Grant Agreement N°: 957317
Topic: ICT-42-2020
Type of action: IA

AFFORDABLE 5G

High-tech and affordable 5G network roll-out to every corner

D1.1: State of the art, technical system requirements analysis and pilot element descriptions

Revision: v.1.0

Work package	WP 1
Task	Task 1.1
Due date	30/11/2020
Submission date	30/11/2020
Deliverable lead	Ubiwhere
Version	1.0

Abstract

As first technical deliverable of Affordable 5G, this document focuses on three key topics to steer the developments of Affordable5G. The deliverable starts with an analysis of the state of the art, focusing on multiple aspects of Private 5G networks; the state of the art is followed by a detailed discussion on the three pilots (covering respective use cases and scenarios). Based on the pilot descriptions, the main system requirements were identified. These requirements that will act as guidance to steer the next project developments. Initially, as described in the project Description of Action, Affordable5G included only two pilots, a third one was added to ensure that technology advancements not covered by the original two pilots (namely non-public networks for Industry 4.0) were covered as well.

Keywords: Private5G networks, System requirements, Use cases, State of the art, Pilots

List of Contributors

Partner	Short name	Contributor(s)
ATOS SPAIN SA	ATOS	Josep Martrat Sergio González
ADVA Optical Networking Israel Ltd	ADVA	Andrew Sergeev
RETEVISION I SA	CEL	Raul Gonzalez Prats Luis Miguel Quintero
ACCELLERAN	ACC	Simon Pryor
ATHONET SRL	ATH	Daniele Munaretto Marco Centenaro Daniele Ronzani
THINK SILICON EREYNA KAI TECHNOLOGIA ANONYMI ETAIRIA	THI	Georgios Keramidas
RUNEL NGMT LTD	REL	Israel Koffman
NEMERGENT SOLUTIONS S.L.	NEM	Eneko Atxutegi, Marta Amor Egoitz Alonso
UBIWHERE LDA	UBI	Luís Conceição João Peixoto (lead editor)
MARTEL GMBH	MAR	Federico M. Facca Gabriele Cerfoglio
INCITES CONSULTING SARL	INC	Ioannis Neokosmidis
EIGHT BELLS LTD	8BELLS	George Kontopoulos
NEARBY COMPUTING SL	NBC	Josep Marti Oscar Trullols
UNIVERSIDAD DE MALAGA	UMA	Pedro Merino Francisco Luque-Schempp Iván González
ETHNIKO KAI KAPODISTRIAKO PANEPISTIMIO ATHINON	NKUA	Panagiotis Trakadas, Anastasios Giannopoulos, Sotirios Spantideas
FUNDACIO PRIVADA I2CAT, INTERNET I INNOVACIO DIGITAL A CATALUNYA	I2CAT	Estefanía Coronado Giovanni Rigazzi
EURECOM	EUR	Navid Nikaein

Document Revision History

Version	Date	Description of change	List of contributor(s)
V0.1	22/09/2020	ToC	UBI, NKUA
V0.2	26/10/2020	Pilot 1, 2 and 3 - requirements and use cases System requirements section	8BELLS, NBC, NEM, NKUA, UBI, UMA
V0.3	05/11/2020	Section 1	ATOS
V0.4	11/11/2020	Improvements in section 1, 2 and 3	ALL
V0.5	13/11/2020	Update and revision of section 1.3	8BELLS, ATOS
V0.6	13/11/2020	First version for review	ALL
V0.7	23/11/2000	Second version for review	ALL
V0.8	25/11/2020	*First review*	*I2CAT (Estefanía Coronado), NKUA (Panagiotis Trakadas), THI (Georgios Keramidas)*
V0.9	26/11/2020	Integration of all suggestions	UBI
V0.10	27/11/2020	Update in section 1 and pilot 1	NEM, NKUA
V0.11	27/11/2020	*Second review*	*MAR (Federico Facca)*
V0.12	30/11/2020	Integration of last reviews	NEM, NKUA, UBI
V1.0	30/11/2020	QA and Final version	ATOS, UBI

Disclaimer

The information, documentation and figures available in this deliverable, is written by the Affordable5G (High-tech and affordable 5G network roll-out to every corner) – project consortium under EC grant agreement 957317 and does not necessarily reflect the views of the European Commission. The European Commission is not liable for any use that may be made of the information contained herein.

Project co-funded by the European Commission in the H2020 Programme		
Nature of the deliverable:		R
Dissemination Level		
PU	Public, fully open, e.g. web	√
CI	Classified, information as referred to in Commission Decision 2001/844/EC	
CO	Confidential to Affordable5G project and Commission Services	

EXECUTIVE SUMMARY

The deliverable “D1.1: State of the art, technical system requirements analysis and pilot element descriptions” reports the achievements of “Task 1.1: Pilots description and Technical requirements”.

The main objective of this document is the definition of the system requirements for Affordable5G project that will guide the design of the system architecture and the later implementation in the technical WPs. These system requirements should align with the Affordable5G vision that aims at optimising hardware usage and open software platforms for 5G network elements.

The Affordable5G system should be able to cope with requirements of pervasive private and enterprise networks in the three pilots, namely: (i) emergency communications, (ii) dense smart city and (iii) industry/manufacturing. To ensure that these requirements are well captured, this deliverable describes and analyses in detail the three pilots and their respective use cases and scenarios. It is relevant to note that only the first two pilots were originally defined in the DoA (Description of Action) but the Affordable5G consortium decided at the early stage of the project that it would be interesting to elaborate an additional third pilot in the area of manufacturing vertical industry.

Accordingly, this deliverable contributes to realise the Affordable5G project vision by:

- Exploring the contributions of Affordable5G on Private5G networks topic, and identifying possible business opportunities in this area, mainly driven by the industrial partners of the project;
- Defining pilot scenarios that describe the required functionalities related to the management and orchestration of the access, edge and core part segments of private and enterprise networks;
- Identifying and charactering the system requirements that allows the selection of the network elements and the 3GPP, ETSI and O-RAN specifications that need to be taken as a reference in the Affordable5G system architecture.

The collection of system requirements (functional and non-functional), aligned with the Affordable5G vision and the characteristics of the three pilots, will be used as input to the specifications of the Affordable5G system architecture in the Task 1.2.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ABBREVIATIONS

3GPP	3rd Generation Partnership Project
5GC	5G Core SBA based sub-system (evolution of the 4G EPC)
5GS	5G System
AR	Augmented Reality
CAGR	Compound Annual Growth Rate
CAPEX	Capital Expenditures
CESC	Cloud Enabled Small Cells
CN	Core Network
COTS	Commercial Off-The-Shelf
CP	Control Plane
CU	Centralised Unit
CUPS	Control and User Plane Separation
C-RAN	Centralised RAN
DA-RAN	Dis-Aggregated RAN
DN	Data Network (Termination of 5G User-plane after UPF in 5GC or NG-RAN)
DU	Distributed Unit
E2E	End-to-End
eMBB	Enhanced Mobile Broadband
EPC	Evolved Packet Core
GSA	Global mobile Suppliers Association
IIoT	Industrial IoT
IoT	Internet of Things
KPI	Key Performance Indicator
LAN	Local Area Network
LTE	Long Term Evolution (4G Network and LTE radio which is used in 5G)
MANO	Management and Orchestration
MCData	Mission Critical Data
MCPTT	Mission Critical Push To Talk
MCS	Mission Critical Services
MCVideo	Mission Critical Video
MEC	Multi-Access Edge Computing
mMTC	Massive Machine-Type Communications
MNO	Mobile Network Operator
MR	Mixed Reality

MVNO	Mobile Virtual Network Operator
NFV	Network Function Virtualisation
NFVI	Network Functions Virtualisation Infrastructure
NG-RAN	5G New-Radio RAN (supporting 5G-NR and possible LTE)
NPN	Non-Public Network
OAI	OpenAirInterface
OPEX	Operational Expenditures
OSM	Open Source MANO
OTT	Over-The-Top
O-RAN	Open RAN
PDCP	Packet Data Convergence Protocol
PNI-NPN	Private Network Integrated NPN
PPP	Public Private Partnership
QoS	Quality of Service
QPP	Quality of service, Priority and Pre-emption
RAN	Radio Access Network
RIC	RAN Intelligent Controller
ROI	Return Of Investment
RU	Remote Unit
SA	Stand-Alone
SBA	Service Based Architecture
SC	Small Cell
SCaaS	Small Cell as-a-Service
SDK	Service Development Kit
SLA	Service Level Agreement
SLP	Smart Lamp Post
SMO	Service Management and Orchestration
SNPN	Stand-Alone Non-Public Network (synonymous with ‘Private 5G’ network)
TSN	Time Sensitive Networking
UP	Urban Platform
UPF	User Plane Functions
URLLC	Ultra-Reliable Low-Latency
VR	Virtual Reality
WAN	Wide Area Network

1 INTRODUCTION

1.1 Affordable5G Vision for Private5G Networks

5G is becoming a reality and Mobile Network Operators (MNO) are starting to commercialise their 5G network deployments, expecting to drive a set of new ground-breaking services around the 5G ecosystem. 5G networks are designed around new pervasive concepts, such as Network Function Virtualisation and Software Define Network, that embodied the whole telco infrastructure. Thus, as such 5G networks are not only evolving 3G and 4G standards at network access level, but, thanks to the adoption of a service-based architecture, they introduce a whole new set of dynamic and modular capacities in the whole communication infrastructure (from the core to the access network), making the integration between transport and access network capacities and service delivery capacities more automated, flexible, modular, scalable and interoperable.

This shift, in contrast to 5G System (5GS) predecessors, whose architectural paradigms were mainly targeting either human-to-human or human-to-IT communications, allows for a much broader range of communications patterns that attracts applications and services from various vertical domains, such as industrial automation [1], [2], mission critical services [3], smart city and transportation [4] and secure services [5]. This wide ensemble of innovative services can be realised today thanks to 5G and its unique technical features, including modularity, programmability and flexibility that are based on novel technologies, like neutral hosting, spectrum sharing, network slicing, etc., as foreseen and specified in the latest 3GPP release documents [6], [7]. All these services will be settled on the plethora of new cutting-edge innovations offered by 5G networks, in the areas of Enhanced Mobile Broadband (eMBB), Ultra-Reliable Low-Latency (URLLC) and Massive Machine-Type Communications (mMTC). Nonetheless, while the vast majority of 5G deployments are targeting public outdoor networks, the 5G capabilities bring new business opportunities also to dedicated private (either outdoors or indoors) network that, until now, are facing several challenges:

- Mission critical services are still serving only narrowband applications, although there is a clear need for broadband and zero-latency services that has not been covered by current technologies (TETRA, P25, WIMAX);
- Agriculture and Factory logistics are seeking for productivity gains through the support of process automation, enhanced mobility and location services, and new paradigms for seamless enterprise connectivity leveraging Machine-to-Machine or Device-to-Device communication patterns;
- Manufacturing processes, under the umbrella of industry 4.0 concept, are demanding automation and real-time decisions, supporting ultra-dense networks of M2M devices as well as data-heavy applications;
- Protection of critical assets and enhanced data security measures becomes a necessity under the new era of cybersecurity, where multi-tenancy and resource sharing must be supported.

Consequently, many enterprises are interested in the deployment of their own private 5G networks, especially the companies focused on industrial manufacturing, critical communications and Internet of Things (IoT) scenarios, that which will be particularly benefited from eMBB, URLLC and mMTC services, as foreseen in the 5G ecosystem. **A private 5G network is a particular realization of the 5G system designed and configured for a private use by an enterprise or an exclusive group of users. It can be deployed to cover the needs of a specific application, or multiple applications or even a vertical domain**.

1.1.1 Why 5G private networks are key for innovation of private internet services

The advantages arising from the deployments of such private 5G networks (or Non-Public Networks, as defined in the 3rd Generation Partnership Project (3GPP) [8] are numerous, spanning across several dimensions:

1. Unlike a public network, ***a private 5G network can be configured according to the specific needs of the enterprise***. These needs may impose different characteristics either based on geographic locations or specific needs per enterprise site. For example, depending on the type of work that is conducted in one site/location of the enterprise, the system might be able of supporting a slice addressing mMTC requirements, while in another enterprise site, the business needs might require spectrum sharing among public and private 5G spectrum in several bands to cover eMBB services.
2. ***A private network might be instantiated for a special purpose and for a particular time interval and coverage quality***. This is a reality for mission critical services, where spontaneous networks must be deployed in a short period of time to cover needs of a geographic area. Such a network must be deployed and maintained by onsite personnel, enabling fast responses to physical disasters or sudden events.
3. Cybersecurity and cyber-resilience guarantees are much higher than ever before in public networks due to the wide spread of threats and attacks across all types of public networks and services hosted within. ***A private 5G network provides the privilege to an enterprise to share only the subset of data that cannot reveal security holes of the system or corporate secrets and also give the freedom to the company to decide on the granularity of external access to company data and thus safeguard privacy preservation***.
4. ***A private network allows enterprises to have a Service Level Agreement (SLA) tailored to their needs***, including the resources to be allocated under normal conditions and how the system will react in adverse conditions (options of the SLA related to scale in/out, scale up/down, migration of functions to the edge, spectrum sharing, etc.). In this respect, a private network may offer complete control to the enterprise and cater for specific implementations that would be really costly in a public network. An interesting example could be the provisioning of deterministic Time Sensitive Networking (TSN) characteristics to fulfil the requirements of an enterprise. Taking advantage of the flexibility and deployment options foreseen in the 5G Radio Access Network (RAN) and the Core Network (CN) parts of the network, such implementations can be supported without exceeding too much the associated costs for an enterprise.

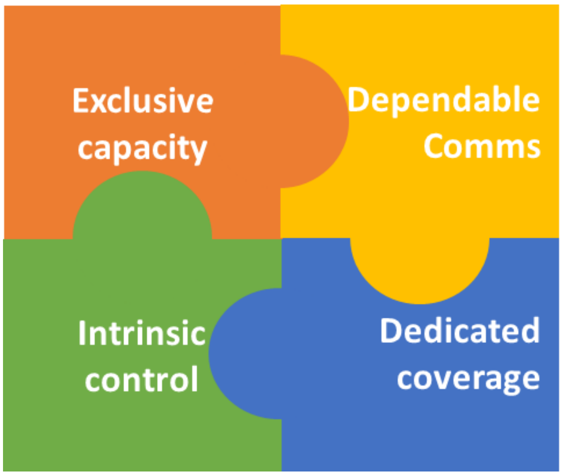

Figure 1: Advantages of Private 5G Networks

1.1.2 Overcoming today limitations of 5G private networks

However, in most of the cases, while showing great benefits, the deployment of a 5G network is still costly compared to other established technologies in this type of environments, such as Wi-Fi (including IEEE 802.11ax, also known as WIFI-6), Private LTE or specific technologies like TETRA, WirelessHART, MODBUS, etc. For these reasons, the Affordable5G project envisions an end-to-end affordable 5G system targeted to private and enterprise networks, aiming to reduce the required (CAPEX and OPEX) investments, while still offering the benefits of 5G to private companies.

In the first place, ***Affordable5G envisages a cost-efficient 5G solution by means of the Network Function Virtualisation (NFV) paradigm***. NFV allows to the decoupling of the network functions from dedicated and proprietary hardware, enabling their execution in Commercial Off-The-Shelf (COTS) equipment [9]. The 5G system has evolved towards a service-based architecture, fully adopting the NFV paradigm in order to increase the flexibility while reducing the network deployment cost. Current mobile network architectures present a clear split of functionalities, separating the network in two segments, the **Radio Access Network (RAN)** and the **Core Network (CN**) with both segments supporting different degrees of Virtualisation, enabling different 5G deployment considerations.

Previous RAN architectures were based on monolithic designs, according to which all the protocol stack was integrated in local nodes, thus limiting the flexibility of the radio segment needed in 5G networks. Recent RAN designs are focusing on increasing the flexibility and expanding the network capacity while remaining profitable with low capital expenditures (CAPEX) and operational expenditures (OPEX), and following this trend, 3GPP introduced the **RAN functional splitting** in Release 15 [6]. The concept of functional splitting is based on the detachment of the protocol stack functions in separated units, allowing higher degrees of centralization and thus, reducing the deployment cost. Also commonly known as Centralised RAN (C-RAN), this concept is aligned with the Virtualisation trend, enabling the execution of some of these functions in virtualised environments. Currently there are eight different functional split options that can be distributed in three different units, i) the Remote Unit (RU), containing the antennas, the radio frequency front end and even the lower part of the PHY layer; ii) the Distributed Unit (DU), including the upper PHY, MAC and RLC layers and iii) the Centralised Unit (CU) including Packet Data Convergence Protocol (PDCP) and the layer 3 interfaces. However, the independent deployment of the CU requires a dedicated optical fibre connection to the DU through the F1 interface, with stringent latency and throughput requirements. Alternatively, the CU and DU can be collocated, resulting in a relaxation of the network requirements and endorse a more affordable RAN deployment.

Nevertheless, the vast majority of C-RAN implementations rely on vendor specific technologies and do not support interoperability, suffering from vendor lock-in. Hence, this fact is limiting the use of these novel RAN technologies in deployments since specialised equipment is usually associated with a reasonably higher cost. However, new communities such as the O-RAN Alliance [10] are aiming to drastically change the landscape by defining **open interfaces** between the RAN units, allowing to consolidate its usage and its interoperability with other open platforms.

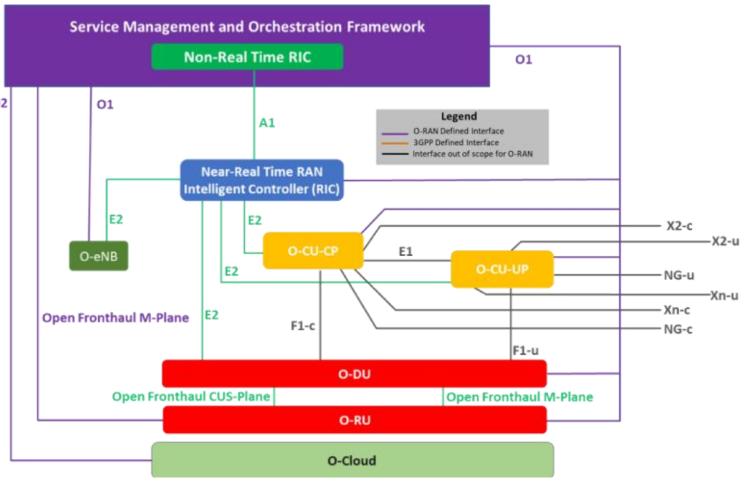

Figure 2: O-RAN overall logical architecture

This open ecosystem also introduces new potential vendors that will be able to develop affordable and interoperable hardware and software solutions for the radio access segment. The usage of **open platforms** will not only be in the RAN. To complement Open Source RANs, Affordable5G vision fosters the adoption of open **edge computing platforms** like Akraino [11] and KubeEdge [12], virtualised 5GCore solutions and the integration with widely used **open management and orchestration frameworks**, like Open Source MANO [13]. With such technological landscape in mind, the Affordable5G project aims to consolidate the adoption and interoperability of open source solutions for all the different network segments, providing a cost-efficient heterogeneous 5G system architecture.

Traditional network deployments, in which each network operator deploys its own infrastructure, lacks of practicality and cost efficiency in ultra-dense scenarios, where a big number of radio elements should be deployed, posing several issues due to the lack of space that limits the number of radio antennas. For these reasons, 5G network deployment should drastically change the deployment strategy. Affordable5G aims to overcome these limitations and significantly reduce the CAPEX and OPEX by means of **enhanced sharing strategies** [14] between different actors, maximizing the infrastructure usage and interoperability of open-source platforms running in COTS equipment. This cost-saving approach will help to maximise the Return On Investment (ROI) through neutral hosting and network slicing. The Afforable5G project will enhance the current slicing techniques, exploring new isolation and resource optimization mechanisms at different network levels, including the RAN and Multi-Access Edge computing (MEC) infrastructures in order to define enforceable Service Level Agreements (SLAs). The advantages offered by **network slicing techniques** will allow to run isolated end-to-end services with different requirements on top of the same physical infrastructure, creating new business opportunities for virtual providers. Similarly, the **neutral hosting model** allows the deployment of small cells as a permanent physical infrastructure in certain scenarios that requires 5G RAN densification, such as stadiums, shopping malls or industries, opening the access to third parties, sharing and leasing out network slices, and allowing to increase the network coverage and performance.

