter-UAS

Table 13: UC2SC3 Service Enablers

Entity	Function	Description
UAV	Interface with autopilot	Interfacing with autopilot for C2 link and telemetry streaming to GCS (CUP)
	UAV video camera streaming	From UAV to Operator through CAFA Field video solution
IoT camera	IoT camera based on LTE-M Cat1/2 technology	Provides video from hotspots
Edge	Police Video Analyser and CAFA Field streaming software (PVA)	PVA analyses videos from UAV and from IoT sensors/cameras and streams videos to field officers and to Police Command Centre and to Operator
	CAFA Tech UGCS based platform (CUP)	C2 flight management Interfacing with UTM
Cloud	Police Command Centre Server (CAFA Tech Central server)	Provides situational awareness thanks to UAVs video feed and IoT cameras and provides the access to CUP platform.
Operator (Police Command Centre)	Video and IoT data stream reception and visualisation	Through Police Video Analyser (PVA) and CAFA Field streaming software
	Controlling UAVs	Using CAFA CUP platform

6.2.4. Use Case 3: Situation Awareness

6.2.4.1. UC3 Scenario 1: Infrastructure Inspection

- UC3 Sc1 Sub-scenario 1: 3D Mapping of 5G QoS

Table 14: UC3SC1Sub1 Service Enablers

Entity	Function	Description
UAV	Interface with autopilot	Interfacing with autopilot for C2 link and telemetry streaming to GCS (CUP)
	Sensor data streaming	From UAV to Operator (through CAFA Field) – QoS data and photos for 3D mapping

Entity	Function	Description
Edge	CAFA Analyser	Analysing QoS and 3D Mapping
	CAFA Tech UGCS based platform (CUP)	Flight management Interfacing with UTM
Cloud	CAFA Central platform	Data storage and Big Data analysing
	3D Map processing software	Processing 3D map from photos collected by the UAV
Operator	CAFA Tech UGCS based platform (CUP)	Controlling UAVs
	CAFA Analyser	Viewing 5G QoS

- UC3 Sc1 Sub-scenario 2: Long Range Power Line Inspection**

Table 15: UC3SC1Sub2 Service Enablers

Entity	Function	Description
UAV	Interface with autopilot	Interfacing with autopilot for C2 link and telemetry streaming to Hepta's GCS
	Sensor data streaming	From UAV to Operator and data processing on Edge – Video stream + Pictures and LIDAR data
Edge	Data processing	Image processing SLAM with LIDAR data
Cloud	Hepta's Data Cloud	
Operator	Hepta's GCS	Receiving FPV video stream and telemetry from UAV and controlling UAV Interfacing with UTM

- UC3 Sc1 Sub-scenario 3: Inspection and Search & Recovery Operations in Large Body of Water**

Table 16: UC3SC1Sub3 Service Enablers

Entity	Function	Description
UAV	Interface with autopilot	Interfacing with autopilot for C2 link and telemetry streaming to GCS
	Sensor data streaming	From UAV to Operator and Data processing on edge – Video and sensor data
Edge	Data processing	Sensor data processing
Operator	Alerion's GCS	Receiving FPV video stream and telemetry from UAV and controlling UAV

	Interfacing with UTM
--	----------------------

6.2.4.2. UC3 Scenario 2: UAV-enhanced IoT Data Collection

Table 17: UC3SC2 Service Enablers

Entity	Function	Description
UAV	Interface with autopilot	Interfacing with autopilot for C2 link and telemetry streaming to virtual flight controller
	Sensor data streaming	From UAV to Operator– Video + IoT Sensors data
Cloud	Virtual flight controller (UAV operator software)	Receiving UAV mission Controlling UAV Interfacing with UTM
	Data processing (streamer, transcoder, cache, IoT data aggregator)	Performing video streaming, transcoding and caching Data aggregation and analysis
Edge	Virtual flight controller and data processing components can also be deployed at the edge	Performing video streaming, transcoding and caching Data aggregation and analysis

6.2.4.3. UC3 Scenario 3: Location of UE in non-GPS Environments

Table 18: UC3SC3 Service Enablers

Entity	Function	Description
UAV	C2 Link & Telemetry interface	C2 link and telemetry streaming between UAV and virtual flight controller
	Sensor data streaming	From UAV to Edge Position software
Edge	Positioning analysis application	
	Data collection and mapping	For collection and storage of incoming data
Cloud	UAV Control	Controlling UAV with video feed

6.2.5. Use Case 4: Connectivity During Crowded Events

6.2.5.1. UC4 Scenario 1: Connectivity extension and offloading

Table 19: UC4SC1 Service Enablers

Entity	Function	Description
--------	----------	-------------

UAV	Interface with autopilot	Interfacing with autopilot for C2 link and telemetry streaming to GCS (UL-CCP) through UL-ACE and CAFA CUP (for Mavic drone)
	Video streaming	From UAV to Operator and to Command Centre through CAFA Field video
	5G QoS sensor	QoS sensor sends from UAV to CAFA Analyser
Edge	Unmanned Life Central Command Platform (UL-CCP)	Video stream forwarding to video streaming server Mission management Swarm control Interfacing with UTM
	CAFA CUP (for DJI Mavic)	Mission management and Interfacing with UTM
	CAFA Field	Video streaming software
Cloud	CAFA 3D Map	Processing of 3D QoS data
Operator (Command centre)	CAFA 3D Map	Real time network quality 3D environment visualisation
	CAFA Field	UAVs Video stream visualisation
	UL-ACE and CAFA CUP	Controlling UAVs and interfacing with autopilot for C2 link and telemetry streaming to GCS (UL-CCP) through UL-ACE and CAFA CUP (for Mavic drone)

6.3. Cybersecurity Support

Cybersecurity support in 5G!Drones encompasses both cybersecurity of 5G network and services in scope. To have it framed we propose the 5G!Drones high-level security architecture to mostly follow the 5G security architecture originating from 5G-ENSURE, exploited at 5G-PPP Architecture WG, and continued in SENDATE (see its description in the following documents [9], [10] (§2.5) and [11]).