Altogether, Affordable5G aims to deliver a cost-effective and complete end-to-end 5G network architecture specifically tailored for private companies and enterprises that would cover the requirements stemming from the enterprise and private companies ecosystem, as shown in Figure 3. This cost-effectiveness, and hence affordability, will be achieved by means of using virtualised deployments in COTS hardware focused on open solutions and open-source MANO frameworks, such as O-RAN and OSM respectively, simplifying and automatizing the deployment and operation while, at the same time, enhancing the interoperability in the whole network through open interfaces. Furthermore, Affordable5G will also help to reduce the cost by using novel sharing techniques based on network slicing and neutral host enabling technologies. The Affordable5G vision opens a set of new opportunities and business models to new software and hardware vendors and SMEs, moving away from the traditional costly and vendor-locked specialised equipment and network deployments.

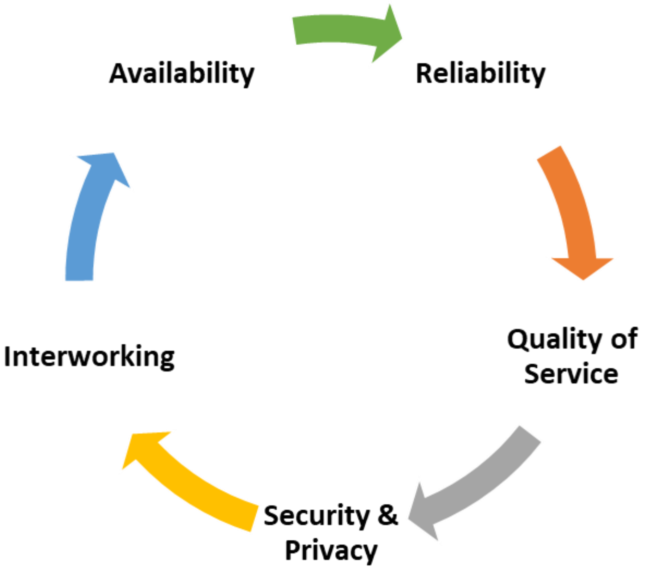

Figure 3: Private 5G Networks Requirements

1.2 Different deployment options for Private 5G Networks

The flexibility provided by the functional split, the network softwarization paradigm (based on NFV and SDN concepts) and the novel C-RAN designs, enable tailored private network deployments for different use cases with diverse network requirements. These paradigms fostered the creation of the 5G system architecture as a service-based evolution of the actual 4G architecture, clearly differentiating three network parts:

- The Radio Access Network (RAN) is in charge of the radio-related functions, including the modulation and coding scheme and the physical resource scheduling. In this segment, the design of C-RAN decomposes the radio access functionalities in different functional splits for RUs/CUs/DUs, thus increasing the flexibility of cell deployments.
- The Core Network (CN) is in charge of the non-radio related functions, including the user authentication, charging, mobility management and gateway connectivity. The CN

can be decomposed into two different functional blocks, namely the Control Plane Function (CPF) and the User Plane Function (UPF). The CPF manages authentication, mobility charging and policing, while the UPF is responsible for data forwarding, gateway connectivity and mobility anchoring.

- The **Management and Orchestration** (MANO) part of the 5GS controls network function, service and user management functions (including the configuration, deployment and lifecycle management of network functions and services), network slicing and service performance monitoring and billing.

As mentioned earlier, Private 5G networks are envisioned for the exclusive use by a private entity or by a closed group of users. Notwithstanding, these Private 5G networks can serve one or multiple industrial sites, such as a campus or a factory, segmenting the facility on different premises (e.g., different departments, production lines, etc.). **Private networks deployed in multi-site scenarios can support different levels of centralization, allowing to centralise control and user plane functions while only distributing the radio access sections over the different sites**.

1.2.1 Deployment options based on centralization of 5GS network segments

In this section we analyse the different deployment options for Private 5G networks based on the degree of centralization of the different sections of the 5GS architecture.

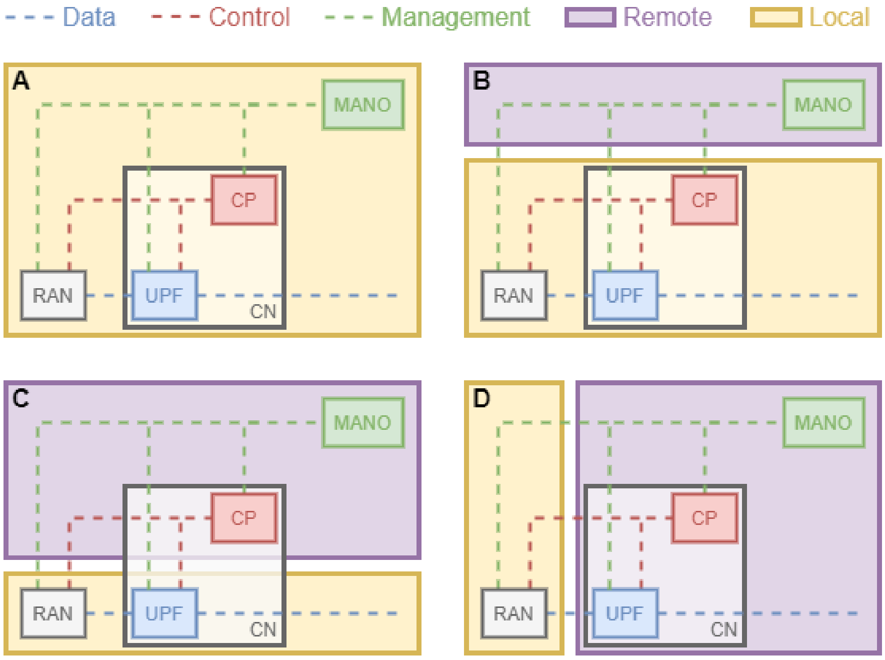

Figure 4: Private 5G Network Deployment options

The first deployment option, depicted as model A in Figure 4, is the ***local deployment***, in which all the functional blocks are deployed locally on the private network premises. This deployment option stands out for its high security enforcement and robustness, since all the network elements are isolated and located under the premise perimeter. This approach is interesting for industries or companies with strict security regulations. The facilities can be segmented into different security zones with independent local 5G private networks in order to better protect and minimise the probability of unauthorised access to their data. However, such a deployment assumes that the geographic area to be covered is restricted and enterprises with several sites on different, dispersed geographic locations can hardly be covered by such a deployment. By contrast, this deployment option can offer the best performance in terms of latency and throughput for latency-sensitive applications as all the functional blocks, and specially the UPF and CPF, are collocated in the private network premises. On the contrary, this option offers less flexibility and deployment cost efficiency since it is the less centralised solution of the four requiring the deployment of independent RAN, CN and MANO elements in each facility.

The second deployment consideration, depicted as model B in Figure 4, increases the centralization degree, maintaining the RAN, UPF and CPF functions in the local facilities but placing the MANO functions in a remote location. This option allows the centralization of the MANO functions for different local premises, which is especially useful for multi-site scenarios. This solution offers better cost efficiency and flexibility but lower security than the previous one, and still provides good performance for latency-sensitive applications since the UPF and CPF are still deployed locally. From an operational viewpoint, this deployment option assumes that the enterprise provides remote management and orchestration capabilities, possibly to another entity, e.g., service provider, and can be considered as a special case of Service-as-a-Service (SaaS) provisioning.

The third deployment scenario places the CPF and the MANO functions on a remote site and maintains the user plane and radio access function on the local premise, as it can be shown as model C in Figure 4. The local instantiation of the control plane is not critical for low-latency scenarios, since all the data traffic is carried by the user plane functions that are still placed locally. It also increases the flexibility while reducing the deployment cost but, on the contrary, this deployment option hinders the enforcement and control of stringent security regulations due to the higher degree of decentralization.

Finally, the last deployment option, which is depicted as model D in Figure 4 centralises the MANO, control and user planes and only distributes the RAN section. This solution clearly simplifies the deployment, operation and management of the network and offers the lowest deployment cost of the four options described herein, since it is the most centralised option. The centralization of network functions over multiple private networks reduces the robustness and can also negatively affect the network performance, since the UPF is located farther from the UEs.

As noted from the previous analysis, the key message is that the functions centralization in 5G private networks deployments clearly increases the flexibility and reduces the cost, while the function distribution enhances the robustness and security while offering a better performance.

1.2.2 Deployment options based on 5G Public - Private networking interactions

As a second categorization in our analysis, Private 5G networks can be deployed as Stand-alone Non-Public Network (SNPN) or they can interact and be deployed in conjunction with Public 5G networks (PNI-NPN), in order to share the network infrastructure, increase the network coverage or delegate the management of some network segments to network operators and thus reduce associated costs. However, the integration with Public 5G networks highly depends on many factors such as the level of trust, the infrastructure ownership or the frequency spectrum utilised and shared.

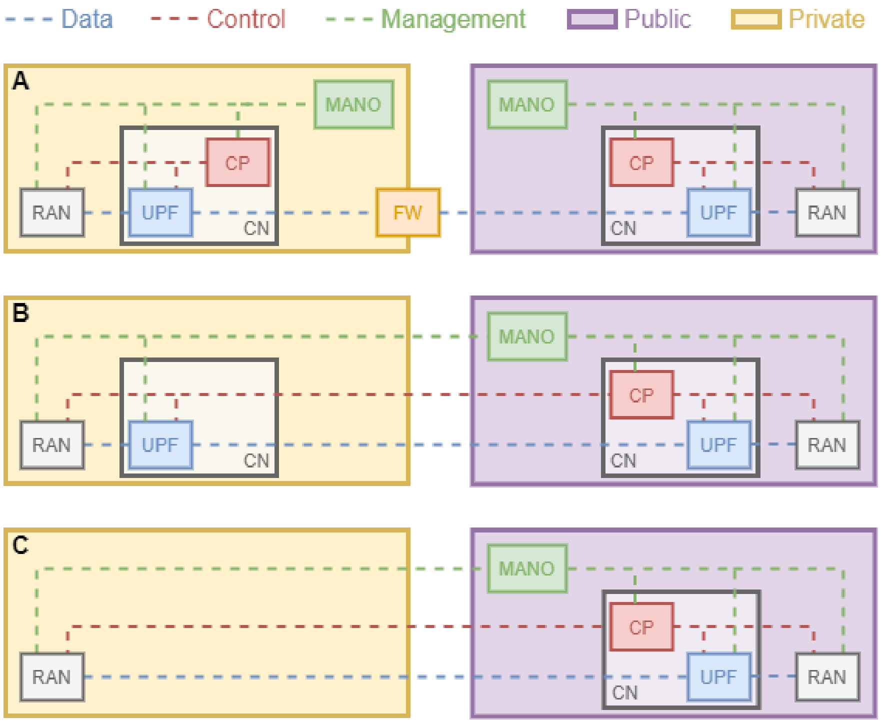

Figure 5: Integration of private and public mobile networks

When Private 5G networks are deployed as standalone independent networks, as it is depicted as model A in Figure 5, all the network segments are located within the company premises, being fully operated by the company owner. In this case, the interaction with public networks should be done through a firewall to enable access to public network services under the private network coverage, taking into consideration that this interaction is subject to roaming agreements with public network operators.

Other private networks deployment options consider a higher integration with public networks, sharing the RAN and being partially or totally hosted by public network operators, such as model B and model C in Figure 5, maintaining always the Private 5G network services accommodated and instantiated on the private network premises. The management and operation of a mobile network is not a trivial task and operators have broader expertise than infrastructure owners in this field; for that reason, the public network (partial or total) hosting highly simplifies the management of the network for the private network owner, but at the same time, it can also pose some security and performance issues for companies with strict security regulations or stringent latency and throughput requirements. If the CP is hosted by the public operator (model B in Figure 5), the network subscription will be managed outside the premises, while if by contrast the UPF is the component hosted by the public network (model C in Figure 5), the data traffic will be forwarded through the public network infrastructure, without physical resource isolation, and sharing the network with the public subscribers that may impact the private network traffic.

As it is shown in this section, **there are several options for 5G private networks deployments, offering diverse benefits depending on the desired level of isolation, performance characteristics, associated costs, timeliness of deployment, privacy dependencies and level of public network integration. In any case, there is a clear trade-off between performance, security and flexibility that must be carefully analysed in order to choose the right deployment model. In conclusion, it is evident that there is not one-size-fits-all solution to address the stringent and conflicting requirements of Private 5G networks**.

1.3 State of the art in 5G-PPP ecosystem

Europe has been at the forefront of 5G research under the umbrella of Horizon 2020 projects. The technology and scientific solutions developed during these 5G PPP projects have contributed to the development of 5G standardization activities that defined the deployments we are seeing nowadays. Some of the projects under the 5G PPP scope already targeted 5G private networks as their main research topic. For this reason, this section analyses the present and past 5G PPP projects focused on private 5G networks, detailing the added value and differentiation offered by Affordable5G compared to the state of the art.

During 5G PPP Phase 2 four projects have initially investigated the most relevant aspects and requirements of the deployment of 5G private networks, namely 5GCity, 5G-ESSENCE, 5G-MoNArch and 5G-PICTURE.

5GCity is the Phase 2 project that has mainly targeted the private deployment of 5G networks [15]. This project started in June 2017 and focused on a hot topic also investigated in Affordable5G, namely the neutral hosting concept. Through neutral hosting some intermediaries, like municipalities, deploy their own 5G infrastructure and, by leveraging a virtualised platform, they are able to share and lease the infrastructure by means of the network slicing concept to third-party operators and verticals. 5GCity, as well as Affordable5G, digs into the edge computing paradigm benefiting from the closeness to the data sources for faster response time in latency-sensitive services and local data access for privacy considerations.

The 5G City architecture was designed following a three-tier model, dividing the infrastructure into i) far edge, where small cell and micro computing elements are deployed, ii) edge, that includes street cabinets with higher computing capabilities and iii) central/core where big data centres are placed with huge computing capabilities, integrating these three layers into a heterogeneous neutral hosting platform. At the end, 5GCity aimed to create a common platform at the far edge of the network, turning municipalities into distributed edge infrastructures, integrating computing, network and storage resources near to the small cells in several technical locations, such as: lamp posts, street cabinets, urban furniture and traditional big datacentres. The 5GCity project also developed a Service Development Kit (SDK) to open the proposed neutral hosting infrastructure to third-party vertical industries. This SDK abstracts the infrastructure capabilities and provides several tools, templates, and a software platform, to simplify the service planning, design and deployment in the neutral hosting infrastructure.

The 5GCity project was validated in three different pilots located in Barcelona, Bristol and Lucca, finalizing on spring 2020.

5G ESSENCE [16] started in June 2017, and that focused on the Small Cell (SC) market, enabling a multi-tenant neutral host model. The project aimed at providing Small Cell coverage to multiple operators building on the “as-a-Service” paradigm. The project envisioned a two-tier architecture: a first distributed tier for providing low latency services and a second centralised tier for providing high processing power for compute-intensive network applications. By means of end-to-end (E2E) network slicing mechanisms the infrastructure was shared among multiple operators/vertical industries, where the capabilities of the slices were customised on a per-tenant basis. By using the proposed solution, multiple network operators (tenants) can provide services to their users through a set of Cloud Enabled Small Cells (CESCs) deployed, owned, and managed by a third party (i.e., the CESC provider). This Small Cell as-a-Service (SCaaS) approach can be more efficient in highly dense scenarios than solutions based on independent deployments on a per-operator basis. With a total duration of 30 months, the 5G ESSENCE project already finished at the end of 2019.

5G-MoNArch [17] started on July 2017, and that although it has not directly focused on private networks, it has developed a comprehensive network slicing framework. Leveraging the flexibility of this framework allows integrating functions required for industrial, media & entertainment, and smart city use cases.

The 5G-MoNArch common mobile network architecture provides full E2E network slicing support by integrating slice-specific and slice-common functions, multi-tenancy capable management and orchestration, inter-slice resource management, and optional integration of RAN control applications. The project framework has been evaluated in testbeds with real vertical stakeholders (e.g., the Hamburg Port Authority), addressing the main technical architecture concepts such as network slicing, network orchestration, resilience, reliability, security and elasticity. The 5G-MoNArcht project lasted 24 months, finalizing in July 2019.

5G-PICTURE [18] focused on supporting multi-tenancy on the access and transport networks through the development of a converged fronthaul and backhaul infrastructure, integrating advanced wireless and novel optical and packet network solutions. The project has exploited the concept of flexible functional splits that can be dynamically selected to optimise resource and energy efficiency. This results in a paradigm shift from RAN and C-RAN to “Dis-Aggregated RAN” (DA-RAN).

Under the DA-RAN concept, hardware and software components are disaggregated across the wireless, optical and compute/storage domains. Resource disaggregation allows decoupling these components, creating a common “pool of resources” that can be independently selected and allocated on demand to compose any infrastructure service. The project aims at providing a stakeholder/service-driven approach towards optimal infrastructure resource utilization for the traditionally established Telecom Operators. Verticals can also be empowered towards deploying and operating smaller scale 5G infrastructures for their specific telecommunication needs. 5G-PICTURE had a duration of 36 months, finalizing in June 2020.

Nonetheless, the concept of 5G private networks have been more investigated in the 5G PPP phase 3 projects, by means of the projects included in ICT-19 call such as 5G-SMART and 5Growth, which started in June 2019.

First, **5G-SMART** [19] focuses on the industrial ecosystem, demonstrating and validating the potential use of 5G in smart factories. The project analyses the co-existence of private and public 5G networks in the industry and manufacturing environment, investigating the business roles and models of the introduction of 5G connectivity in industrial scenarios, in three use cases: i) time critical processes, ii) non-time critical in-factory communications in dense scenarios, and iii) remote operation of devices.

Thus, 5G-SMART project tackles first the integration of industrial LAN features, such as TSN into the 5G ecosystem for URLLC services, including slicing mechanisms for the simultaneous support of several TSN streams with diverse Quality of Service (QoS) requirements. The project also aims to test different spectrum bands and the coexistence between indoor and outdoor 5G networks. A key research topic also investigated in 5G-SMART is the utilization of cloud and edge infrastructure for sensor and context-information data processing, enabling the cloud-based control, real time monitoring and digital twining of the manufacturing robotic equipment. 5G-SMART is an ongoing project expecting to finish in December 2021.

Then, **5Growth** [20] targets the technical and business validation of 5G technologies from the point of view of a vertical industry, following a field-trial-based approach on vertical sites. 5Growth focuses on the development of a vertical service platform that allows the provision of 5G connectivity and services to vertical industries directly in the industry premises. The 5Growth platform enables automated hierarchical multi-domain service orchestration with seamless integration with other existing platforms. This integration will be demonstrated in the trials, in which 5Growth aims at demonstrating the selected vertical use cases in conjunction with ICT-17 platforms, envisioning the 5Growth platform as a private network deployment on the vertical industry premises interacting with such ICT-17 platforms [21] (**5G-EVE** and **5G-**

VINNI) deployed as public networks, thus investigating the interoperability and integration of public and private networks. 5Growth is an ongoing project that is expected to finish in December 2021.

Continuing with the ICT-20 call, the **5G-Clarity** project [22], which started in November 2019, is investigating a beyond 5G architecture that integrates L2 SDN network with different radio access technologies such as Wi-Fi, 5G and LiFi for private networks. In addition to the enhanced spectrum flexibility provided by the multiple radio access technologies, this project also explores novel management techniques based on AI for network automation for the radio, transport and compute resources, following the O-RAN reference architecture and interfaces and adopting the user and control plane separation defined in 3GPP. The 5G-Clarity infrastructure will be demonstrated in two different pilots, the first one in the 5GUK facilities in the university of Bristol and the second in a BOSCH factory in Barcelona, focusing on an Industry 4.0 use case. 5G-Clarity is an ongoing project that is expected to finalise in spring 2022.

Within the same ICT-20 call, **5GZORRO** [23], which started in November 2019, aims to go beyond traditional bilateral B2B business models for operators (e.g., Telco with TowerCo, MNO with MVNO), towards a multi-party distributed model to unleash new network business. The vision of the project is to enable cross-operator/cross-domain service chains, with security and trust among parties (telecom operators – verticals/slice owners – spectrum-only owners – passive and active edge facility owners – wholesale fibre owners, etc.). To facilitate the establishment of multi-party agreements on top of 3rd party resources, the project will produce a conceptual architecture for AI-driven zero-touch operations, security and trust in multi-operator 5G networks. The platform instantiated in each operator domain will enable the sharing of heterogeneous types of resources (i.e., spectrum, virtualised radio access, virtualised edge/core, software defined WAN, etc.) across multiple operators and infrastructure / resource providers. 5GZORRO is still ongoing, and it is expected to finish at the same time as 5G-Clarity, in spring 2022.

Finally, within the same call as Affordable5G (ICT-42), starting in September 2020, Fudge-5G [24] and 5G-Records [25] also address the topic of private 5G networks.

The **Fudge5G** [24] project aims to create a disintegrated environment, based on virtualisation technologies, where the mobile network components can be deployed in edge and cloud environments running as micro-services in commodity hardware. The Fudge5G project aims to feature 5GLAN (Local Area Network) based on Ethernet, 5G-TSN, 5G-Multicast and intelligent orchestration mechanisms in its architecture. The Fudge5G project is defining five different vertical use cases that will be validated in the ICT-17 platform of 5G-VINNI. These use cases investigate the media distribution using 5G-Multicast, Mission Critical Services (MCS) for public protection, corporate 5G networks, Industry 4.0 with TSN in a naval factory and the interoperability of Wi-Fi and 5G across academic institutions. The Fudge5G project started at the same time as Affordable5G, running in parallel, but with a longer duration it is expecting to finish at the beginning of 2022.

5G-RECORDS [25] aims at investigating the applicability of 5G private networks for professional audio-visual content production environments. The project aims to integrate local 5G network infrastructures, including the 5GCore, the RAN and the end devices with media creation workflows, including audio-visual infrastructure backbones. The 5G-RECORDS solution will also address the integration of private and public 5G networks and will be based on 3GPP Release 15 and 16. The use cases envisioned in the 5G-RECORDS project are focused on i) live audio production using 5G microphones with low latency requirements, ii) multiple cameras connected wirelessly through 5G in a video production studio, and iii) live immersive real-time media transmission using Free-Viewpoint Video (FTV). 5G-RECORDS started at the same time than Affordable5G, and with the same duration, it is also expected to finish simultaneously, running completely in parallel.

As can be seen from the above analysis, **different 5G PPP projects already targeted the utilization of 5G private networks under their research scope, investigating as well different sharing strategies for cost reduction. However, the utilization of open interfaces in the radio access network was not deeply investigated. Standard RAN equipment relies on vendor specific technologies, suffering from vendor lock-in and hence, having a limited interoperability with other vendor's hardware and software. Such closed ecosystem restricts the utilization of novel RAN technologies in affordable private deployments since specialised equipment is usually very costly. For that reason, Affordable5G aims to investigate the inclusion and interoperability of open platforms for the radio access, such as O-RAN, which defines open interfaces between the RAN components. The Affordable5G architecture also aims to incorporate other open-source solutions in the rest of the mobile network segments (OpenAirInterface, FlexRAN, Kubernetes, Akraino) in addition to advanced sharing strategies, creating an open 5G architecture that attempts to drastically reduce the required investment for private network deployments. The project will also investigate the integration of TSN mechanisms into 5G networks, enabling its utilization in industrial environments with tight latency requirements. Such an open private 5G network architecture has not been investigated yet in any of the aforementioned projects, aiming to break the economic barriers of 5G deployments with an affordable solution, accelerating its adoption in industry and enterprise environments, which clearly differentiates Affordable5G from the rest of 5G PPP projects.**

1.4 Relevant Alliances, Fora and Working Groups

Several alliances, open source communities and standardization have been established to deal with different flavours and application domains of the 5GS. This section provides an overview of those targeting any type of issue related to Private 5G Networking, including specifications, testing, validation, implementation, etc.

5G-ACIA [26] is the central global forum for shaping 5G in the industrial domain. As it was also referred in the previous sections, one of the main differences between 5G and previous generations of cellular networks lies in the strong focus of 5G on machine-type communication and IoT. In particular, 5G supports communication with unprecedented reliability and very low latencies, as well as massive IoT connectivity. This paves the way for the next era in industrial production, known as "Industry 4.0", which aims to significantly improve the flexibility, versatility, usability, and efficiency of future smart factories. In this context, several documents have been published within the 5G-ACIA framework, identifying potential industrial use cases that can be supported with 5G networks, analysing testing and validation requirements as well as covering security aspects for 5G industrial networks. In [27] various Industrial IoT (IIoT) deployment scenarios for non-public 3GPP-defined 5G networks are described. Special emphasis is given either to the coexistence of standalone NPNs and NPNs with public networks. In [28] the white paper presents industrial network security requirements and current practices, and examines 5G security features and how well they match industrial needs. The paper also describes use cases and deployment scenarios to help to identify 5G-specfic security requirements, based on four deployment scenarios, namely standalone NPNs, shared radio access NPNs, shared radio and control plane, as well as shared radio, control and user planes.

The most recent publication of 5G-ACIA [29] deals with the functional requirements to expose the capabilities of non-public 5G systems to connected industries and automation applications. Via exposure interfaces, industrial applications can access 5G capabilities for factory and process automation, production IT, logistics and warehousing. Industrial applications have also access to communication service monitoring and network management capabilities.

3GPP is a partnership body that brings together standardization organizations from around the world to create globally acceptable specifications for mobile networks. As its name implies, it was first created to establish such specifications for the third generation (3G) of mobile systems. It has continued its work for subsequent generations, including the one considered here, the fifth generation (5G). In this context, the work in [30] presents the system architecture for the 5G system. The 'Vertical LAN' work item, in 3GPP Release-16, introduces the following three new and distinct 5G enablers for Industry 4.0, namely support for time sensitive communications by seamlessly integrating the 5G system as a bridge to IEEE TSN, support for Non-Public networks and support for a 5G-LAN type service. The IEEE TSN specifications are considered the convergence technology that will enable deterministic and low-latency communication in the factories of the future. 5G TSC is a service that supports deterministic and/or isochronous communication with high reliability and availability [31]. The document in [32] defines the Stage 2 procedures and Network Function Services for the 5G system architecture, which is described in TS 23.501 [30], and for the policy and charging control framework, which is described in TS 23.503 [33].

Other documents focus on security and authentication procedures, such as 3GPP TS 22.261 [32], which states that the 5G system shall support operator-controlled alternative authentication methods with credentials that differ from 3GPP specifications for network access for IoT devices in isolated deployment scenarios, such as for industrial automation.

O-RAN ALLIANCE [10] has been founded in February 2018 by AT&T, China Mobile, Deutsche Telekom, NTT DOCOMO and Orange. It was formed by a merge of two organizations, namely the C-RAN Alliance and the XRAN Forum. It has been established as a German entity in August 2018. Since then, O-RAN ALLIANCE has become a world-wide community of mobile network operators, vendors, and research & academic institutions operating in the RAN industry. O-RAN underscores streamlined 5G RAN performance objectives through the common attributes of efficiency, intelligence, and versatility. Open RAN deployed at the network edge will benefit 5G applications, such as autonomous vehicles and IoT, support network slicing use cases effectively, and enable secure and efficient over-the-air firmware upgrades. All related specifications can be found in [34].

The **Telecom Infra Project (TIP)** [35] was formed by Facebook in 2016 as a global community of companies and organizations working towards accelerating the development and deployment of open, disaggregated, and standards-based technology solutions that deliver global telecom network infrastructure, enabling global access for all. One of TIP's project group is focused on OpenRAN, but, while the O-RAN Alliance develops standards, TIP is more focused on deployment and execution. TIP enables the Open RAN ecosystem, by ensuring interoperability of different vendor's software and hardware equipment, productization of use cases, facilitating of trials, plug fests and field testing.

The **O-RAN Software Community (SC)** [36] is a collaboration between the O-RAN Alliance and Linux Foundation, with the mission of supporting the creation of open-source software for the RAN. The O-RAN Software Community is focused on the alignment with the O-RAN architecture and specifications to achieve a solution that can be utilised for industry deployment.

The **Small Cell Forum (SCF)** [37] has created its own ecosystem of Open RAN with small cells in mind. Focusing heavily on creating open interfaces, they have released a set of specifications, enabling small cells to be constructed using components from different vendors in order to address the diverse mixture of 5G use cases. One of the focus areas is private networks, and a recent report introduces SCF’s position on building Private Cellular Networks with Small Cells [38].

The **OpenAirInterface** (OAI) Software Alliance (OSA) is a non-profit consortium fostering a community of industrial as well as research contributors for open source software and hardware development for the core network (EPC), access network and user equipment (EUTRAN) of 3GPP cellular networks [39]. The OpenAirInterface Software Alliance has launched the OAI 5G Core Network Project Group. The scope of 5G CN developments in the context of this group is to deliver a 3GPP compliant 5G CN under the OAI Public License V1.1.

The Fraunhofer FOKUS **Open5GCore** toolkit is a worldwide first practical implementation of the 3GPP 5G core network. It mirrors in a prototype form the 3GPP Release 15 for the core network functionality and its integration with 5G New Radio (Standalone and Non-Standalone) [40]. Open5GCore Rel. 5 integrates with 5G New Radio Stand-Alone (SA), off-the-shelf LTE and NB-IoT LTE and non-3GPP access networks, such as WiFi and 60Ghz WiFi, enabling immediate demonstration of different features and applications and supporting the current need to have a genuine 5G Core Network in addition to the evolved EPC one.

The **Critical Communications Association (TCCA)** [41] is a global industry body established over 20 years ago to represent the needs of the critical communications sector ranging from governments to industry. The TCCA leads the global development and promotion of standardised critical communications solutions for professional users and works closely with organisations responsible for the development of open standards relating to critical mobile communications, including ETSI and 3GPP.

The **GSMA** [42] represents the interests of mobile operators worldwide and the broader mobile ecosystem. In matters related to private networks, the GSMA usually adopts the view of the mobile operators. For example, in a public policy position paper, related to spectrum best practice for industry verticals, GSMA advocates that spectrum should only be allocated to MNOs, as they could serve industry verticals through network slicing [43].

The **CBRS Alliance** [44] is an industry organization that aims to promote LTE and 5G New Radio-based solutions for the US 3.5GHz CBRS band. The Alliance uses the OnGo name as its consumer-facing brand. It focuses heavily on private networks and industrial IoT for various verticals.

IEEE Future Networks [45] is an initiative focusing on the development and deployment of 5G, while envisioning the landscape of connectivity and applications in beyond 5G networks. Initially launched as IEEE 5G Initiative in December 2016, the initiative was re-branded to IEEE Future Networks, in August 2018. IEEE Future Networks is one of the IEEE Future Directions initiative [46]. There are eight working groups, including Standards and Technology Roadmap.

5G Americas [47] is an industry trade organization composed of telecommunications service providers and manufacturers with the mission of fostering the advancement and full capabilities of LTE and evolution to 5G. 5G Americas is represented in 3GPP and focuses heavily on private networks. A recently published white paper is 5G Technologies in Private Networks [48].

1.5 Business Opportunities for Private 5G Networks solutions

Although governments are pushing the deployment of 5G networks, MNOs are reluctant to invest since they cannot see a killer application that will ensure a profitable return on investments. It should also be highlighted that consumers are not willing to pay more for 5G services and especially for only higher speeds. On the other hand, enterprises can pay more in case 5G solves existing problems and unlocks new business models. Thus, MNOs and service providers should shift their focus from consumers to enterprises to generate new revenue streams.

According to a report from Ericsson [49], consumer-related service revenues are expected to remain close to flat at an annual growth rate of 0.75 percent through 2030. On the other hand, business opportunities across industries are expected to grow with a Compound Annual Growth Rate (CAGR) of about 12 percent over the same time period (Figure 6). However, the real challenge for the ecosystem (operators, service providers, etc.) is to define its strategy and identify/prioritise the target areas/industries.

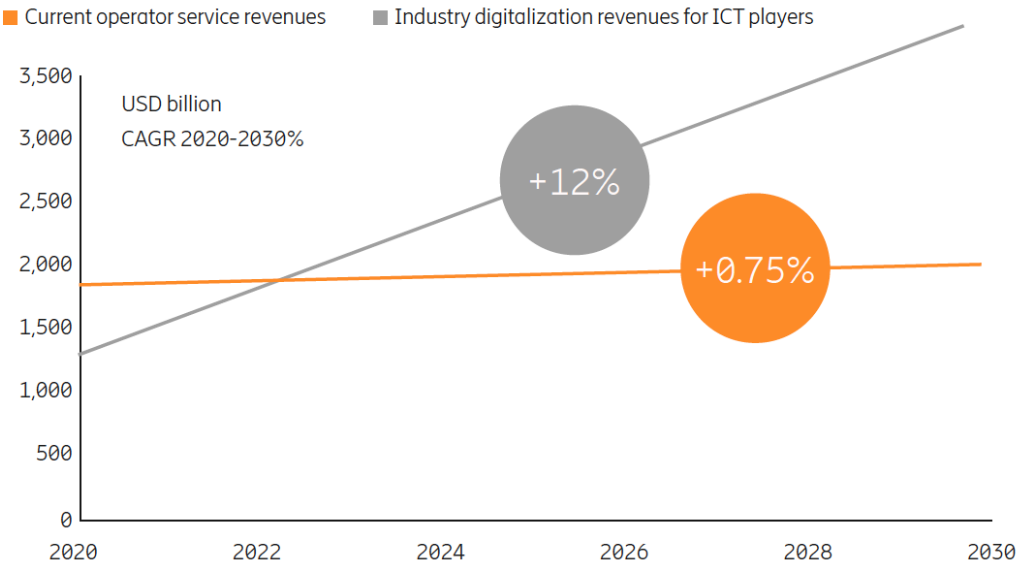

Figure 6: The service provider challenge (Source: Ericsson and Arthur D. Little)

According to a study conducted by Forbes [50], in partnership with Huawei, more than 80% of executives believe that 5G can provide a range of benefits while industrial managers have perceived 5G as a means/platform for the upgrade and transformation of multiple aspects of their operations releasing the full potential of digitalisation. These business benefits offer the opportunity to MNOs and service providers to enhance their value proposition towards enterprise customers transforming 5G to a business need:

- The minimization of human error and the improvement of decision making through machine assisted techniques.
- New business models that can exploit the vast amount of data availability, through countless connected devices such as sensors, cars, IoT devices, etc.
- The ability to transfer and visualise data in real time will provide operations personnel or customers with great insights and the ability to read and react effectively.
- The seamless interconnection of numerous devices will open a new era of agile automation without hurting customization, flexibility or quality.
- Access to data and computational power will create a combinatory force that improves efficiency and process quality, reducing friction and wastage.
- Connection trustworthiness through the provision of critical services/products that ensure data security and network uptime.

Hence, it seems that although eMBB services will not be the profitable case, it will support the deployment of 5G and facilitate its success mainly through the elimination of information islands, the transformation of diverse industries, the implementation of the digital transformation in production, product and service provision, sales, and ongoing support processes. Thus, 5G will have a significant impact on the market, offering new business opportunities for MNOs and service providers from eMBB to applications for vertical industries customers.

According to KPMG [51], an estimated US$4.3 trillion in value is waiting to be unlocked across the major industry verticals (Figure 7).

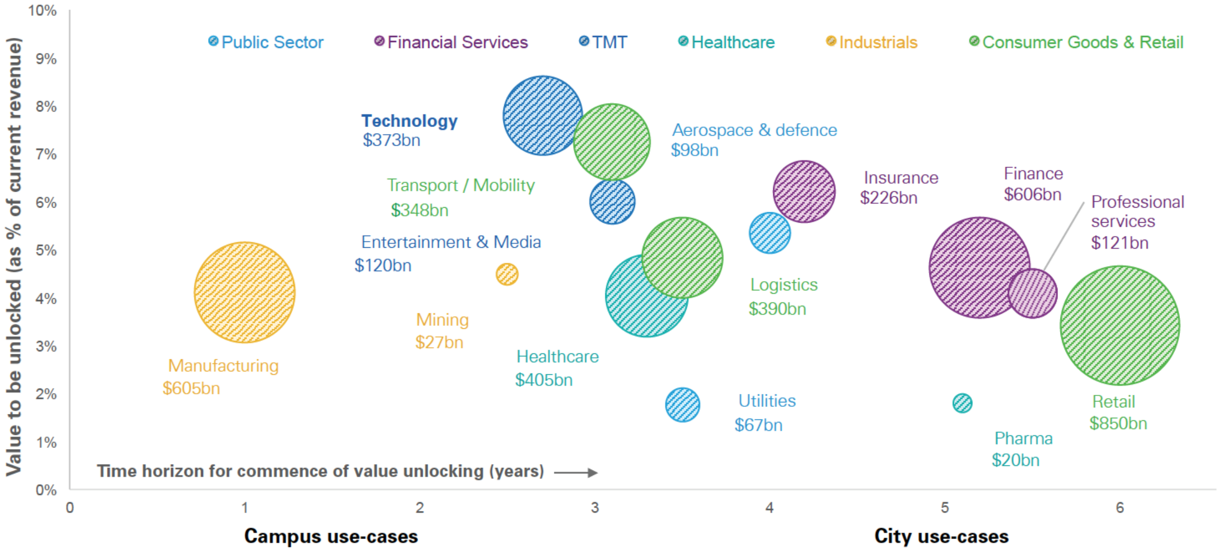

Figure 7: 5G enterprise value (source: KPMG)

Private networks are expected to play a significant role in the enterprise market, unlocking new business opportunities for MNOs, service providers and/or industries depending on national spectrum availability and in-house expertise. In fact, private networks can be assumed as a means for industry digitalization by providing i) scalable solutions by leveraging connectivity and platform services across a broad range of industries (horizontal approach), or/and ii) industry-specific end-to-end solutions by leveraging applications, service provisioning and service delivery on top of connectivity and platforms (vertical approach).

There are several 5G technological advancements that facilitate business opportunities and make the deployment of private networks especially enticing. Spectrum sharing is one such case that will simplify the access and more efficient usage of spectrum, which could produce broad socioeconomic benefits. Private networks require access to spectrum, a costly and scarce resource that is, in most cases, licensed to and used by large operators. The ability to actively share this resource and enable different network tenants to operate under an efficient and cost-cutting deployment will provide a solid foundation for innovativeness. As a result, shared spectrum can enable more types of services, being fully and efficiently utilised while reducing interference issues, achieving in the process major goals set by regulators around the world. Ease of access to spectrum, renders private networks more deployable allowing new revenue streams to flourish. Private networks create a paradigm shift in the management and operation of networks as enterprises can now manage their private cellular communication networks dedicated to their business, providing even greater flexibility. Spectrum sharing is relaxing the need for costly investments and coupled with the capabilities that network slicing is providing, an entirely new approach for the provision of services is revealing itself to the business world. The network owner cannot only efficiently manage RF resources but at the same time provide specialised, software-defined network slices to its tenants that caters to their specific needs in terms of specifications and architectural components.

In the pre-5G era, networks were not so adaptable, which made them unable to host diverse types of service providers. Nowadays, network operators, industries, service providers, and other organizations can all benefit from the ability to access 5G networks specialised to their needs. Network slicing allows the creation of isolated networks within a network, serving varied industrial applications with different QoS requirements and simultaneously providing isolation of computing, storage, and networking resource. Resource management is thus maximised as private network slices' functionalities are optimised based on needs and requirements, not to be affected by the network's initial architecture. Moreover, privacy and security requirements are more easily safeguarded since traffic flows through the appropriate network slice, providing solutions to data storage and accessibility related issues. The orchestration of tasks is another benefit of network slicing as resources are allocated according to need, ensuring reliability for prioritises tasks, a critical feature in cases like e-health.