To summarise, this architecture consists of:

- 5G (Network) Domains: such domain is a logical grouping of network entities (physical or logical) that belong to specific actor(s) with a specific role/responsibility; split in three categories:
 - Infrastructure Domains;
 - Tenant Domains;
 - Compound Domains (mix of Infrastructure and Tenant Domains), among which the Slice Domains.
- 5G Strata: A Stratum is a coarse-grained grouping of protocols, data types and functions related to a specific aspect of services provided by one or more Domains, with similar security requirements. The architecture identifies the following strata:

- Application stratum;
- Home & Serving stratum (further split in two in [12] for instance);
- Transport stratum;
- Management stratum.
- Security Control Classes (SCC): a SCC is a collection of security controls addressing a common security goal. Identified SCCs (see aforementioned publications for definitions):
 - Identity & Access Management;
 - Authentication;
 - Non-repudiation;
 - Confidentiality;
 - Integrity;
 - Availability;
 - Privacy;
 - Audit;
 - Trust & Assurance;
 - Compliance.

A joint analysis of Domains and Strata enables 5G system architects to identify the required security control points for each kind of protocol, data or function; and the security control classes help select the appropriate controls for each kind of security goal.

We propose to develop a bit further the aforementioned generic architecture approach to achieve a security architecture baseline made of 5G Security Enablers elaborated in the next sections. The terminology originates mostly from SCCs mentioned earlier, completed by documents [13], [14].

The 5G Security architecture approach advocated here for 5G!Drones is aligned with overall 5G!Drones architecture underlying concepts and paradigm (e.g. SDN, NFV, ..) with objective to get them declined to Security topics moving towards Software-Defined SECurity (SD-SEC) and Security as a Service (SECaaS).

6.3.1. Identity and Access Management (IAM) Services

The IAM Services include the following:

- Digital Identity Services: manage the lifecycle of identities of all network entities (e.g. UEs, UAVs, VNFs/PNFs, slices) of the 5G system, as well as end-users (e.g. tenant administrators from UAV verticals).
- Directory Services: provide standard interfaces to store and search for identities, associated attributes, esp. security-relevant attributes (roles, groups, organisation, etc.); and user self-services where they can manage their own account.
- Credentialing Services: bind credentials (certificate, public key, password, hardware tokens, etc.) to an identity for authentication.

- **Authentication Services:** provides authentication of network entities, including UEs and UAVs, required for network access, UAV application access, Trial Controller's API or web portal access, as well as access to MANO and security services management interfaces.
- **Security Token Services:** issue security assertions, preferably in form of self-contained signed tokens, that can be reused as access token for most if not all protected interfaces of the 5G system that require authentication.
- **Identity Federation Services:** provide mechanisms to reuse identities of a third-party domains; this is essential when entities have identities and authentication capabilities pre-existing to the 5G system since it gives the opportunity to reuse those and perform just-in-time provisioning of their identities in the 5G system. This requires establishing a trust relationship between the 5G system's IAM service and the third-party identity management system.
- **Privilege Management Services (incl. role/group management):** for access control purposes (e.g. allowing only tenant admins to access the MANO interfaces), it is necessary to assign and manage roles, groups and other authorisation attributes of end-entities.
- **Authorisation Service (Policy Decision):** provides access policy management and decision engine that provides access control decisions (Permit/Deny with possibly associated obligations) to Policy Enforcement Points enforcing access control typically in the data plane (or MANO interfaces), based on various types of attributes of the access request, including the attributes of the access requester (e.g. user/UAV), requested action, requested resource, and environment/context attributes (e.g. from Security Monitoring Services).

6.3.2. Digital Certificate Services (PKI)

Digital Certificate Services provide digital certificate lifecycle management. They should support:

- PKI standards: X.509, CRL, OCSP, EST, CMP;
- HSM integration for private key protection;
- CA hierarchies;
- Cross-certification.

Digital Certificate Services provide certificates used in many 5G-related communication protocols (e.g. EAP-TLS, IPsec/SSL VPN), and UAV and MANO transport-level or application-level data exchange protocols (e.g. HTTPS), for mutual authentication and signature (verification). Most importantly, it provides the root of trust for interactions between the various network entities.

6.3.3. Cryptography Services

The cryptography services provide secure access to high-integrity cryptographic operations backed by a HSM (or vHSM supported by a physical HSM) through standard interfaces such as PKCS#11 or higher-level remote API:

- **Cryptographic Key Management Services**
Provide secure generation and secure storage of symmetric keys as well as asymmetric key pairs.
- **Cryptographic Functions API**

Enables clients to call the following cryptographic primitives with one of the managed keys as argument:

- Encryption (e.g. AES);
- Signing (e.g. RSA, ECDSA, EdDSA);
- MACing (e.g. HMAC-SHA256);
- Message digesting (e.g. SHA256);
- Secure random number generation.