Especially important is the fact that the described 5G features come along with reduced costs as MNOs can more efficiently deploy and manage the slices without the need for infrastructural changes. This is a great opportunity for all stakeholders and adds further potential to initiatives that aim to increase 5G collaboration.

Network softwarization also decouples infrastructure from vendor exclusivity as open source solutions are trending in the 5G sphere. This is the case of the O-RAN Alliance, which promotes openness through virtualised and fully interoperable mobile networks. The employment of open source solutions can enhance the flexibility of 5G networks enabling modularity, AI integration, and collaborative competitiveness, thus accelerating the innovativeness related to the 5G ecosystem. This new open paradigm will unlock new business opportunities as networks become able to incorporate a great degree of fluidity that comes along with software-based components within the physical infrastructure. Additionally, the ability to distance networks from proprietary hardware-software attachments will reduce the costs and increase efficiency.

A business model that seamlessly brings together the aforementioned 5G technological opportunities is the Neutral Host (NH) model. The NH deploys and operates its own network and leverages slicing techniques to provide access to other entities (tenants), which are only responsible for handling their own slices. The NH is in charge of managing the spectrum while hosting tenants with diverse needs, allowing for adaptable implementations on a common platform that can bring under its roof various types of business models. The NH model is very appealing since it can provide answers to questions related to cost of ownership, spectrum sharing and network management without loss in flexibility. The NH alleviates these issues as it allows the deployment of a single network by a neutral entity, e.g., enterprise, venue owner, other partnerships, overcoming problems related to lack of space and investment replication, and offering wholesale access to its tenants, who do not need to make the costly investments associated with 5G deployment. In the context of private networks, the NH is more likely to bring enterprises and mobile operators together. For example, corporations and venue owners, which need to offer their staff and clients mobile access, would greatly benefit from inviting all operators to participate in their networks providing an overall higher quality of service, and covering all potential end users. By promoting overall efficiency through spectrum sharing and infrastructure sharing, and assuming the role of network operator, the NH helps reduce overall capital and operational expenditures producing significant socioeconomic benefits. Even in the case where no NH is established, a greater degree of resource sharing can prove to be highly beneficial. Network sharing has been established as a viable cost reducing mechanism in the past reducing capital and operational expenditure and Total Cost of Ownership. 5G offers greater possibilities for wholesale network sharing models, for example in the case of enhanced broadband. Due to the ability to virtualise core & radio, wholesale models can offer end-to-end customizable private networks that are completely suited to customers' needs, addressing different verticals with specific service performance packages.

The value of private 5G networks is already being successfully explored on several occasions.

1.5.1 Private 5G Network deployments around the world

Access to spectrum is one of the keys to unlock the private networking market. The ability to deploy networks without dependencies on public cellular systems or licensed operators gives enterprises greater ability to control their operations and removes friction from the market. Dedicated enterprise spectrum and shared unlicensed spectrum are both important to accelerate the adoption of private networks.

Private networks can use spectrum across a range of frequencies, subject to diverse license terms. From an industrial IoT perspective, it is important that spectrum is available, supported by a product and integrator ecosystem, and subject to stable regulations that allow for long-term planning. These are all important to for industrial users seeking to make major investment into operational technologies that have long life cycles.

In this context, a 5G private network has been deployed at a gas terminal by Vodafone ending paper processes and implementing predictive maintenance leading to improved productivity and saving £5 million in one year.

The EU-funded project MoNArch tested a 5G dedicated network at the Hamburg Port to transmit movement and environmental data in real time across large areas.

Swisscom also tested a private 5G network at the 2020 Youth Olympic Games in Switzerland to greatly reduce equipment installation time and the required manpower by connecting all the production equipment at the venue wirelessly.

Other industries where 5G private networks could be deployed include healthcare, airports, and mining. However, manufacturing can be proved to be the most mature sector for digital transformation through 5G private networks enabling dynamic, self-regulating, and self-adjusting processes that translate into agility, speed, and higher productivity, which, in turn leads to competitive advantage and new revenue opportunities. These will transform linear processes into circular ones creating significant value. Moreover, this transformation will also benefit end customers through customization, quality, and speed of delivery.

According to a study by Nokia and Nokia Bell Labs, a combination of private networks with edge computing and data analytics (5G+ ecosystem) will further contribute to growth and drive the global economy upwards by seven percent, potentially, or $8 trillion in 2030. This 5G+ ecosystem will promote the digital transformation of "physical industries", transforming them into "augmented physical industries". It is also interesting to highlight that COVID-19 pandemic boosted this digital change.

The Global mobile Suppliers Association (GSA) recently confirmed that it is tracking at least 330 companies that have been or are investing in private mobile networks based in LTE or 5G, in the form of trials and pilot deployments, commercial network launches or investment in licences that would enable deployment of private LTE or 5G networks.

Analysys Mason, who are tracking commercial Private LTE/5G networks worldwide, are reporting 319 networks as of September 2020 (101 of them public domain).

The US-based company Verizon is working with Nokia to build 5G infrastructure in factories, offices, and other private sites. In this context, the goal is to create a global private 5G service for enterprises outside the US, focusing on the Asia-Pacific region and Europe.

In addition, many European countries have already set realistic timetables regarding the introduction of private 5G NPNs. The German telecoms regulator, BNetzA, reserved 100MHz of spectrum in the 3700MHz-3800MHz band to private companies. According to the regulator, 33 companies have bought 5G private licenses so far including Bosch, BMW, BASF, Lufthansa, Siemens, and Volkswagen. Lufthansa, using their own spectrum at 3.5GHz, was one of the pioneer companies to adopt 5G SA for private networks for the engine hangars, with main use cases including Remote and Virtual inspection.

Netherlands has allocated 100 MHz of spectrum for private networks in the 3.5 GHz band 43, in addition to 5 MHz that were already available in the 1.8 GHz guard band. There have already been 179 applications for the new allocation, with uptake extraordinarily strong in healthcare institutions, warehousing, production, and other verticals. An example of a private network running a very business-critical application is the private LTE network in the port of Rotterdam.

Groupe ADP and Air France are deploying a private mobile LTE/5G network covering Paris-Charles de Gaulle, Paris-Orly and Paris-Le Bourget airports. The network will serve an ecosystem of more than 120,000 people who work at the three Paris airports, across 1,000 companies of sizes and sectors. The network will cover all airport outdoor spaces by the end of 2020 and indoors across all public and reserved areas for professionals working at the terminals by the end of 2021.

In the UK, OFCOM issued a consultation from November 2019 until December 3, 2019 on draft statutory instruments that would support its local spectrum access and spectrum sharing policies. The regulator will dedicate the 3.8-4.2 GHz band for local deployments, requiring national operators to hand over unused licensed spectrum to enterprises. The lower 26 GHz band will be reserved for private and shared access as well. Other countries outside Europe including Japan, Australia and Hong Kong are also moving forward with their plans to identify and allocate spectrum for localised, private 5G networks with a primary focus on the 3.7, 26 and 28 GHz frequency bands.

In Belgium, the regulator has not allocated a band for private usage yet. However, there is a player called Citymesh that acquired 3.5 GHz spectrum some years back, originally intended for backhaul of urban Wi-Fi networks. That very spectrum is now deployed by Citymesh for campus networks and enterprise mobility. With the emergence of private mobile network demand, Citymesh on occasions has also granted access to its spectrum for individual use cases and third-party private networks. Examples are the seaport of Zeebrugge, and Brussels Zaventem airport.

2 PILOTS AND USE CASES DESCRIPTION

With the purpose of testing and demonstrating the capabilities of Affordable 5G achievements it is planned to provide three pilots addressing three different pillars of a 5G ecosystem. The first pilot addresses Mission Critical Communications, the second pilot focuses Smart Cities and IoT devices and the third pilot addresses 5G non-public networks as required for the Industry 4.0. Within each pilot one or more deployment scenarios are defined to meet the requirements of the pilot, i.e., the compute resources, network resources, as well as their high-level interconnectivity. Finally, one or more use cases are defined within each deployment scenario to describe the way the scenarios will be used/exploited to demonstrate the added value.

2.1 Pilot 1: Emergency communications

2.1.1 Description and goal of the pilot

In the context of spectrum scarcity and technological obsolescence, and under the impetus of the potential users of major mission critical services potential users, such as national authorities, as well as major industries across different domains (including railway, mining, transport), 3GPP 5G standardization has been widely chosen to develop and lead these mission critical systems into innovative, interoperable and future seeking ways to communicate within first responders and business ecosystems.

Mission critical services over 5G networks provide users with access to secure, reliable and high-performant communication services integrated with the network and providing the service even under extraordinary emergency circumstances. MCS are mainly used for voice applications such as group voice calls, also known as push-to-talk or walkie-talkie type applications, the transfer of short messages or very low data rates and mission critical video.

The transformation of mission critical services in the 5G architecture aims to revolutionise the way people work and collaborate, notably sharing data and video with a dedicated QoS to maximise call set-up times and prioritization of services in the event of congestion and operation in isolated mode (site isolated from the core network).

This pilot aims at demonstrating the 5G private network concept, and the it is suitable to address the performance and reliability requirements of MCS, allowing the owner to control their 5G network to serve a limited geographic area with optimised services using dedicated equipment.

The pilot will enable the implementation, validation and demonstration of a robust solution that will leverage the cloud native functions of monitoring, flexible deployment and scaling, as well as standardised 3GPP-compliant MCS communication channels, mainly including Mission Critical Push To Talk (MCPTT), Mission Critical Video (MCVideo) and Mission Critical Data (MCData), following 3GPP documents [3].

The aim of the use cases within this pilot is to achieve the provisioning of a responsive service that is able to cope with drastic service consumption increase or adverse network conditions so that the first-responders are able to keep communicating regardless of outages, communication demand increase, detection of poor communication quality, etc.

In order to exploit the 5G private and public network interaction regarding the emergency communication use cases two possible deployment scenarios are described to address the various use cases and events. The list of use cases is the same regardless the selected scenario, but each deployment scenario poses different prerequisites and therefore distinct boundary conditions.

The first deployment scenario describes a private 5G network providing services to various tenants or authorities in a concrete coverage area. The second one intends to give response to an emergency situation in which national external authorities would access the concrete coverage area either by their own commercial network (in the case private and public coverages would overlap) or by attaching to the network already existent in the area. In this case the coexistence of a Public 5G network to cover the needs of regular consumers and national authorities in the same coverage area where the Private 5G network is deployed, will be considered in order to differentiate between the needs that each user, tenant or authority has in terms of QoS, priority and re-emption (QPP) among other features. In order to cope with the QPP requirements of first-responders, the use cases will deliver the emergency communication critical system as a private "pop up network", providing security and privacy, control and flexibility – leveraged by network slicing, vast bandwidth, light costs and low latency.

2.1.1.1 Deployment Scenario 1

The first scenario is based on a specific area covered by a neutral host provider. In this area, different authorities or tenants are going to be able to connect to services hosted in a private core/service infrastructure. They will already be under the local coverage provided by the neutral host when an emergency occurs and will access the mission critical service under the already deployed specific slice for these communications. The slicing will be managed across the infrastructures and in the case an edge instantiation of the core and services occur, a slice will be instantiated covering the edge infrastructure. Some of the tenants could also act as first responders regarding the emergency. Each authority will use a separate, totally isolated MCS service with its own provision, in the sense that even though each tenant will be located on the same service area, each one will have their personal provision and will have access to only their MCS service. In other words, all the tenants will share the same private coverage, as provided by the neutral host solution. **Neutral host operator** will provide the frequencies, antennas and connectivity between the radio access and the main and edge infrastructures.

Each tenant or authority shown in Figure 8, categorised on network services, will be instantiated via a specific slice defined per service, depending on the QoS and resources needs of each service.

Since due to very specific emergency events the above-mentioned service isolation could result in an impossibility of each tenant to communicate with other tenants, the scenario also envisions a way to intercommunicate authorities and therefore different MCS instances. To achieve this, additional MCS management and interconnection instance will need to be deployed to allow the regrouping of different authorities or tenant talk-groups in a single one. This typology of scenario envisions to show the interoperability, dynamism, and diverse system connection possibilities that legacy mission critical communications could not offer to cope with emergency situations.

This description just covers the prerequisites of this deployment scenario. Use case sections will describe how the use cases will be applied and under which network or service conditions, so that the scenario can be as responsive as the MCS services need to be.

This kind of deployment would fit with scenarios in which a specific coverage is required to guarantee the communications. It will provide a secure and reliable way to tenants to access their MCS services in an emergency situation. Airports and industrial zones could be considered as representative examples of potential users/area types of this deployment.

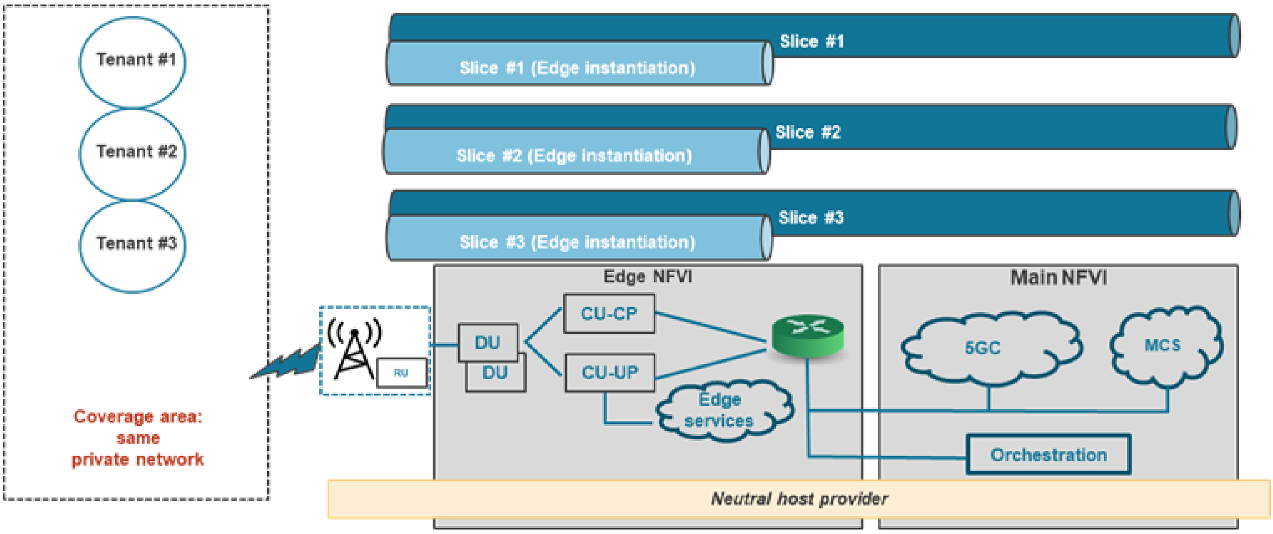

Figure 8: Pilot 1 deployment scenario 1

2.1.1.2 Deployment Scenario 2

This second scenario includes a regional or national security/emergency authority that will act as first responders to give support to the local tenants. Tenants and first responders in this second scenario are the ones under the local coverage and also the external national security authorities which, depending on their coverage, can connect to the local coverage or remain on the commercial one. We can consider the following deployment scenario as an enhancement of the first one in terms of geographic dispersion and service scalability. For scenarios where both a regional or national security/emergency authority and local or isolated ones coexist, the deployment possibilities are at least twofold:

- In the case that the regional or national security/emergency authority arrives to the specific area covered by the neutral host infrastructure and cannot depend on regular coverage offered by the national network provider, an MCS instance of the national authority will be deployed at the core part of the neutral host infrastructure. Additionally, the neutral host could also instantiate a lightweight 5G core of the M(V)NO hosting the national security authority and, in this way, allow MCS communication of the national authority through the neutral host network without requiring external connections. In case the scenario evolves to allow communication between separate MCS instances, the inter-MCS will occur within the same network (of the neutral host).
- In the case that the national authority is able to connect to the national network provider and wants to maintain this connection, the use case will involve two coverage areas and therefore, the inter-MCS environment will involve two different networks with external connection between them (this use case is not shown in the diagram below). As well as the previous one, this kind of deployment would fit with scenarios in which a specific coverage is required to guarantee the communications. Not only it will provide an equitable and reliable way and to assure the access to each tenant´s mission critical services but also to external emergency authorities, joining the area in an emergency situation to their own mission critical services. Similar to the previous scenario, airports and industrial zones could be considered as representative examples of potential users/area types of this deployment.

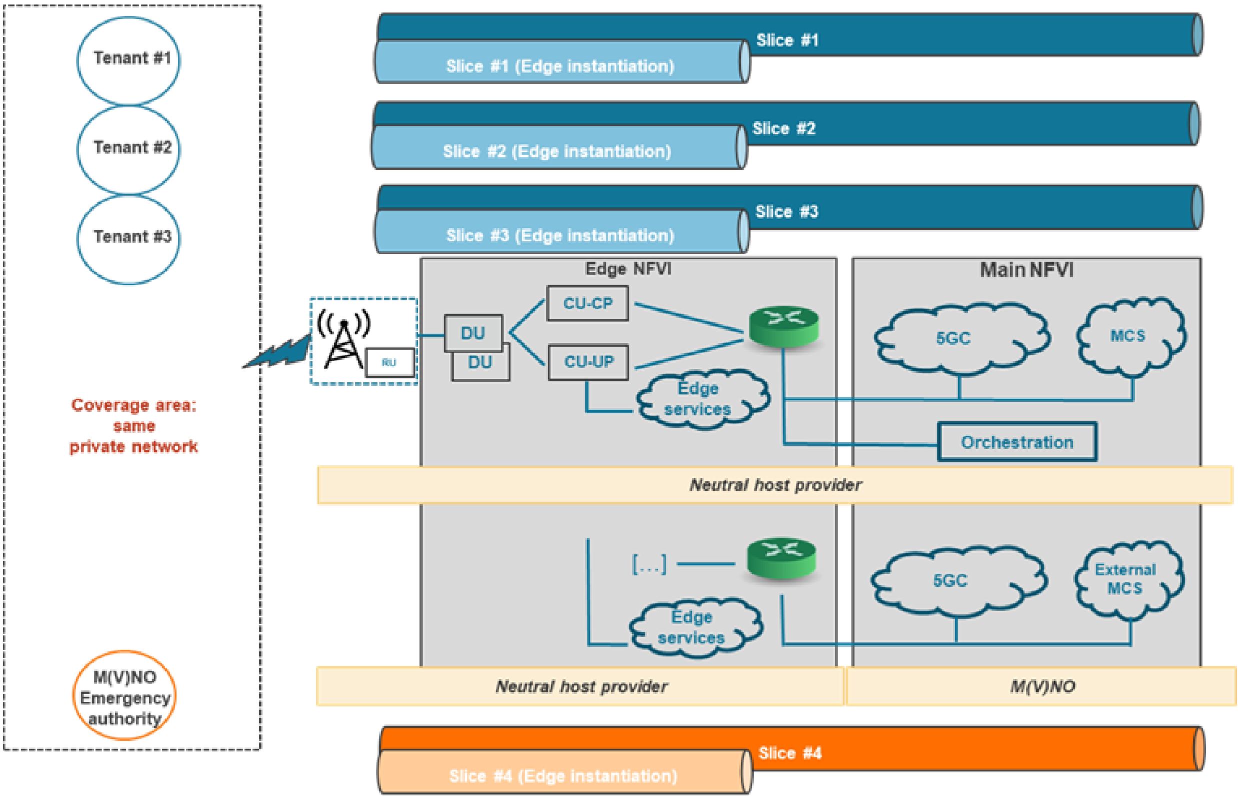

Figure 9: Pilot 1 deployment scenario 2

2.1.1.3 Use cases

NOTE: The following use cases equally apply to the two above-mentioned deployment scenarios, being each one just a conglomerate of prerequisites and boundary conditions. For each of the use cases described below, a monitoring module and an orchestration system are necessary.