6.3.4. Network Access Control Services (NAC)

Perform access control at the network-level (e.g. 5GC's SMF/AUSF, DN-AAA).

6.3.5. Security Policy Management and Orchestration Service (SPS)

This service is also known as policy enforcement framework in [11], § 5.2. To summarise, based on input tenant-specified security policies, or policy-annotated network slice templates, the service computes a policy-compliant E2E slice deployment in the form of security VNFs and/or VNF/PNF security tuning, and composition/orchestration thereof, and/or SDN applications; and deploys it via the NFV orchestrator and SDN controller.

The service may also reconfigure or re-deploy a slice (or slice subnet) automatically, upon receiving specific input from the Security Monitoring services such as a particular security event, in order to remedy a detected security issue. This strategy enables DDoS mitigation for instance:

1. An anomalous traffic increase is detected by the Security Monitoring Service, translated to meaningful security event for the decision engine of the Security Policy Management and Orchestration service.
2. The latter is then triggered to remedy the situation by instantiating new VNFs to handle (block/limit/divert) the DDoS traffic via the NFV orchestrator on the one hand; and reconfiguring the VNF forwarding graph via the SDN controller on the other hand.

The types of policies that the service should support correspond to the Security Control classes mentioned earlier:

- Confidentiality protection policies (e.g. encryption)
- Integrity, authenticity and non-repudiation protection policies (e.g. MACing, signing, etc.)
- Availability protection policies (e.g. (D)DoS mitigation, load-balancing, failover, scaling, replication, etc.)
- Firewalling policies
- Access Control policies, e.g. network-level (AAA), transport-level or application-level:
 - Authentication policies;
 - Authorisation policies;
 - Accounting/Audit policies.
- Privacy policies

- Audit policies (not specific to access control)
- Compliance policies (e.g. regulations, directives, etc.)
- Trustworthiness policies (e.g. security certification level, trusted boot, TEE, binary protection, etc.)

This software-defined, policy-driven approach to security management is applicable for drones. It may also be explored for other verticals (e.g. vehicular systems [96], [98]), and beyond security [97].

6.3.6. Security Policy Enforcement Point Services (PEP)

Security PEPs are policy-driven security controls, orchestrated by the SPS. PEPs are typically deployed as part of the network slice (data plane):

- Security VNFs or security modules on-board VNF/PNF, in the Core Network and the MEC;
- Security modules on board the UE/UAV.

We identify the following kinds of PEPs according to the kinds of policies identified in the previous section:

- Network (Slice) Access Control PEPs (Switch, Firewall, VPN gateway, SEAF/AUSF, etc.)
- Network/Transport/Application-layer security filters/proxies/gateways (e.g. WAF, API security gateway, etc.)
- IDS/IPS
- SIEM/SLA/Compliance Monitoring Agents
- VNF/PNF component and Endpoint (e.g. UE/UAV) security controls: Trusted Boot, TEE, cryptographic module, communications security modules (incl. VPN client), authentication modules, OS security modules, compliance verification, vulnerability scanner, anti-malware, etc.

However, this is merely an initial proposal that we expect to change as the specifications of the UAV use cases are being refined.

6.3.7. Security Information and Event Management Services (SIEM)

As defined in NATO C3 Taxonomy baseline 3.1, “*The Security Information and Event Management (SIEM) Services combines support of security information management and security event management to provide real-time analysis of security alerts generated by service assets (e.g. user applications, IT Services and communications equipment), to identify security threats, detect and prevent breaches, and provide forensic analysis. SIEM Services also support logging and analysis of security data and generation of reports for compliance purposes.*” In short, SIEM services include among others:

- Security event log management;
- Security monitoring and alerting;
- Security auditing and reporting.

The main sources of logs for the SIEM services are the Security PEPs mentioned previously, and other Security Services such as IAM services, NAC services, Security SLA Management Service. The SIEM interacts with the SPS to trigger countermeasures for security issues.

6.3.8. Security SLA Management Service

This service is also known as *Security SLA Monitoring and Metrics* in [11]. To summarise, it is responsible for capturing metrics, compare them against security SLAs, and in case of deviations, notify the SIEM service which may translate that into the proper security event for the Security Policy Orchestration Service to deploy the counter-measure if any.

6.3.9. Airbus MCS Security

The security of the Airbus MCS, i.e. Push-To-Talk (MCPTT), Video (MCVideo) and Data (MCData) communications, is partially compliant with 3GPP TS 33.180 [95], which specifies MCS security. In this regard, Airbus MCS offers the following features:

- Signalling plane security mechanisms:
 - Protection of the signalling plane;
 - Protection of intra domain interfaces.
- application plane security mechanisms:
 - Authentication and authorisation of MCS users;
 - Security of RTCP for floor and transmission control using SRTCP;
 - And end-to-end security of user media using SRTP.
- A centralised Key Management Server (KMS) provisions the key material for MCS users, MCS Server and Group Management Server.

6.3.10. Security for IoT solutions

In 5G!Drones, four of the trialled use cases will feature IoT sensors: UC1 Sc4 (“UAV Logistics”), UC2 Sc1 (“Monitoring a wildfire”), UC2 Sc3 (“Police incl. Counter-UAS”) and UC3 Sc2 (“UAV-based IoT data collection”). It is therefore important to ensure a thorough IoT support in the context of 5G. Several articles have been published on this topic, as the importance of the domain increases every year. One possible solution is shown below.

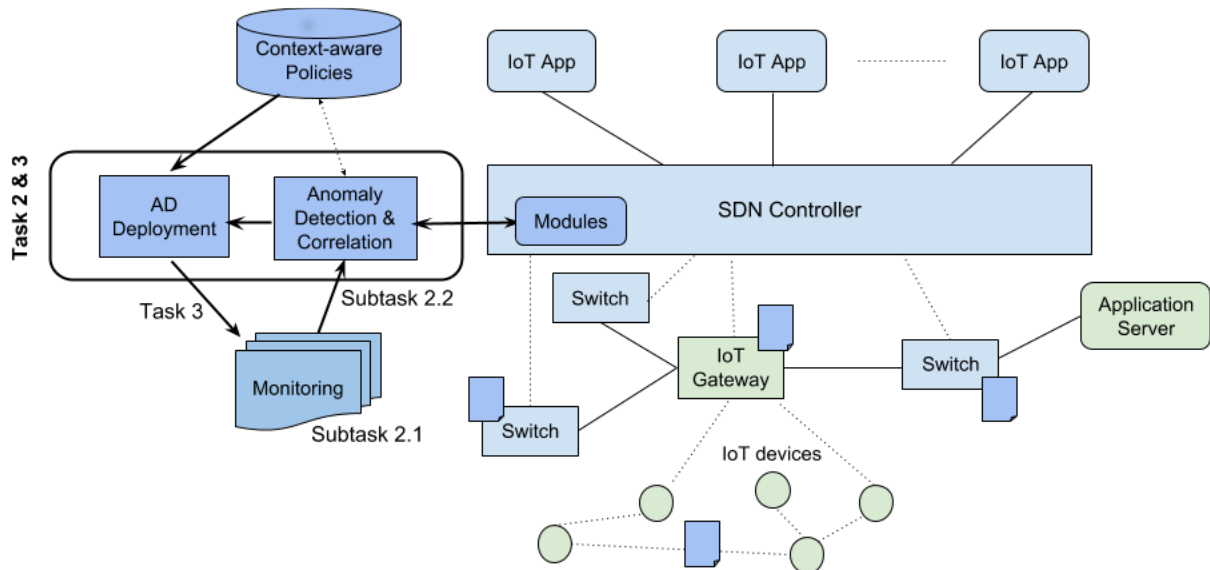


Figure 28 - Proposed IoT Network Forensics Framework [44]

Figure 28 outlines the main operating principles of dynamic forensics framework, which need to be addressed in the field of IoT device security. Those principles notably encompass two important mechanisms:

- Big data analytics for security intelligence: traffic monitoring, data collection, pre-processing, fusion, analysis and anomaly detection;
- Proactive network control for timely, optimal reactions: deployment of anomaly detectors, enforcement of security policies.

The security features that need to be implemented to adequately protect IoT Service assets are specific to each service. Therefore, it remains the responsibility of the IoT Service Provider to use proper risk and privacy impact assessment processes to derive their specific security needs. MNOs and IoT Service Providers often share similar security requirements to protect their assets, therefore it makes sense for them to leverage on common security solutions rather than implementing duplicate (and potentially redundant) security infrastructures [84].

The service platform guidelines offered in [85] may benefit the MNOs who support IoT Connectivity Management Platforms. These guidelines contain the following recommendations:

- Network Operators should make sure access to their IoT Connectivity Management Platform's web portal, which could be Network Operator or Cloud hosted, uses 'best in class' encryption as per the most recently published industry guidance from organisations such as NIST and ECRYPT2;
- MNOs should ensure that accessing to their IoT Connectivity Management Platform's web portal makes use of standard "best practice" procedures for password creation, updating and resetting [84].

Security in Service Endpoint environments can be designed using common pieces of infrastructure, strategies, and policies, regardless of the topology or innovations used to build an application architecture. Each aspect of the Service Ecosystem can be broken down into components. These components must be secured individually, but using similar methodologies.

For example, consider the common components in building a simple service that is capable of fielding queries and sending responses from and to endpoints, partners, and users. This model should contain, but not be limited to, the following tiers [85]:

- A Web Service Tier;
- An Application Server Tier;
- A Database Tier;
- An Authentication Tier;
- A Network Tier;
- Third party application tiers, such as a Billing tier.

In this context, the main challenges involve three main domains:

1. Data, which is volatile and hard to process at device-level (lack of context and scarcity of resources) need for more effective monitoring tools and platforms;

2. Baseline, i.e. lack of global network visibility and variety of IoT data deep learning algorithms for real-time anomaly detection;
3. Reconfiguration, i.e. lack of infrastructure and dynamicity of IoT event-driven, context-aware and self-adaptive anomaly detectors deployment using SDN/NFV [44].

6.3.11. Cybersecurity tests

In complement to the design of a cybersecurity suite adapted to the needs of 5G!Drones, which has been reported in subsections 6.3.1 to 6.3.10, it is also necessary to evaluate the aforementioned cybersecurity solutions and perform subsequent tests as follows:

- Vulnerability Scanning;
- Security Scanning;
- Penetration testing;
- Risk Assessment.

Based on 5G!Drones deliverable D1.4 (Integration plan), the following trials are planned:

- Feasibility tests;
- Preliminary trials;
- Preliminary trials (Phase 2);
- Final trials.

It is worth highlighting that these trials are ideal for testing cybersecurity solutions too. Therefore, it makes sense to perform cybersecurity tests before and during the planned UAV trials. In general, the applicability of the aforementioned security concepts will be analysed in the project work packages WP2 and WP3 as part of the detailed design. Moreover, those tests will be detailed with the further 5G!Drones integration plan, and reported in the final version of this deliverable, D1.6.