Monitoring module: Alarm and detection systems are required to notice any variation of the nominal values from the system and MCS Key Performance Indicator (KPI). A communication between the orchestrator, the MCS Service and the infrastructures is considered. Depending on the KPI reports received from them, various alarm types will inform the orchestrator about the status.

Orchestration and slicing: The orchestration layer shall provide management and operation of network slice creation across the whole infrastructure and the services instances to support an adapted 5G QoS mapping associated to mission critical services. The orchestrator shall trigger the actions depending on the alarms received from the monitoring module.

1- **Service capacity:**

First responders communicating simultaneously in an emergency could lead to a MC service overload and the robustness of the whole network shall respond to the possible service dysfunctions in these situations.

Whenever the system detects a service KPI degradation due to an increasing number of connections or a load increase, an MCS scaling mechanism is implemented to deploy a new MCS VNF.

In order to be able to cope promptly with the service KPI degradation through an efficient scaling mechanism, a centralised or synchronised communication status database functionality withing the MC Service among the different instances shall be implemented as well as a service discovery so that the already deployed instances are notified by the orchestrator about the scaling of the service. A load balancer between instances to equilibrate the flows is also recommended.

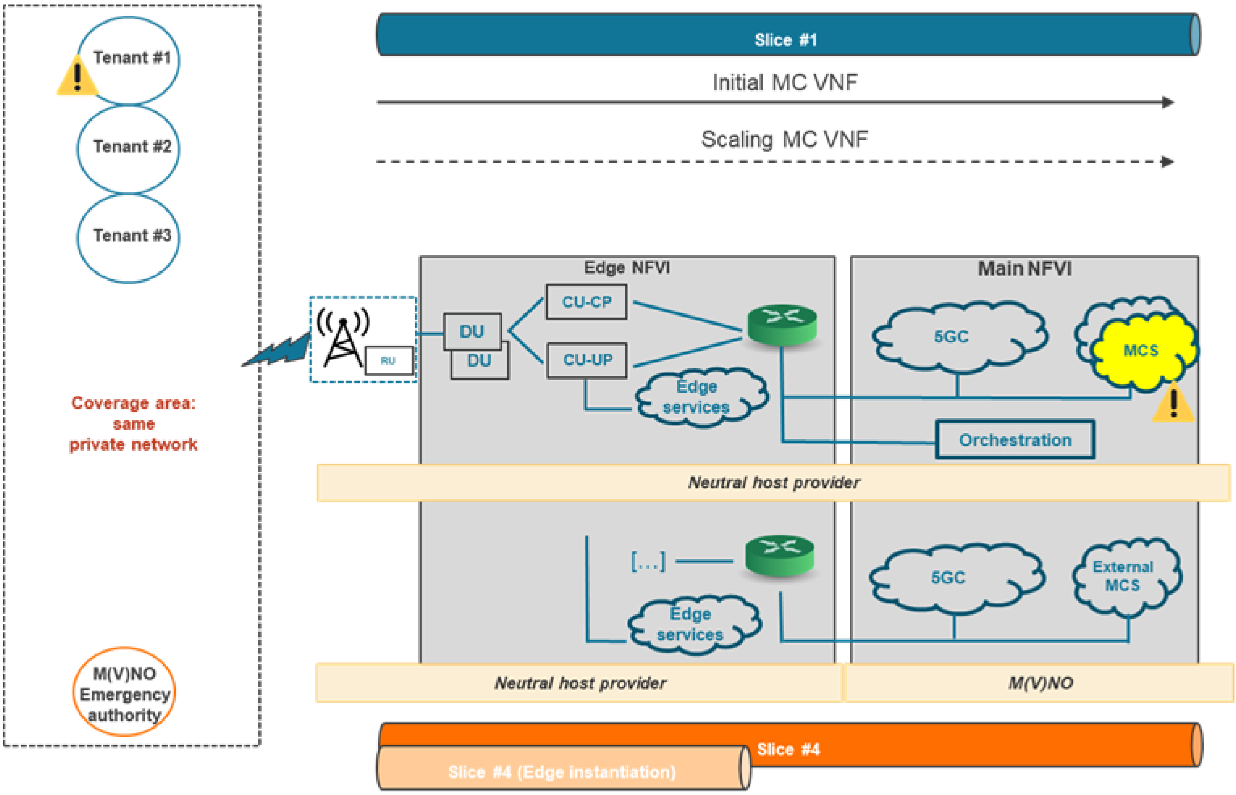

Figure 10: Pilot 1 use case 1 - service capacity

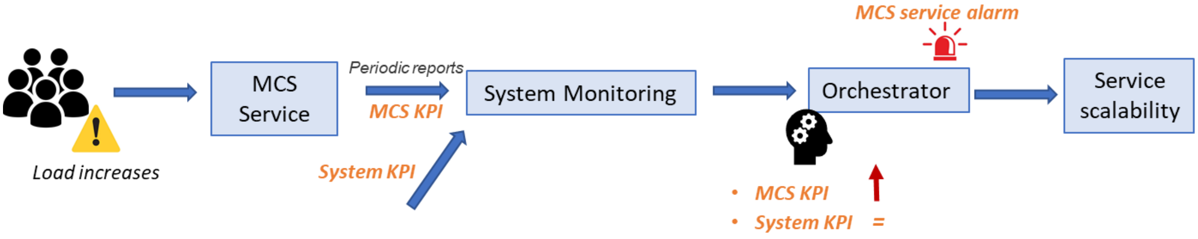

Figure 11: Service capacity use case main blocks

2- Increasing latency:

In a mission critical scenario, the required KPIs are strict so that the information exchange occurs in the least time with the maximum level of robustness. In that sense, latency is a key performance metric for emergency communications and during these situations, latency sensitive flows (e. g., MC Video) and a geographically distant Network Functions Virtualisation Infrastructure (NFVI) hosting the service could threaten the optimal performance of the communications.

Whenever the KPI values degrade from the predefined threshold (according to the MC service) and if an edge service deployment and a MC service instantiation may be possible, another MC instance in the edge will be implemented.

In both described deployment scenarios, when both first responders, local and national authorities, come to the area in which the emergency is ongoing, the neutral host may provide access to the service via the edge NFVI.

To be able to keep synchronization with the main core components, the orchestration framework should be able to maintain the described multiple point of presence (multi-PoP).

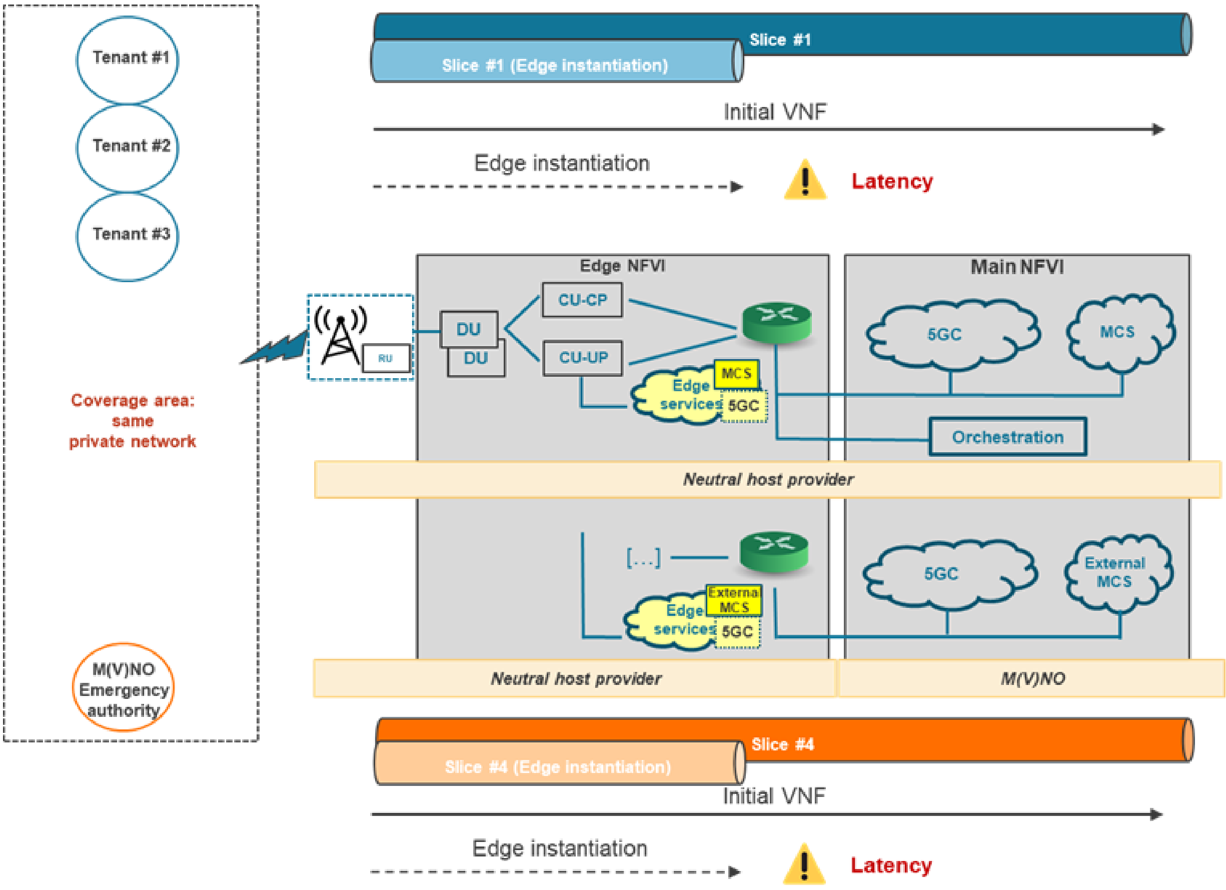

Figure 12: Pilot 1 use case 2 - increasing latency

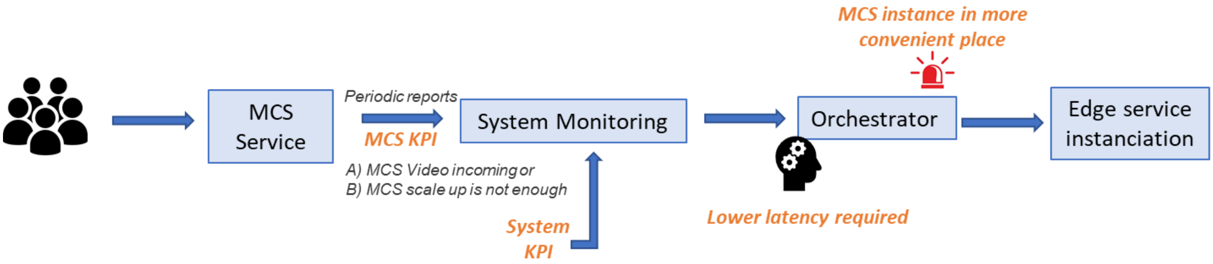

Figure 13: Increasing latency use case main blocks

3- Main core outage:

In case of catastrophic events, it is common to suffer either sudden outages or infrastructure damage or failure. To be able to give a technical response to first-responders to such a network transition, this use case aims at switching off the connection between the main core and the edge server so that the responsibility of the service delivery only relies on the edge deployment. The MCS system should be either notified by the orchestrator about this fact or be able to detect the situation. In any case, the MCS system should be able to launch the necessary availability procedures to reach a master-slave quorum inside the edge core without requiring any information or synchronization with the main one.

In this use case, both main NFVI (hosting the service reached by the local or the national authorities) are out of service and a copy of the core and service instances will occur in the edge NFVI. Neutral host provider will be in charge of managing the edge location and infrastructure.

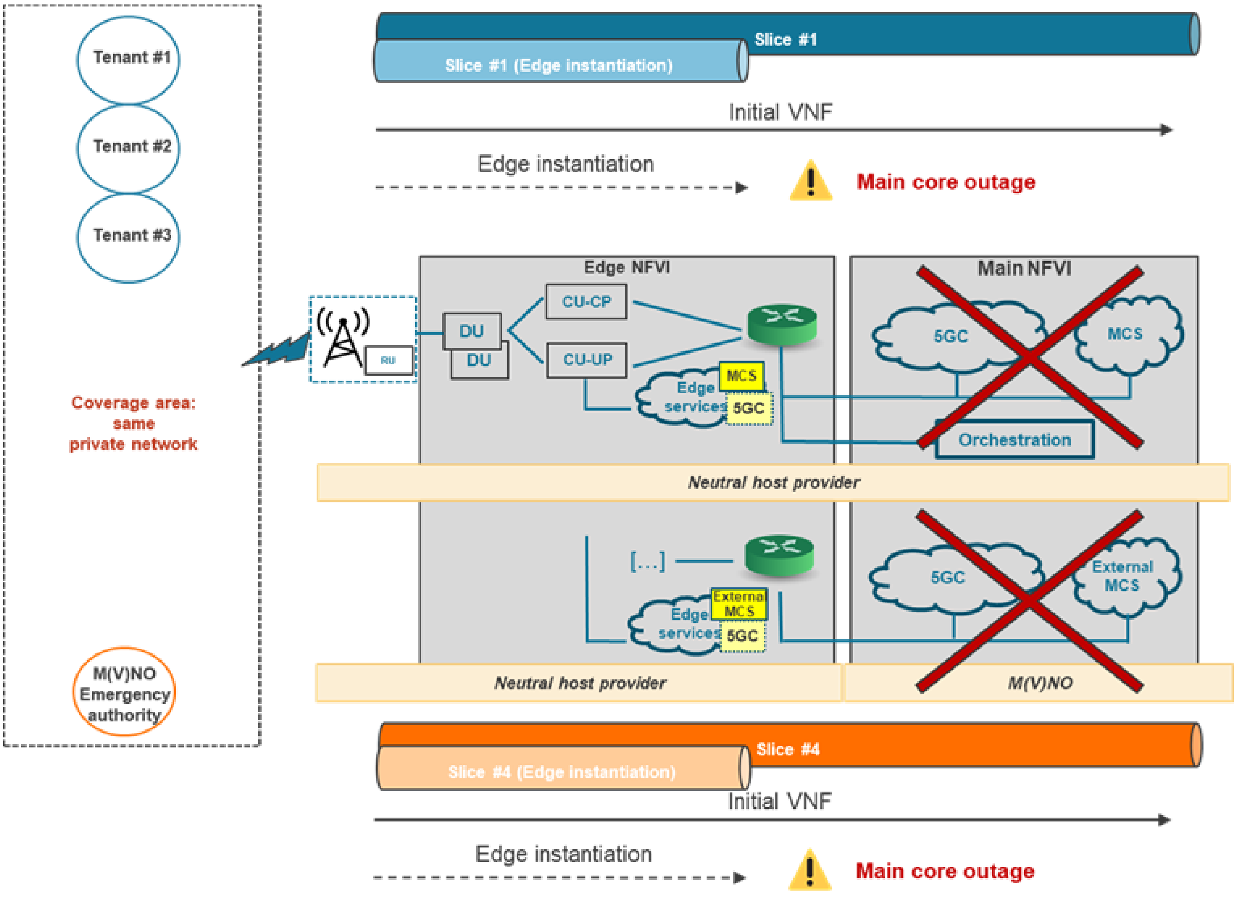

Figure 14: Pilot 1 use case 3 - main core outage

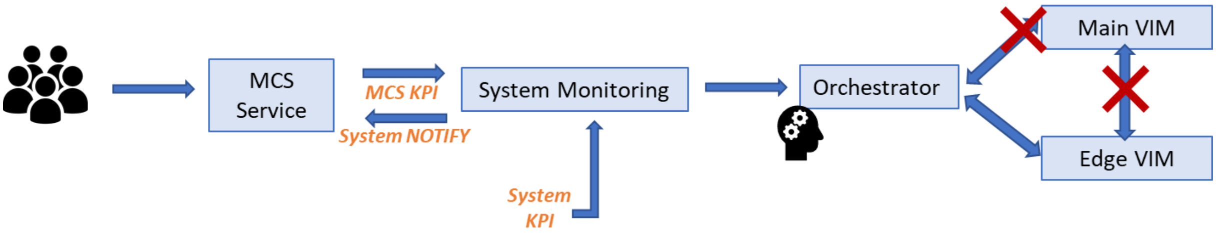

Figure 15: Main core outage use case main blocks

2.1.2 Entities/resources involved in the pilot

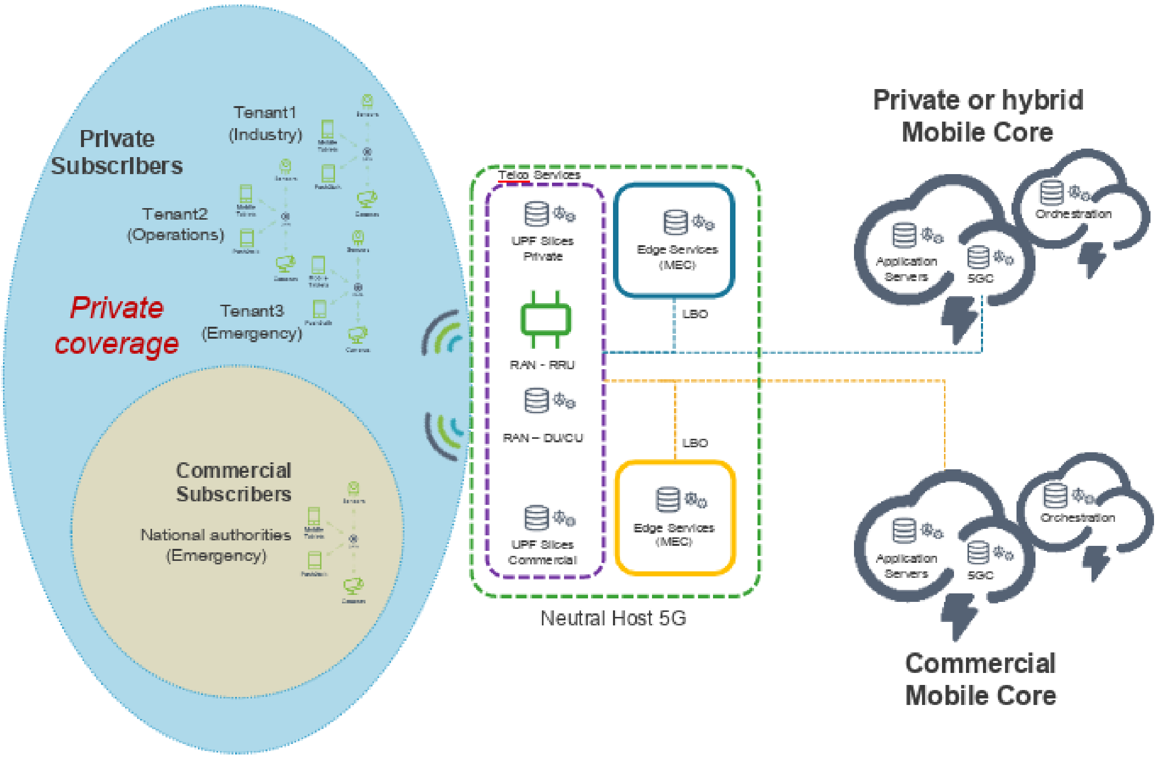

Figure 16: Main entities/resources involved in pilot 1

Pilot 1 will be carried out in the campus of Malaga and the circuit of Castellolí´s in which the deployment of the mission critical and 5G components will allow the validation of the various scenarios.

Málaga campus

In pilot 1, an O-RAN radio access solution, provided by Accelleran, RunEL, CellNex, is envisaged to be used as Neutral Host Provider, assuming spectrum is available for its usage at the Málaga testbed with this deployment. Additionally, UMA will provide its current RAN deployment composed of Nokia equipment as M(V)NO for the deployment scenario 2, with spectrum provided by Telefónica from its collaboration with UMA in the 5GENESIS ICT-17 project.

In a similar way, UMA currently possess UEs used in the testbed that will serve for pilot 1, although some additional UEs may be provided by other partners.