7. CONCLUSION

This deliverable D1.3 has addressed the general objective from the 5G!Drones project, formulated as follows: first to support the selected use cases over a federated, multi-domain 5G infrastructure, and secondly, to execute large-scale UAV trials.

To that end, D1.3 provided introductory and contextual information in Section 2, to clarify the general purpose of the 5G!Drones project. In particular, it summarised the concepts of UTM and U-Space, along with the outcomes of relevant European projects and regulation bodies. This aspect, together with the summary of the envisioned UAV use cases which are further reported in deliverable D1.1, gave an overview on the structuring aspects that influence the project system architecture.

In Section 3, D1.3 then gave an overview of the main generic aspects of the 5G architecture that are relevant to 5G!Drones. A general description of the 5G system was followed by a more in-depth description of software-defined networking, network function virtualisation, network slicing and multi-access edge computing, which, among other topics explained in this overview, are key concepts for the support of the 5G!Drones overall architecture. This part of the deliverable also summarised the different approaches taken by standardisation bodies such as 3GPP to consider the interoperability of 5G systems with UTMs. Likewise, a description of the potential interrelations between the 5G!Drones architecture with relevant projects from the 5G Infrastructure Public Private Partnership (5G PPP) was given. On that basis, deliverable D1.3 then provided in Section 4 a high-level representation of the overall 5G!Drones architecture, notably giving a breakdown of this architecture into major components. It explained how they are meant to interact together, with the UAV verticals and with 5G Facilities to enforce the relevant UAV service logic.

This description was followed, in Section 5, by a study of how trialled UAV use case requirements will be met by the specific 5G Facilities, through a gap analysis respectively in the context of the X-Network, 5GEVE, 5GTN and 5GENESIS Facilities. In this context, D1.3 started the outline, in Section 6, of the 5G system enablers as well as the UAV Enablers which shall be designed in the 5G!Drones project. Section 6 also embraces cybersecurity support, introducing approach to 5G!Drones security high-level architecture as well as a set of 5G relevant security enablers.

Moreover, this deliverable shall be updated in the general timeline of the 5G!Drones project lifecycle. In particular, its release will be followed by deliverable D1.6, due at month 18. It is expected that the update will address two main objectives. First, it will provide a calibrated view on the project overall architecture, based on feedback from implementation and integration activities conducted in work packages WP2-WP4. At the release of D1.3, one of the primary purposes of task T1.4 is therefore to tightly interact with the aforementioned work packages, in order to consistently collect the relevant architectural information and gradually prepare D1.6. Secondly, several structuring sections from deliverable D1.3 will require, along the road towards the publication of deliverable D1.6, a careful analysis of the progress made by the Academia, the Industry, the involved standardisation and regulation bodies, and other relevant parties. That is notably the case of the general landscape of UTMs and U-Space, in Section 2, which will require a careful observation and, if and where applicable, relevant updates as well as an analysis of the potential impacts of the 5G!Drones architecture. Likewise, the progress made by the different standardisation bodies such as 3GPP, for instance to consider the interoperability of 5G systems with UTMs, will require a careful update in Section 3. That is also the case of the end of Section 3, focusing on the potential interrelations between the 5G!Drones architecture with relevant projects from the 5G Infrastructure Public Private Partnership (5G PPP), whose outcomes are likely to evolve until the release of D1.6.

References

- [1] “MEC in 5G networks,” ETSI WP#28. 1st ed., 2018.
https://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp28_mec_in_5G_FINAL.pdf
- [2] “Network Transformation (Orchestration, Network and Service Management Framework),” ETSI WP#32, 1st ed., 2019.
https://www.etsi.org/images/files/ETSIWhitePapers/ETSI_White_Paper_Network_Transformation_2019_N32.pdf
- [3] “Multi-access Edge Computing (MEC); Framework and Reference Architecture,” ETSI GS MEC 003 V2.1.1, 2019.
https://www.etsi.org/deliver/etsi_gs/MEC/001_099/003/02.01.01_60/gs_MEC003v020101p.pdf
- [4] “Developing Software for Multi-Access Edge Computing,” ETSI WP#20. 2nd edition, 2019
https://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp20ed2_MEC_SoftwareDevelopment.pdf
- [5] 5G!Drones project Grant Agreement
- [6] ETSI Multi-access edge computing main web page, <https://www.etsi.org/technologies/multi-access-edge-computing>
- [7] “System Architecture for the 5G System (5GS),” 3GPP TS 23.501 v16.2.0, 2019,
<https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3144>
- [8] “MEC Deployments in 4G and Evolution Towards 5G,” ETSI WP#24,
https://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp24_MEC_deployment_in_4G_5G_FINAL.pdf
- [9] “Security Architecture,” deliverable D2.4, 5G-ENSURE project, H2020-ICT-2014-2, 2016.
- [10] “View on 5G Architecture (Version 3.0),” 5G PPP Architecture Working Group, Whitepaper, 2019, https://5g-ppp.eu/wp-content/uploads/2019/07/5G-PPP-5G-Architecture-White-Paper_v3.0_PublicConsultation.pdf
- [11] “Reference Architecture,” deliverable D4.1.2, Celtic+ project SENDATE TANDEM
- [12] “General Universal Mobile Telecommunications System (UMTS) architecture,” 3GPP TS 23.101 version 15.0.0 Release 15, 2018,
<https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=782>
- [13] “C3 Taxonomy Baseline 3.1,” Consultation, Command and Control Board (C3B), NATO Unclassified, 2019.
- [14] “Security as a Service concepts and applicability, Design & SLA,” deliverable D4.4.1, Celtic+ project SENDATE-TANDEM, 2017.
- [15] U-Space Blueprint, SESAR Joint Undertaking, 2017,
<https://www.sesarju.eu/sites/default/files/documents/reports/U-space%20Blueprint%20brochure%20final.PDF>
- [16] Concept of Operation for European UTM Systems (CORUS) H2020 Project, SESAR Joint Undertaking Website, last retrieved Dec. 2019, <https://www.sesarju.eu/projects/corus>
- [17] “Initial view on Principles for the U-space architecture,” SESAR Joint Undertaking, 2019,
<https://www.sesarju.eu/node/3402>
- [18] “Manual on System-Wide Information Management (SWIM) Concept,” ICAO, Doc. 10039,
<https://www.icao.int/airnavigation/IMP/Documents/SWIM%20Concept%20V2%20Draft%20with%20DISCLAIMER.pdf>
- [19] “Network Operator Perspectives on NFV priorities for 5G,” ETSI White Paper issue 1, 2017,
https://portal.etsi.org/NFV/NFV_White_Paper_5G.pdf
- [20] “Network Functions Virtualisation (NFV) - Network Operator Perspectives on Industry Progress,” ETSI White Paper WP#3 issue 1, 2015,
https://portal.etsi.org/Portals/0/TBpages/NFV/Docs/NFV_White_Paper3.pdf
- [21] “Network Functions Virtualisation (NFV) - Architectural Framework,” ETSI Group Specification GS NFV 002 V1.2.1, 2014,
https://www.etsi.org/deliver/etsi_gs/NFV/001_099/002/01.02.01_60/gs_NFV002v010201p.pdf

- [22] A. Tzanakaki, M. Anastasopoulos and I. Berberana, “Wireless-Optical Network Convergence: Enabling the 5G Architecture to Support Operational and End-User Services,” IEEE Comm. Mag., vol. 55, no. 10, pp. 184-192, 2017.
- [23] “Linux KVM,” Last retrieved Jan. 2020, <https://www.linux-kvm.org>
- [24] “Dell, VMware,” Last retrieved Jan. 2020, <https://www.vmware.com>
- [25] M. Mahalingam et al., “Virtual eXtensible Local Area Network (VXLAN): A Framework for Overlaying Virtualized Layer 2 Networks over Layer 3 Networks,” IETF RFC 7348, 2014, <https://tools.ietf.org/html/rfc7348>
- [26] P. Garg et al., “NVGRE: Network Virtualization using Generic Routing Encapsulation,” IETF RFC 7637, 2015, <https://tools.ietf.org/html/rfc7637>
- [27] W. Xia, Y. Wen, C. H. Foh, D. Niyato and H. Xie, “A Survey on Software-Defined Networking,” IEEE Communications Surveys & Tutorials, vol. 17, no. 1, pp. 27-51, 2015.
- [28] I. F. Akyildiz, A. Lee, P. Wang, M. Luo and W. Chou, “A Roadmap for Traffic Engineering in SDN-OpenFlow Networks,” Computer Networks, vol. 71, no. 1, pp. 1-30, 2014.
- [29] “Helios by NEC,” Last retrieved Jan. 2020, <http://www.nec.com>
- [30] “5G White Paper,” NGMN Alliance, 2015, <https://www.ngmn.org/work-programme/5g-white-paper.html>
- [31] “Network Functions Virtualisation (NFV); Management and Orchestration,” ETSI GS NFV-MAN 001, v1.1.1, 2014, https://www.etsi.org/deliver/etsi_gs/NFV-MAN/001_099/001/01.01.01_60/gs_NFV-MAN001v010101p.pdf
- [32] “Network Functions Virtualization (NFV); Evolution and Ecosystem; Report on Network Slicing Support with ETSI NFV Architecture Framework,” ETSI GS NFV-EVE 012, v3.1.1, 2017, https://www.etsi.org/deliver/etsi_gr/NFV-EVE/001_099/012/03.01.01_60/gr_NFV-EVE012v030101p.pdf
- [33] “Study on architecture for next generation systems,” 3GPP TR 23.799 v14.0.0, 2016, <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3008>
- [34] “Study on management and orchestration of network slicing for next generation network,” 3GPP TR 28.801, v15.1.0, 2018, <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3091>
- [35] “Study on management and orchestration architecture of next generation network and service,” 3GPP TR 28.800, v15.0.0, 2018, <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3090>
- [36] “Study on management aspects of next generation network architecture and features,” 3GPP TR 28.802, v15.0.0, 2018, <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3092>
- [37] “Management of network slicing in mobile networks; Concepts, use cases and requirements,” 3GPP TS 28.530, v16.1.0, 2020, <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3273>
- [38] “Management and orchestration of networks and network slicing; Provisioning; Stage 1,” 3GPP TS 28.531, v16.4.0, 2020, <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3274>
- [39] “Management and orchestration of networks and network slicing; Provisioning; Stage 2 and stage 3,” 3GPP TS 28.532, v16.2.0, 2020, <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3427>
- [40] “5G System; Network Slice Selection Services; Stage 3,” 3GPP TS 28.533, v16.2.0, 2020, <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3416>
- [41] “Study on security aspect of 5G network management slicing,” 3GPP TR 33.811, v15.0.0, 2018, <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3358>
- [42] “NR; Overall description; Stage-2,” 3GPP TS 38.300, v16.0.0, 2020, <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3191>