As for the backhaul network, UMA will use its current network composed of an optical switch with optical fibre and ethernet cabling. UMA will also provide hardware for both the Edge NFVI and the Main NFVI.

A virtualised 5G standalone (SA) mobile core network will be instantiated on top of the main NFVI to serve MC applications. The 5G SA mobile core network technology will be provided by Athonet. It will be compliant to 3GPP specifications, thus providing all the needed functionalities that enable MC applications to run on top of the mobile core network infrastructures.

NBC will provide their NearbyOne Solution, that addresses the problem of NFV and Application orchestration both at the Core and Edge of the Network. The solution includes as part of the

NFV/App lifecycle, the provisioning and configuration of the edge nodes and core VIM clusters or it can integrate with pre-provisioned clusters at the core or public cloud.

NearbyOne solution for Edge Orchestration can be used to automatically deploy, manage, and operate small cells and edge applications. The solution can trigger the previous mentioned actions based on inputs provided by the edge infrastructure and NFV/Apps KPIs.

Atos will contribute to the NFV MANO and its interaction with the Edge Orchestrator in collaboration with Nearby Computing, extending the multi-PoP NFV MANO management functionalities by splitting the network services allowing hybrid deployments, having simultaneously running some parts on the edge and other parts on the core.

Castellolí circuit

Currently, Castellolí testbed has eight auto sustainable (Power microgeneration, no grid connection) sites with six Accelleran small cells that cover a significant part of the 4,5 km circuit radius. Four of the sites have edge nodes (Lenovo SLE350). Castellolí network backhaul is wireless and does not use optical fibre. There are two backhaul options, i) a combination of P2P and P2M topology with limited bandwidth (100Mbps) using free licence spectrum. Ii) self-organised Metnet SON mmWave backhaul solution (Up to 1Gb). It is possible to move between the eight sites Small cells and edge nodes to create different scenarios.

4G Atto core will be migrated to 5GSA Mobile network Core technology, during Q1-2021. The 5GSA core will be in Castellolí Control room. NearbyOne solution for Edge Orchestration is used to automatically deploy, manage, and operate small cells and Edge Applications using some intelligent algorithms in Castellolí running on a Lenovo SLE350 server. Nearby One will be used with 5GSA core.

Castellolí Testbed has an Optical Fibre connection to Cellnex national network, which makes possible to move 5GSA core network to another Cellnex location and evaluate latency influence.

Cellnex has an agreement with a Spanish MNO, namely Mas Movil, to use their 3,5GHz spectrum in Castellolí premises. All the equipment and facilities described are the basis for developing UC1 in scenario 1 & 2.

For the use cases implementation, Accelleran and RunEl will provide the additional elements, including the O-RAN architecture that will be used as Neutral Host. Cellnex will also offer hardware for both the Edge NFVI and the Main NFVI.

ATOS NFV NANO interaction with NearbyOne orchestration will extend the multi-PoP NFV MANO management functionalities by splitting the network services allowing hybrid deployments, while, at the same time, running some parts on the edge and other elements on the core.

For both testbeds Nemergent Solution will deliver a 3GPP-compliant MCS VNF(s) and Android application for such communications that count with NEM MCS Application Server, NEM MCS Management Servers (Identity MS, Group MS, Configuration MS, Key MS), MSC Dispatcher, NEM MCPTT/MCS Enabler and a core IMS.

The NEM MCS Application server consists of a MCPTT AS, a MCData AS and a MCVideo AS.

The NEM MCS AS can work as a simple e2e Over-The-Top (OTT) solution, without network coupling interfaces, or can support Public Safety requirements such as QoS (through N5 interface or legacy Rx interface). The MCS AS also implements the core functionalities to support on-network private and group calls, affiliation procedures and provides the logic for switching between unicast and multicast transmissions based on the location information provided by the different UEs.

The Management Servers

The Identity Management Server or IdMS is a component defined by 3GPP. It is the main point of identity, thus it acts as the first entry point for the MCS authorisation and authentication.

The Nemergent Configuration Management Server or CMS and Group Management Server or GMS are the responsible party of all the capabilities related with the configuration of the MCS clients and users. Key Management server or KMS manages the system security: via encryption, integrity protection, and confidentiality.

The Nemergent dispatch system / MSC Dispatcher allows operators to receive / make / monitor MCPTT calls and MCData, to monitor running MCPTT users and groups calls and to perform some basic OAM operations.

The Nemergent MCS Enabler provides an API to the system functionalities, including provisioning and call procedure. By using this API, third party products can become MCS-compatible endpoints into the Nemergent MCS system. The Nemergent MCS Enabler acts as a Participating MCS AS to the main MCS system.

2.1.3 Interactions among entities

2.1.3.1 Use case 0: VNF uploading and instantiation

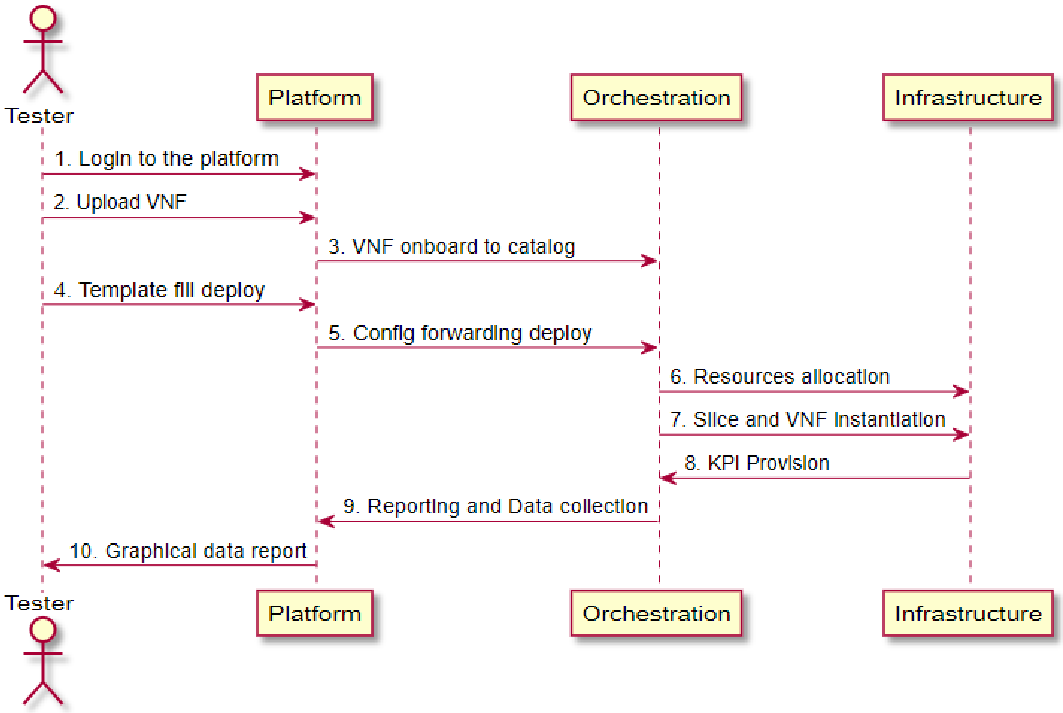

Figure 17: Pilot 1 VNF uploading and instantiation entities interaction

When running the tests, a deployment framework will be needed to authenticate and launch the execution of the deployment. First, the user will upload and onboard the VNF that will be after associated to a network service and a slice.

The following step will be for a user to fill the deployment template so that the platform can forward the information to the orchestrator. The orchestrator will use that deployment information to allocate resources and deploy the required slice and VNF(s).

2.1.3.2 Use case 1: Service capacity

The MCS service scale-up is depicted in Figure 18. The monitoring system will analyse the periodic service KPIs and system KPIs to alert the orchestrator when the current number of MCS instances cannot handle the incoming MCS load and the number of requests has been exceeded. The orchestrator will next allocate the resources in the main infrastructure in order to instantiate another MCS VNF.

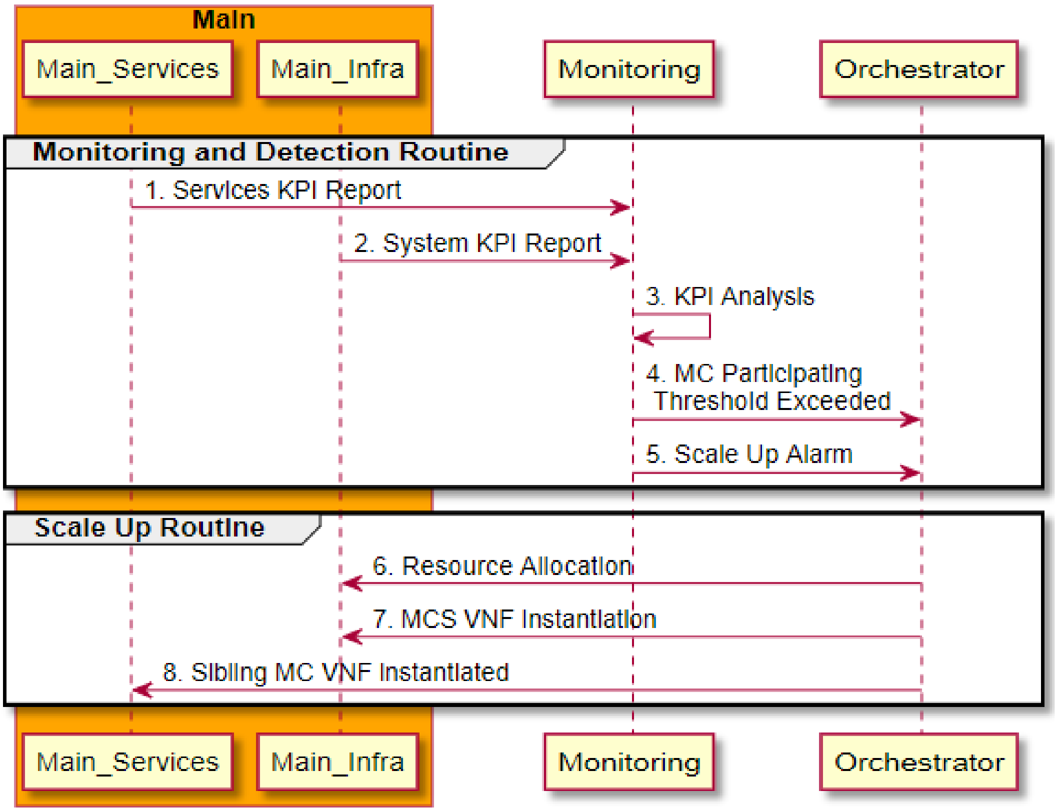

Figure 18: Pilot 1 use case 1 simplified entities interaction

2.1.3.3 Use case 2: Increasing latency

The MCS service instantiation in the edge will occur when periodic system KPI varies from the nominal expected values regarding latency and high performance. The monitoring system will alert the orchestrator in order to allocate resources and instantiate another slice containing the MCS VNF. After that, main and edge services will negotiate a master slave quorum as seen in Figure 19 below.

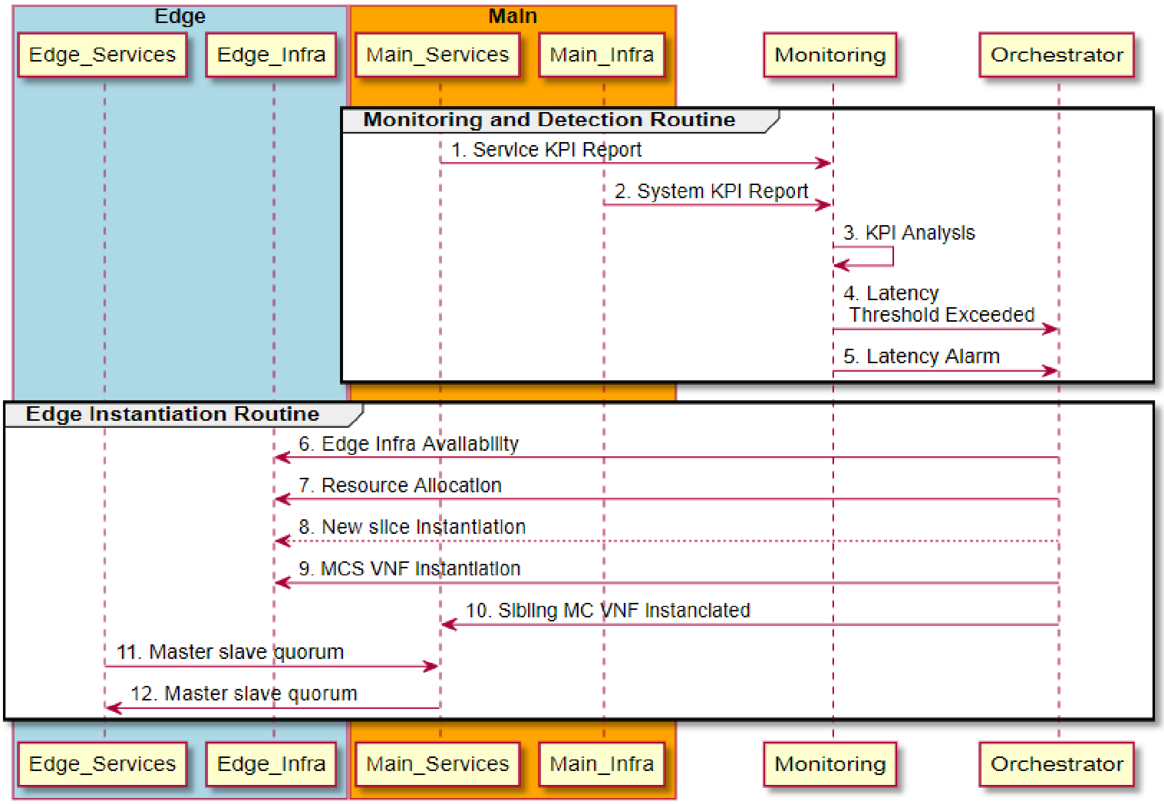

Figure 19: Pilot 1 use case 2 simplified entities interaction

2.1.3.4 Use case 3: Main core outage

- Main NFVI loses connectivity with the orchestrator and Edge NFVI:

Whenever this event occurs, the monitoring system will trigger an alarm to the orchestrator that will warn the already deployed MCS service about that the main one is not reachable as shown in Figure 20. The edge service will launch the necessary multi-PoP high availability synchronization procedures to reach a master-slave quorum inside the edge core without requiring any information or synchronization with the main one.

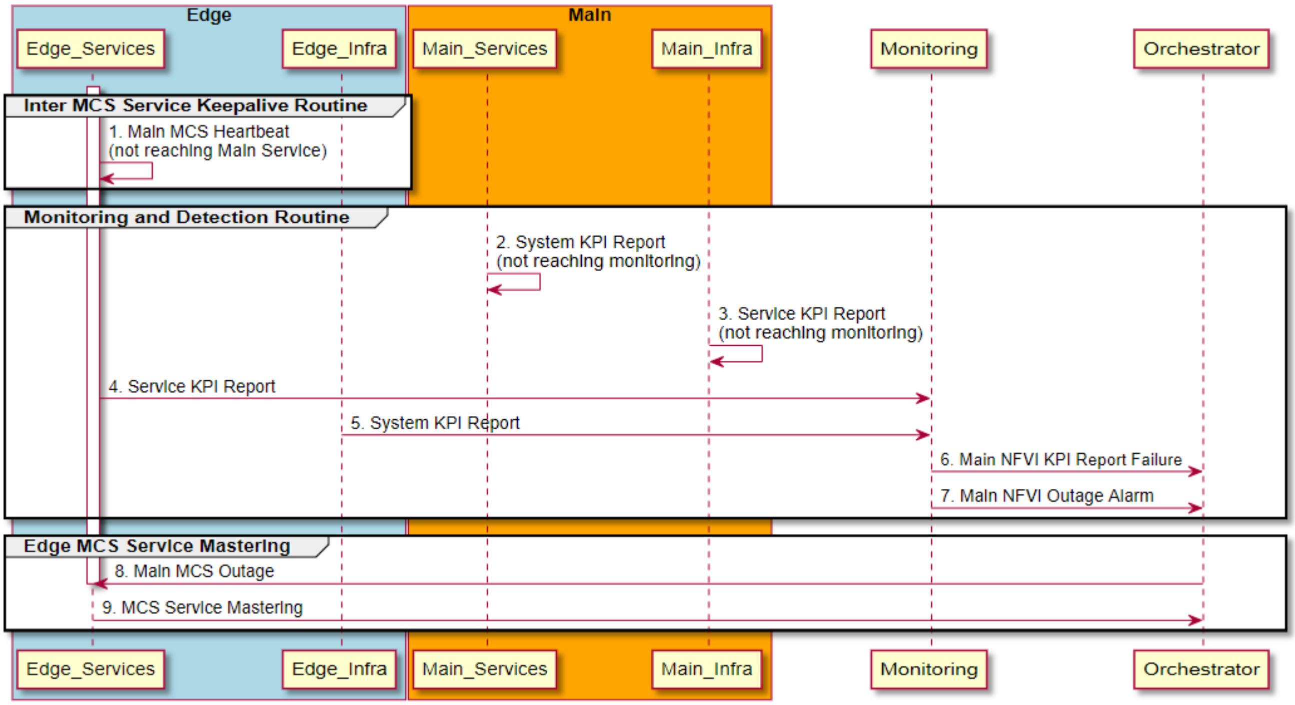

Figure 20: Pilot 1 use case 3.1 simplified entities interaction

- Edge NFVI is isolated from main NFVI and the orchestrator:

In Figure 21, when the Edge MCS service is unable to reach the main MCS service and no signal is received from the orchestrator, the edge will declare itself master.

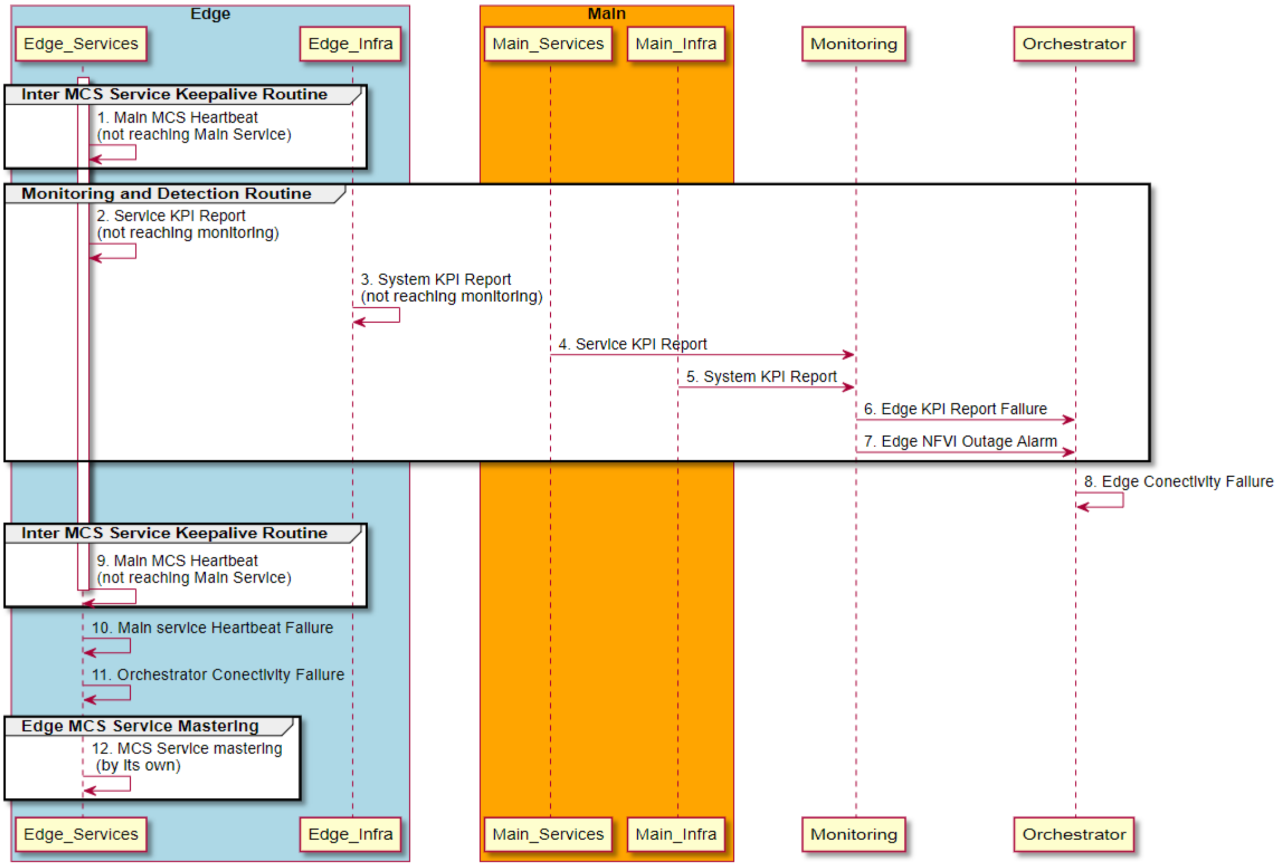
Edge
Main
Edge_Services
Edge_Infra
Main_Services
Main_Infra
Monitoring
Orchestrator
Inter MCS Service Keepalive Routine
1. Main MCS Heartbeat (not reaching Main Service)
Monitoring and Detection Routine
2. Service KPI Report (not reaching monitoring)
3. System KPI Report (not reaching monitoring)
4. Service KPI Report
5. System KPI Report
6. Edge KPI Report Failure
7. Edge NFVI Outage Alarm
8. Edge Conectivity Failure
Inter MCS Service Keepalive Routine
9. Main MCS Heartbeat (not reaching Main Service)
10. Main service Heartbeat Failure
11. Orchestrator Conectivity Failure
Edge MCS Service Mastering
12. MCS Service mastering (by its own)
Edge_Services
Edge_Infra
Main_Services
Main_Infra
Monitoring
Orchestrator

Figure 21: Pilot 1 use case 3.2 simplified entities interaction

2.2 Pilot 2: Smart City Edge and Lamp post IoT deployment

The assembly of use cases around the usage of 5G connectivity in urban environments will be the essence of future smart cities. The vertical sector focuses on integrating and demonstrating the advantage of combining different components contributed by the consortium partners in the Smartlamppost (SLP) product. SLP is a commercial solution currently being developed by UBI in a closed consortium of three Portuguese companies. This urban infrastructure is a modular solution (in the form of streetlight pole) able to be equipped with different hardware for specific cities/industry/context needs. The centralised collection and processing of data from the group of Smartlamppost is handled by the Urban Platform (UP). UP provides the seamless integration and standardisation of different kinds of communication protocols and standards. Besides, UP enables the integration of different IoT smart city verticals at the data collection level, processing and analysis based on defined KPIs.

2.2.1 Description and goal of the pilot

This pilot will be used to demonstrate the usage of 5G networks across different verticals contributing to the proliferation of smart cities. Given the market trends and spectrum capabilities, the dissemination of such networks in urban scenarios is being performed by the usage of small cells typically equipped with low-range communication RAN spread across strategic geographic locations within a city, with the purpose of increasing bandwidth and decreasing latency for the evermore demanding verticals. In order to facilitate the distribution of networks and compute resources at the network edge, lamp posts will be used to accommodate physical infrastructures able to provide resources such as the RAN, compute and network capabilities. Figure 22 depicts the general scenario of the pilot, comprising the devices that will connect to small cell, the edge components and the Core components.

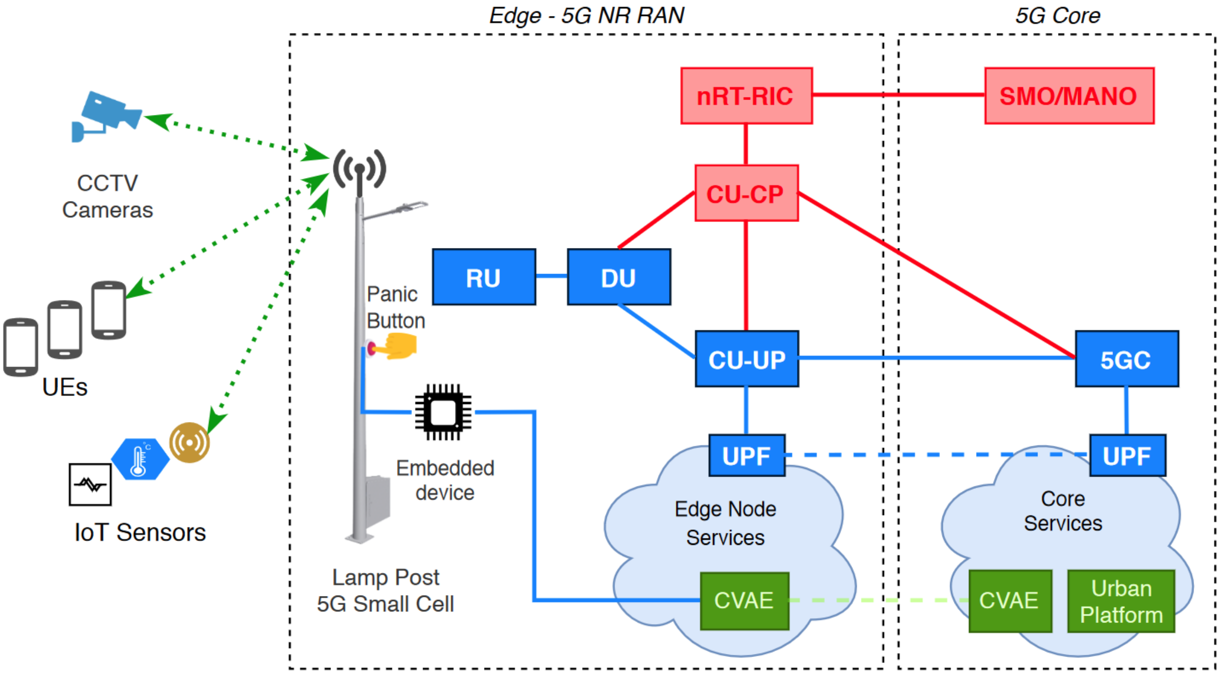

Figure 22: Pilot 2 general scenario

The end-user devices, such as CCTV cameras, User Equipment's (UEs) and IoT devices will connect to the small cell via 5G NR. The lamp posts will be equipped with 5G NR RAN, computing and network resources, which will be all abstracted by a virtualised infrastructure, i.e., virtual RAN (vRAN) and Virtualised Infrastructure Manager (VIM) in order to instantiate services at the edge node. As such, the data fed from the end-user devices flow through the DU and CU, where they can be intercepted and processed by the services running at the edge NFVI. In addition, some lamp posts will have a physical button, namely a Panic Button, which is hardwired to an embedded device with networking capabilities which will be linked to a particular service running at the edge. At the 5G Core a VIM will also be available to ensure the instantiation of NFV services.

To be noted that (although not explicitly depicted in Figure 22) there will be multiple Edge nodes connected to the 5G Core, i.e., multiple lamp posts providing coverage for a certain region/location. Finally, the backhaul between the edges and the core will be assured by a fibre optic cable link.

In the context of the Affordable 5G solution, the resources used in this Pilot will also be provided using a neutral hosting platform, whereas multiple hosted clients, such as Mobile Network Operators (MNOs), public or private operators, will have the ability of deploying their services in the neutral platform. A hosted client is identified as an entity using all or a portion of the resources that are made available by the neutral hosting platform. For instance, a public operator (hosted client), such as a Civil Protection Authority, may choose to lease resources of an edge node, which may comprise the RAN and a portion of the VIM resources, to be able to deploy its services in the premisses of that edge location. The relationship between the hosted client and the neutral hosting platform must follow a commercial agreement/contract that explicitly provides detailed information about the leased resources and service KPIs that must be met according to an SLA.

ACC will provide the RAN control-plane CU-CP and O-RAN aligned near-RT RIC and provide the RAN expertise to integrate into an operational 5G SNPN RAN conformant to 3GPP and O-RAN.

This pilot will be demonstrated at the Castellolí testbed. Currently, the Castellolí testbed has eight auto sustainable (Power microgeneration, no grid connection) sites with six Accelleran small cells that cover a significant part of the 4,5 km circuit radius. Four of the sites has edge nodes (Lenovo SLE350). 24 HD cameras are covering all the track installed in 8 sites. 2 weather stations (Wind speed & direction, temperature, humidity, Rain, irradiation) are installed in 2 different locations. A Sigfox IoT network is covering all the area and 9 HD cameras are ready to be installed inside vehicles.

Castellolí network backhaul connection between the eight sites and the control room is wireless and does not use optical fibre. There are two backhaul options:

- a combination of P2P and P2M topology with limited bandwidth (100Mbps) using free licence spectrum.
- a self-organised Metnet SON mmWave backhaul solution. It is possible to move Small cells and edge nodes to create different scenarios.

The remaining components pertaining Castellolí testbed are same of Pilot 1 and already detailed in the previous section.

For the use cases implementation, Accelleran and RunEl will provide the additional elements, including ORAN that will be used as Neutral Host. Cellnex will also offer hardware for both the Edge NFVI and the Main NFVI.

ATOS NFV NANO interaction with NearbyOne orchestration will extend the multi-PoP NFV MANO management functionalities by splitting the network services allowing hybrid deployments, while, at the same time, running some parts on the edge and other elements on the core.

EURE will provide the RAN user-plane CU-UP and potentially the RAN DU (O-RAN 7.2 IF or nFAPI IF) for the considered pilots. In addition, EURE will provide a complete E2E testbed leveraging open-source OAI and M5G software platforms [39] [52] that includes RAN, CN, RIC, and a range of xApps within the Open5GLab at Eurecom, reproducible by the partners.

I2CAT will provide a multi-RAT non-real-time (non-RT) RIC in line with the O-RAN vision. Specifically, the non-RT RIC will connect to the ACC's near-RT RIC through the A1 interface for coordination and management of the 5G small cells as well as collect and store RAN telemetry. The non-RT RIC will also manage custom Wi-Fi access points via a custom Wi-Fi RAN controller. In addition, I2CAT will provide an infrastructure slice manager and orchestrator able to instantiate slices defined on the radio, the transport, and the compute domains. Additionally, an AI-based component will be deployed to, based on network KPIs, proactively adjust the resources assigned to the slices so that the SLA is maintained by anticipating changes in the resource demand.

MAR has the capability of providing a solution for the Core to Edge Services Deployment and Orchestration, making use of Kubernetes to deploy containerised Services to the Core, and extending it with KubeEdge to handle deployment and Orchestration to the Edge.

NBC also has the capability of providing their NearbyOne solution, that addresses the problem of NFV and Application orchestration both at the Core and Edge of the Network. This solution includes as part of the NFV/App lifecycle, the provisioning and configuration of the edge nodes and core VIM clusters or it can integrate with pre-provisioned clusters at the core or public cloud. NearbyOne solution for Edge Orchestration can be used to automatically deploy, manage, and operate small cells and Edge applications. The solution can take actions based on inputs provided by the edge infrastructure and NFV/Apps KPIs (i.e., sensors, video analytics outputs, etc) to adjust network properties.

THI will provide an FPGA prototype equipped with NEOX accelerator. NEOX is a parallel multicore and multithreaded GPU architecture based on the RISC-V RV64C ISA instruction set with adaptive NoC. Apart from the hardware IP, THI will also utilise the NEOX SDK for optimizing the CNN models in terms of memory footprint and execution time. The SDK also includes a LLVM based compiler. NEOX accelerator will be customised to the CCN models of the vision processing tasks of the project. Prime targets for customization are the number of cores, the number of threads per core, the width of the vector processing lanes and the memory resources (private and shared caches as well as the cache prefetching options). The NEOX multithreading hides long latency delays from external memory controller maintaining high computation throughput for the entire array. NEOX will be provided in a fully functional FPGA prototype based on ZYNQ platforms. ZYNQ FPGAs contain (apart of the FPGA programmable logic) a dual core A9 ARM processor in which a regular Linux operating system has been ported. In this way, the communication of the remaining computational and network components can be performed with standard Linux processes.

UBI will provide one instance of the Urban Platform. The Urban Platform was created with the vision of providing cities with a holistic view of their smart urban environment. Made for cities actively looking to contribute back to those who manage it and to their inhabitants, Ubiwhere started designing and developing several solutions for the demanding challenges that smart cities face (environmental monitoring, energy efficiency, mobility and sustainability, among others).

The Urban Platform will be used for managing smart urban environments, aiming at being integrated with already available systems due to its interoperability layer and open standards compliance. It will be extended to create an ecosystem that promotes the integration of information collected by IoT devices and the assessment of defined KPIs in the project scope, since it is already a solid solution in the market, ready to redefine the industry of Smart Cities, with the ultimate purpose of improving the citizens' quality of life.

Computer Vision Analytics for Emergencies

In this pilot, the aforementioned scenario and features will be showcased by exploring: ***i)*** the potential of 5G video streaming in dense scenarios, and ***ii)*** video processing employing computer vision at the network edge. To tackle these features, Ubiwhere will contribute to the development of a new service, namely the Computer Vision Analytics for Emergencies (CVAE), targeted to be deployed at both the edge and the core of the network. This development of the service will follow a micro-service approach, i.e., composed of multiple VNFs suited to be deployed by the Orchestrator in the form of VMs or containers (still to be defined). In addition, Ubiwhere will also provide the Urban Platform as a service, a geo-located multiple device monitoring platform capable of configuring alerts and provide access to real-time data.

The demonstration of ***i)*** will be performed by the deployment of a dedicated slice for the video transmission in a crowded location (e.g., near a football stadium or a popular race) simulating a significant amount of user equipment units. This scenario will showcase the isolation required between slices to share the infrastructure between different hosted clients. For instance, the MNO that provides 5G connectivity to their users in a dense scenario (e.g., the slice dedicated for a video transmission service to a set of UEs) and another hosted client, specifically a Civil Protection entity, that will receive the transmission of the video and alerts (the slice dedicated to the analysis of uplink video streams).

The demonstration of ***ii)*** will focus on the capability of orchestrating compute resources available at the network edge. The physical enclosure of computing hardware must be suitable for the required computer vision processing power.

Given the mentioned demonstrations, this pilot will be demonstrated using the CVAE service, which is able to detect and identify potential emergency occurrences by the analysis of one or multiple video streams (sourced from CCTV Cameras connected to the edge small cells) based on computer vision software, and that will be deployed in the form of virtualised functions. The specific requirements of such functions will be detailed in their descriptors. The CVAE service will contain different functions following a micro-service paradigm. Moreover, it must be noticed that the CVAE service itself will have a different composition of functions to whether it is instantiated on the core or on the edge of the network. For instance, the CVAE service deployed at the edge will have functions such as video processing analytics and event handler. On the other hand, the CVAE service deployed on the core will provide functions such as correlation of events and objects, storage and information modelling.

Using the CVAE service, two use cases are going to be explored, described as follows.

2.2.1.1 Use Case 1 – Detection and triggering of emergency situations

The main idea behind this use case is based on the triggering of emergency situations at the edge location area. The triggering of emergency situations can be automatic or manual, explained as follows concerning different scenarios.

Scenario 1: Automatic triggering of emergencies

In this scenario, represented in Figure 23, the CVAE service is intended to automatically detect and classify emergency situations by the analysis of video streams using computer vision software, including ML algorithms. The video processing should take place at the edge of the network, exploiting its compute resources, with the purpose of decreasing the backhaul bandwidth usage in the core network and reducing latency of alert transmissions upon emergency event detections. Once an emergency occurrence is detected, an event is generated and sent to CVAE core service and to the monitoring platform, namely the Urban Platform, both deployed at the core network.

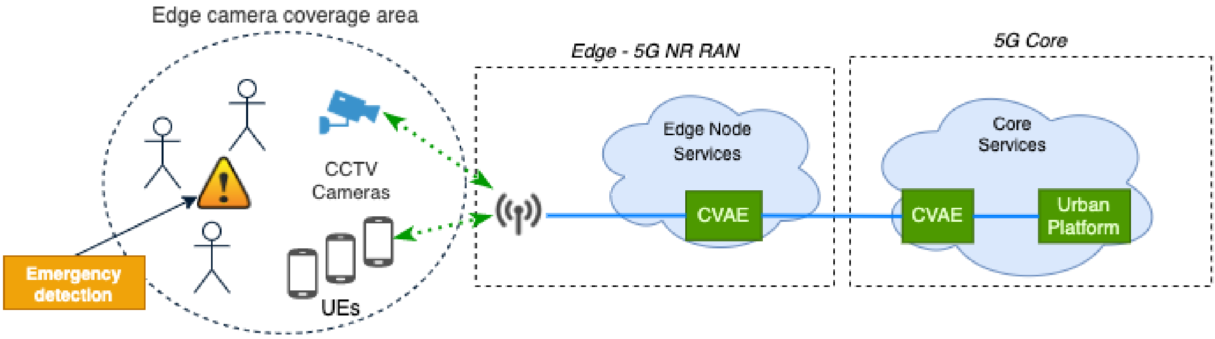

Figure 23: Use Case 1 – Automatic triggering of emergencies

After receiving the automatic event alert of a potentially emergency situation, the Urban Platform operator is able to request a live feed of the origin video stream to assess the situation. In addition, the Urban Platform, deployed at the network core, should also be able to access the recorded images that led to the triggering of the alarm.

Scenario 2: Manual triggering of emergencies

Some lamp posts will have a physical integrated panic button that will provide any user on premises with the ability to trigger an emergency event. The panic button is physically connected to an embedded device (i.e., Raspberry Pi), which will send an event to the CVAE service, instantiated at the edge, which is then responsible to send it to the CVAE service and Urban Platform services at the core.

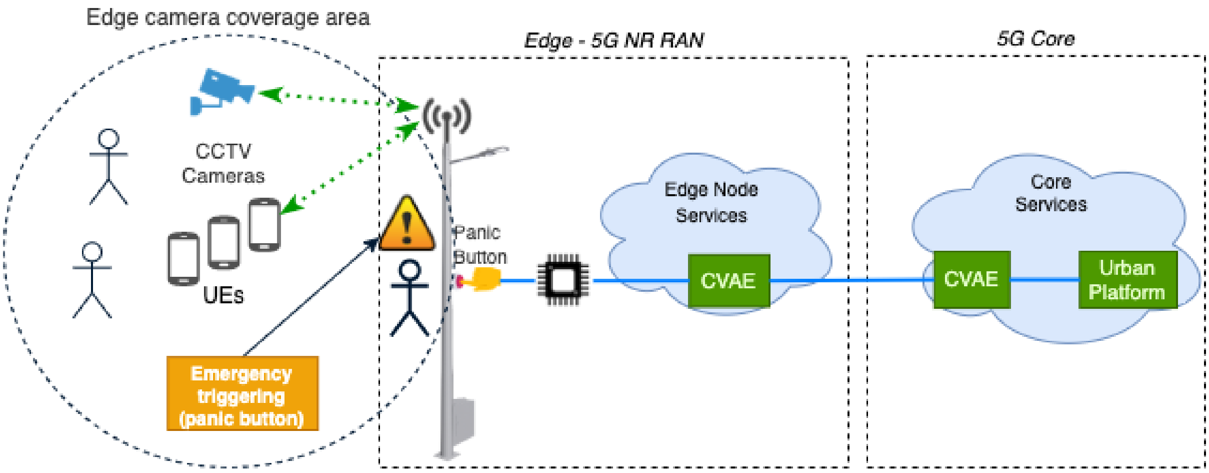

Figure 24: Use Case 2 – Manual triggering of emergencies

After receiving a manual trigger of an emergency situation, the Urban Platform operator is able to open live video feeds to the nearest cameras on the edge premises.

2.2.1.2 Use Case 2 – Tracking of actors

This use case addresses the tracking of actors, namely objects, vehicles and people across different edge domains, with the main purpose of providing the real-time location of a potentially hazardous object and/or person.