- [43] “IMT Vision –Framework and overall objectives of the future development of IMT for 2020 and beyond,” Recommendation ITU-R M.2083-0, Sep. 2015, https://www.itu.int/dms_pubrec/itu-r/rec/m/R-REC-M.2083-0-201509-1!!PDF-E.pdf
- [44] G. Blanc, “5G Security: Research Interests,” 5G PPP Security WG meeting, Presentation on November 22nd, 2019.
- [45] “Multi-access Edge Computing (MEC); MEC Support for Network Slicing,” ETSI GR MEC 024 V2.1.1, 2019, https://www.etsi.org/deliver/etsi_gr/MEC/001_099/024/02.01.01_60/gr_MEC024v020101p.pdf
- [46] “Mobile Edge Computing (MEC); Deployment of Mobile Edge Computing in an NVF environment,” ETSI Group Report, MEC 017, V1.1.1, 2018, https://www.etsi.org/deliver/etsi_gr/MEC/001_099/017/01.01.01_60/gr_MEC017v010101p.pdf
- [47] “Vocabulary for 3GPP Specifications,” 3GPP TR 21.905, v16.0.0, 2019, <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=558>
- [48] “NG-RAN; Architecture description,” 3GPP TS 38.401, v15.6.0, 2019, <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3219>
- [49] “NR; Base Station (BS) radio transmission and reception,” TS 38.104, v16. 2.0, 2020, <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3202>
- [50] “3GPP Newsletter for 5G World Summit 2018,” 3GPP Brochure, 2018, https://www.3gpp.org/ftp/Information/presentations/2017_flip_brochures/2018_05_5g_world_brochure/mobile/index.html#p=5
- [51] “Study on Elevation Beamforming/Full-Dimension (FD) MIMO for LTE,” 3GPP TR 36.897, v13.0.0, 2015, <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2580>
- [52] “Radio Spectrum Policy Programme: the roadmap for a wireless Europe,” presentation of the RSPP on the European Commission institutional Website, last retrieved Jan. 2020, <https://ec.europa.eu/digital-single-market/node/173>
- [53] “UAS – UAV Activities in 3GPP Groups,” 3GPP Website, last retrieved Jan. 2020, <https://www.3gpp.org/uas-uav>
- [54] “Support for UAV Communications in 3GPP Cellular Standards,” Alliance for Telecommunication Industry Solutions (ATIS), ATIS-I-0000069, 2018, https://access.atis.org/apps/group_public/download.php/42855/ATIS-I-0000069.pdf
- [55] “Study on enhanced LTE Support for Aerial Vehicles [FS_LTE_Aerial],” 3GPP RP-171050, <https://portal.3gpp.org/ngppapp/CreateTdoc.aspx?mode=view&contributionUid=RP-171050>
- [56] “Enhanced LTE support for aerial vehicles,” 3GPP 36.777, v15.0.0, 2018, <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3231>
- [57] “New WID on Enhanced LTE Support for Aerial Vehicles,” 3GPP RP-172826, <https://portal.3gpp.org/ngppapp/CreateTdoc.aspx?mode=view&contributionUid=RP-172826>
- [58] “Study on NR to support non-terrestrial networks,” 3GPP 38.811, v15.2.0, 2019, <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3234>
- [59] “Study on Remote Identification of Unmanned Aerial Systems,” 3GPP 22.825, v16.0.0, 2019, <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3527>
- [60] “Enhancement for Unmanned Aerial vehicles”, 3GPP TR 22.829, v17.1.0, 2019, <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3557>
- [61] “Unmanned Aerial System (UAS) support in 3GPP”, 3GPP TS 22.125, <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3545>
- [62] “U-space Concept of Operations,” CORUS project D6.3, SESAR Joint Undertaking, 2019, <https://www.sesarju.eu/sites/default/files/documents/u-space/CORUS%20ConOps%20vol2.pdf>
- [63] “Summary; FIMS, Design and Architecture,” SESAR 2020 GOF USPACE, 2019, <https://www.sesarju.eu/sites/default/files/documents/projects/SESAR%202020%20GOF%20USPACE%20-%20Summary%20-%20Design%20And%20Architecture.pdf>

- [64] “G1128 – The Specification of e-Navigation Technical Services,” Version 1.1, International Association of Marine Aids to Navigation and Lighthouse Authorities, 2018, <https://www.iala-aism.org/product/g1128-specification-e-navigation-technical-services/>
- [65] “Internet of Things Deployment Map,” GSMA Website, last retrieved Jan. 2020, <https://www.gsma.com/iot/deployment-map/#labs>
- [66] “NB-IoT and LTE-M Deployment - Status and Roaming Possibilities?,” 1ot.mobi Website, last retrieved Jan. 2020, <https://1ot.mobi/resources/blog/nb-iot-and-lte-m-deployment-status-and-roaming-possibilities>
- [67] “Mobile IoT in the 5G Future - NB-IoT and LTE-M in the context of 5G,” GSMA whitepaper, 2018, <https://www.gsma.com/iot/wp-content/uploads/2018/05/GSMA-5G-Mobile-IoT.pdf>
- [68] 5G Infrastructure Public Private Partnership Website, last retrieved Jan. 2020, <https://5g-ppp.eu/>
- [69] “5G Pan-EU Trials Roadmap – Time Plan,” 5G PPP, version 4, https://5g-ppp.eu/wp-content/uploads/2018/11/5GInfraPPP_TrialsWG_Roadmap_Version4.0.pdf
- [70] OpenTAP Website, last retrieved Jan. 2020, <https://www.opentap.io>
- [71] Balazs Bertenvi, “Overall RAN timeline - 5G in Release 17 – strong radio evolution,” Dec. 2019, <https://www.3gpp.org/news-events/2098-5g-in-release-17-%E2%80%9393-strong-radio-evolution>
- [72] <https://openbaton.github.io/documentation/zabbix-plugin/>
- [73] “Telecommunication management; Management concept, architecture and requirements for mobile networks that include virtualized network functions,” 3GPP TS 28.500, ver. 15.0.0, 2018, <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2935>
- [74] “Management and orchestration; Architecture framework,” 3GPP TS 28.533, ver. 16.2.0, 2020, <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3416>
- [75] 3GPP, “Proximity-based services (ProSe); Stage 2,” 3GPP TS 23.303, ver. 15.1.0, 2018, <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=840>
- [76] 3GPP, “Study on system enhancement for Proximity based Services (ProSe) in the 5G System (5GS),” 3GPP TR 23.752, ver. 0.3.0, 2020, <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3624>
- [77] “Telecommunication management; Integration Reference Point (IRP) Concept and definitions,” 3GPP TS 32.150, v15.0.0, 2018, <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=1876>
- [78] D. Kim and M. Zarri, “Road to 5G: Introduction and Migration,” GSMA WP, 2018, https://www.gsma.com/futurenetworks/wp-content/uploads/2018/04/Road-to-5G-Introduction-and-Migration_FINAL.pdf
- [79] A-M Bosneag et al., “5GENESIS Overall Facility Design and Specifications,” 5GENESIS deliverable D2.2, 2018, https://5genesis.eu/wp-content/uploads/2019/12/5GENESIS_D2.2_v1.0.pdf
- [80] “Release description; Release 15,” 3GPP TR 21.915, ver. 15.0.0, 2019, <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3389>
- [81] “RAN Rel-16 progress and Rel-17 potential work areas,” 3GPP news events, 2019, <https://www.3gpp.org/news-events/2058-ran-rel-16-progress-and-rel-17-potential-work-areas>
- [82] The 5G-PPP ARIADNE project Home Page, Last retrieved Jan. 2020, <https://5g-ppp.eu/ariadne/>
- [83] A. Hudson, “Mobile Broadband: the Path to 5G,” GSMA Seminar, 2018, https://www.itu.int/dms_pub/itu-r/oth/0a/0E/R0A0E0000D40001PDEE.pdf
- [84] “IoT Security Guidelines for Network Operators,” GSMA CLP 14, ver. 2.1, 2019, <https://www.gsma.com/iot/wp-content/uploads/2019/10/CLP.14-v2.1.pdf>
- [85] “IoT Security Guidelines for IoT Service Ecosystem,” GSMA CLP 12, ver. 2.1, 2019, <https://www.gsma.com/iot/iot-security-guidelines-for-iot-service-ecosystem/>
- [86] “The Málaga Platform (Release B),” H2020 5GENESIS EU-funded project, Deliverable D4.5 v1.0, 2020, https://5genesis.eu/wp-content/uploads/2020/02/5GENESIS_D4.5_v1.0.pdf
- [87] “3GPP Low Power Wide Area Technologies,” GSMA WP, 2016, <https://www.gsma.com/iot/wp-content/uploads/2016/10/3GPP-Low-Power-Wide-Area-Technologies-GSMA-White-Paper.pdf>

- [88] “IoT in the 5G Era, Opportunities and Benefits for Enterprises and Consumers,” GSMA WP, 2019, <https://www.gsma.com/iot/wp-content/uploads/2019/11/201911-GSMA-IoT-Report-IoT-in-the-5G-Era.pdf>
- [89] “Summary of the 5G system enhancements scheduled in Release 17,” 3GPP, last retrieved Feb. 2020, <https://www.3gpp.org/release-17>
- [90] “SESAR Joint Undertaking,” Home Page, last retrieved Feb. 2020, <https://www.sesarju.eu/>
- [91] “Functional architecture and information flows to support Mission Critical Push To Talk (MCPTT); Stage 2,” 3GPP TS 23.379, ver. 14.7.0, 2018, <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3089>
- [92] “Functional architecture and information flows to support Mission Critical Video (MCVideo); Stage 2,” 3GPP TS 23.281, ver. 14.7.0, 2018, <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3087>
- [93] “Functional architecture and information flows to support Mission Critical Data (MCData); Stage 2,” 3GPP TS 23.282, ver. 14.6.0, 2018, <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3088>
- [94] “Common functional architecture to support mission critical services; Stage 2,” 3GPP TS 23.280, ver. 14.6.0, 2018, <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3086>
- [95] “Security of the mission critical service,” 3GPP TS 33.180, ver. 14.8.0, 2019, <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3127>
- [96] M. Kalinin et al., “Software defined security for vehicular ad hoc networks,” IEEE International Conference on Information and Communication Technology Convergence (ICTC), pp. 533-537, 2016.
- [97] S. Din, P. Anand and R. Rehman, “5G-enabled hierarchical architecture for software-defined intelligent transportation system,” Computer Networks, vol. 150, pp. 81-89, 2019.
- [98] M. Lacoste et al., “Software-Defined Vehicular Networking Security: Threats & Security Opportunities for 5G,” Computer & Electronics Security Applications Rendez-vous (C&ESAR), 2019.