Once a potentially hazardous or emergency situation is detected by a particular edge node, the service classifies the actors that are included in the images that triggered the emergency event. The classification and isolation of each actor (object, vehicle, person) is transmitted to the CVAE service at the core of the network. This information is stored at the core and can be later used to positively identify the same actors across different edge domains by using computer vision image correlation algorithms.

Despite the possibility of retrieving the UE location, e.g., by means of the 3GPP Location Services (LCS), it is not guaranteed that the person (or persons) that generated the emergency event are constantly carrying the UE. Thus, this solution is primarily based on the classification and identification of actors by means of computer vision machine learning algorithms.

This use case aims at identifying three different types of actors, traversing between different edge domains, as depicted in Figure 25.

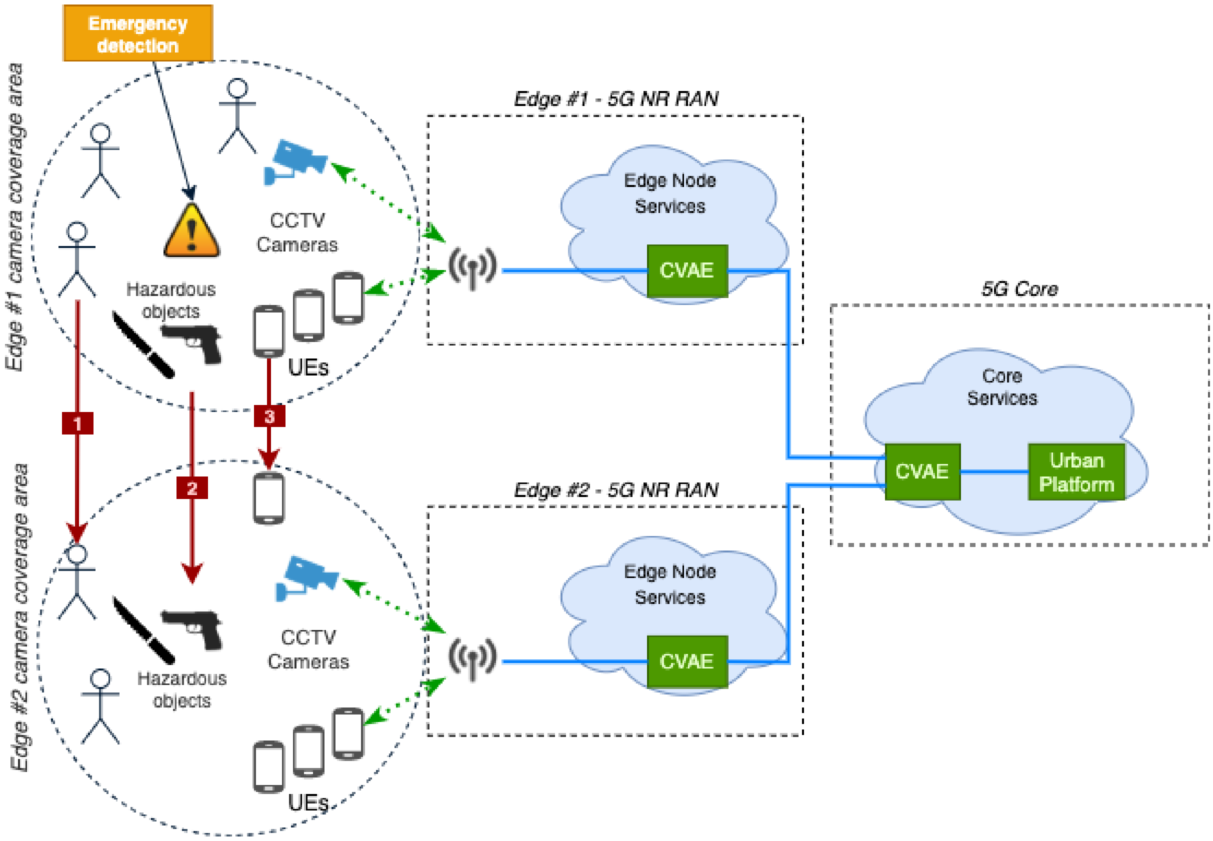

Figure 25: Use Case 2 – Tracking of actors

Several examples of the tracking of actors are described as follows:

1 – Locating the UE is made possible by the accessing the 3GPP Location Services.

2 – A potentially hazardous object is detected by a CCTV camera connected to a small cell of an edge domain. The change of location of that object is possible to be detected once it is again detected and identified in a CCTV camera connected to a different edge domain.

3 – Similarly to hazardous objects, the detection and identification of people can also be done, this time through face recognition algorithms.

It is worth noticing that most of the time the reliability of detection and identification of actors travelling between different edges is not entirely accurate. For instance, a UE carried in an edge by a person A may be in possession of person B in a different edge. The same applies to objects. And, naturally, a person that was captured in the images that triggered the emergency event may be completely irrelevant (i.e., innocent) in what regards to the emergency event. However, the correlation (multiple cross-referenced detections) of the different actors will significantly increase the probability of identifying the correct location of the person that sourced the emergency event. The correlation engine will be running at the CVAE service in the network core in order to correlate information sourced by multiple edges.

2.2.2 Entities/resources involved in the pilot

Neutral Hosting platform

Hosted clients, such as MNOs, Civil Protection entities or other private operators, will be able to lease the neutral host to supply their services at the network edge. As such, the permanent physical infrastructures, such as lamp posts, will be able to provide entry points for services from multiple hosted clients.

The relationship between the neutral hosting platform and the hosted clients must comply with a technical formal Service Level Agreement (SLA) detailed when the contract is sealed. For instance, let us assume that an MNO wishes to provide one or multiple services at some location where a lamppost is installed. A contract specifying the terms and the type and amount of resources must be signed between the MNO and the neutral hosting platform. Furthermore, with the intent to provide service isolation, one or multiple slices should be allocated to the MNO on top of which the services will be instantiated.

Service Management, Orchestration and Slicing

A MANO platform deployed at the edge of the network will be required for the onboarding, instantiation and lifecycle management of the services required for this pilot. Upon the instantiation of a service, the orchestrator should be able to identify the required resources for the service and allocate a slice to accommodate such service.

The management system is also expected to feature an infrastructure slice manager that will bind together slices defined on the radio, the transport and the compute domains to allow Mobile Network Operators (MNOs) to seamlessly control and orchestrate services for different verticals. Each slice is given by a specific SLA related to the Quality of Service (QoS) policy, including networking and computing resources. The slice manager will be responsible for the slice's lifecycle management in an end-to-end fashion.

Additionally, since the services are transversal from the core to the edge of the network, i.e., are composed by virtual functions (VNFs) that are running on the core network (Urban Platform) as well as MEC applications running at the edge (Computer Vision Analytics Processor, Emergency Event Handler and video transmissions for events), an end-to-end orchestrator is required with the ability of instantiating slices and services that extend from the core to the edge of the network (including NFVs like the Packet Core and RAN controllers) as well as managing the services' lifecycle.

2.2.3 Interactions among entities

In this section we divide the interactions related to the management of the platform and instantiation, namely the Service-management interactions, and the functional interactions of the service itself, namely the Service-functional interactions.

Lease of neutral host

To lease resources on the Neutral Hosting platform, a hosted client (e.g. MNO, private operator) must follow the steps stated in the diagram (Figure 26). The Neutral Hosting platform must agree with the SLA and ensure the availability of the resources at the VIM of the edge before allocating the resources to the hosted client.

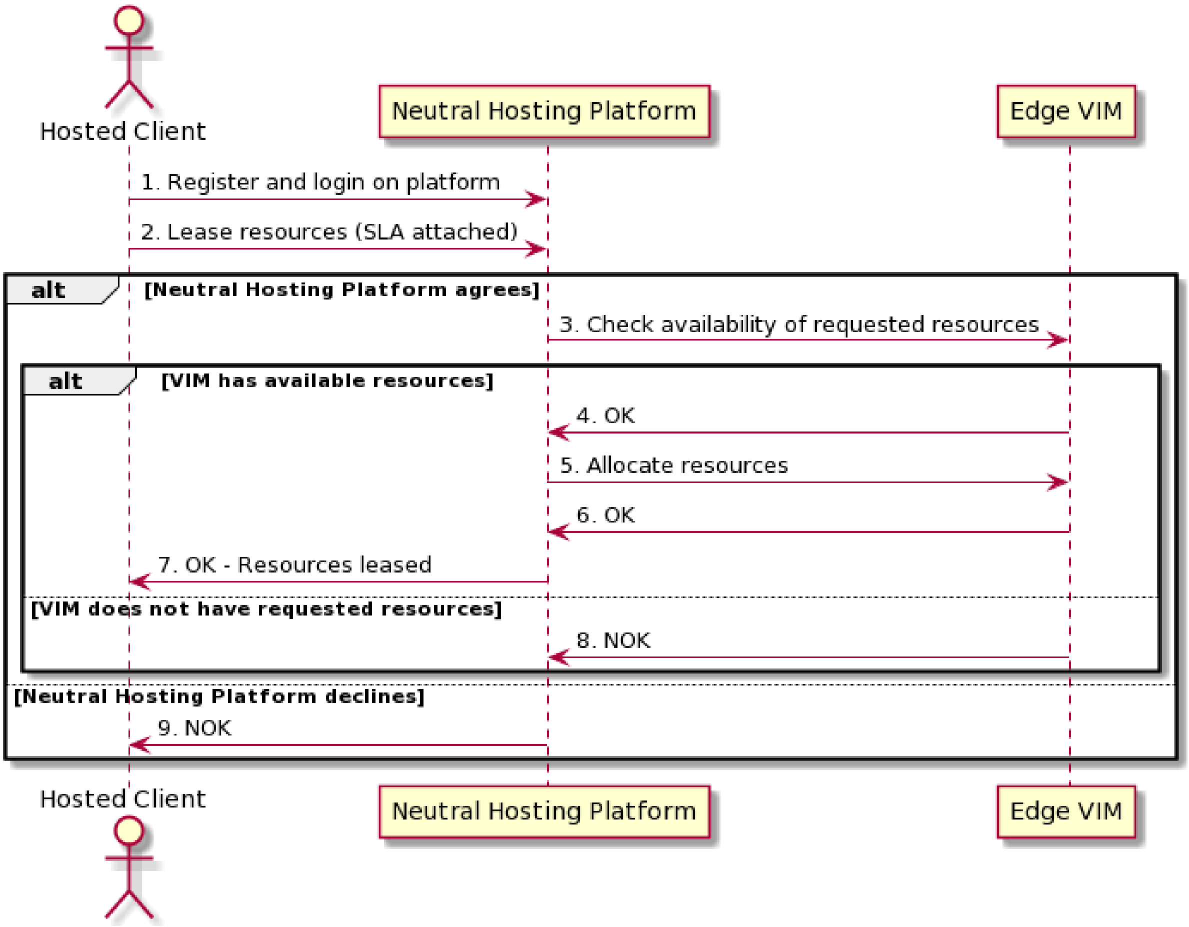
Hosted Client
Neutral Hosting Platform
Edge VIM
1. Register and login on platform
2. Lease resources (SLA attached)
alt
[Neutral Hosting Platform agrees]
3. Check availability of requested resources
alt
[VIM has available resources]
4. OK
5. Allocate resources
6. OK
7. OK - Resources leased
[VIM does not have requested resources]
8. NOK
[Neutral Hosting Platform declines]
9. NOK
Hosted Client
Neutral Hosting Platform
Edge VIM

Figure 26: Lease resources on the Neutral Hosting platform

<u>Onboarding and Instantiation of a Service</u>

The Network Service (NS) onboarding and instantiation is performed following the steps depicted in the diagram (Figure 27). Although not detailed in the diagram, after the ordering of the platform to instantiate a NS, the VIM must ensure that the resources being allocated to the service do not exceed the negotiated terms (SLA) with the hosted client.

After a NS is instantiated, the hosted client should be able to assess KPIs related to the instantiated service.

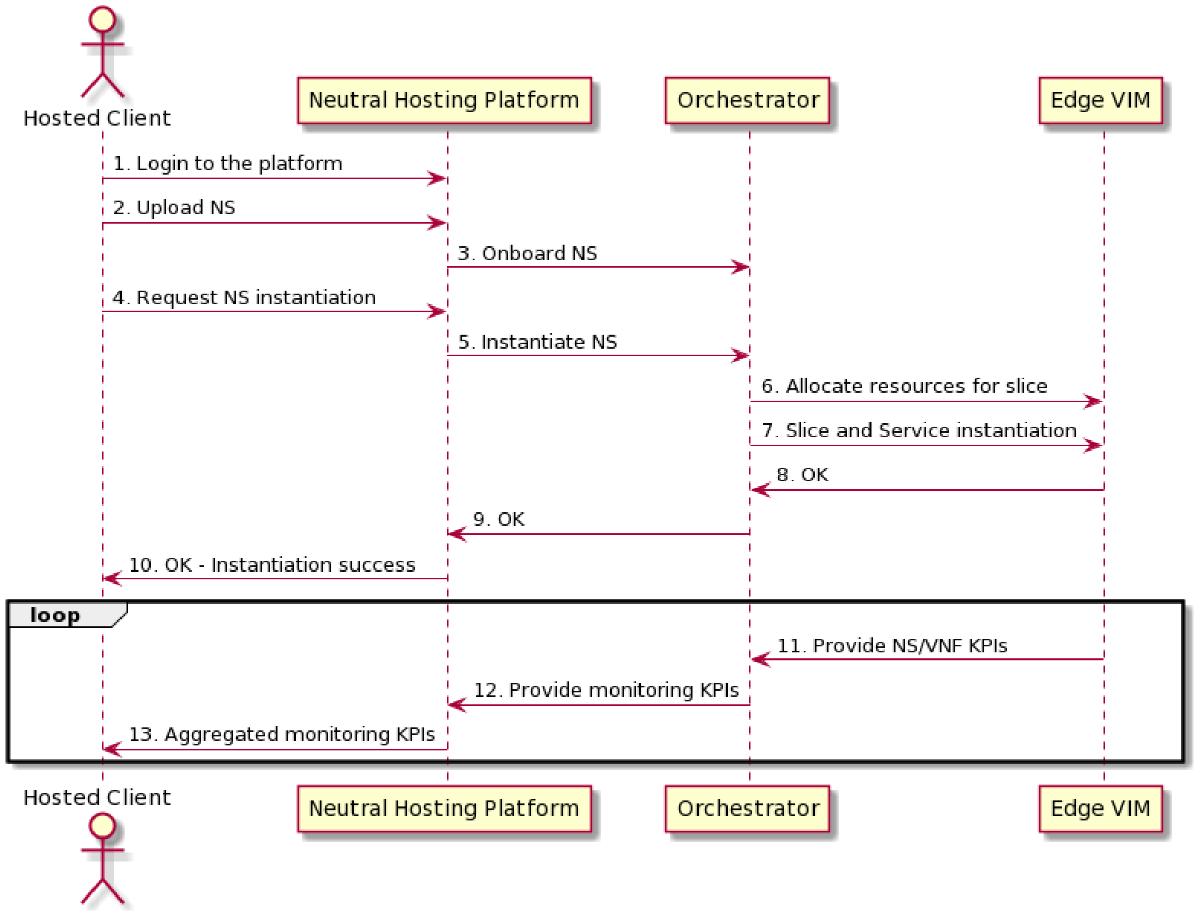
Hosted Client
Neutral Hosting Platform
Orchestrator
Edge VIM
1. Login to the platform
2. Upload NS
3. Onboard NS
4. Request NS instantiation
5. Instantiate NS
6. Allocate resources for slice
7. Slice and Service instantiation
8. OK
9. OK
10. OK - Instantiation success
loop
11. Provide NS/VNF KPIs
12. Provide monitoring KPIs
13. Aggregated monitoring KPIs

Figure 27: Network Service onboarding and instantiation

2.2.3.1 Service-functional interactions

UC1: Detection and triggering of emergency situations

Depending on whether the triggering of emergencies is automatic or manual, the interactions between entities will be slightly different, as discussed below.

Automatic triggering of emergencies

The following sequence diagram (Figure 28) represents the high-level interactions between parties upon an automatic detection of an emergency event using computer vision software. The general rationale is having one or multiple real-time video streams fed to the CVAE service executing at the network edge, which is continuously processing the images aiming to detect emergency occurrences using ML algorithms. When such occurrences are detected, it reports the event to the CVAE service running at the core, which may be forwarded to the Urban Platform monitoring centre. At this point, some decisions can be done by the operator, namely the analysis of the real-time video feed, the analysis of the video recording that originated the emergency event and the ordering of dispatch to emergency authorities.

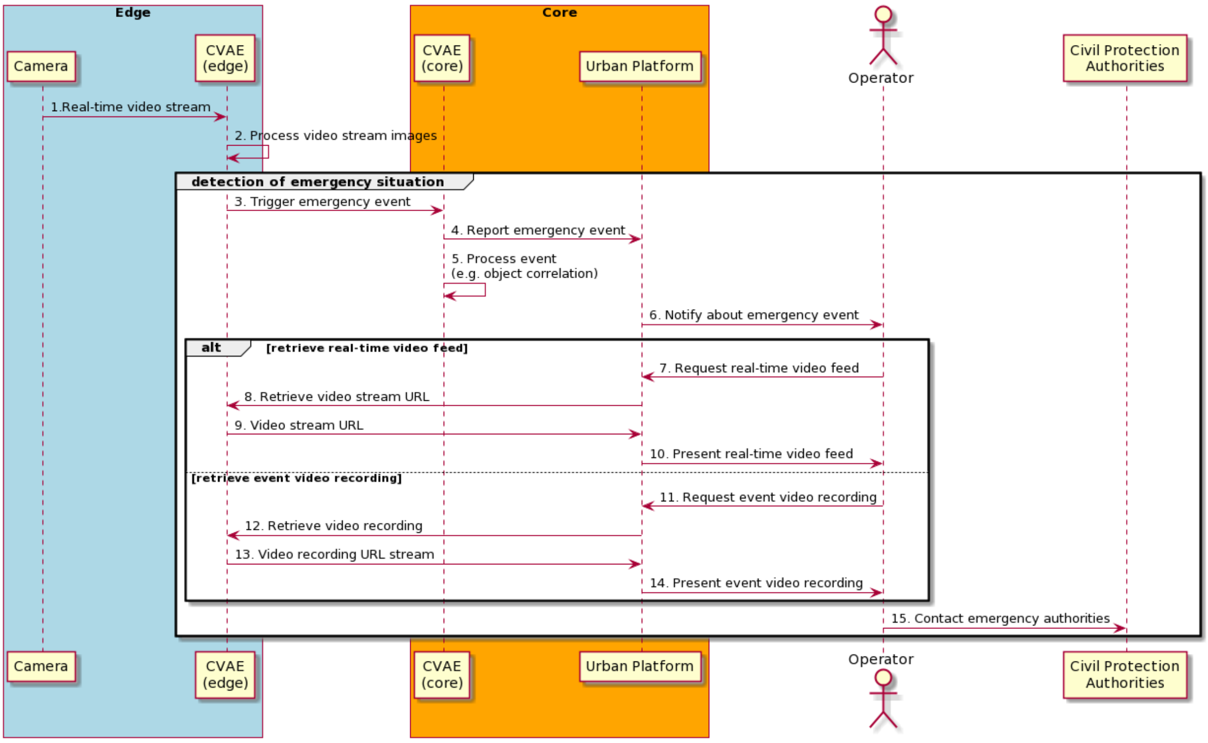
Edge
Core
Camera
CVAE (edge)
CVAE (core)
Urban Platform
Operator
Civil Protection Authorities
1.Real-time video stream
2. Process video stream images
detection of emergency situation
3. Trigger emergency event
4. Report emergency event
5. Process event (e.g. object correlation)
6. Notify about emergency event
alt
[retrieve real-time video feed]
7. Request real-time video feed
8. Retrieve video stream URL
9. Video stream URL
10. Present real-time video feed
[retrieve event video recording]
11. Request event video recording
12. Retrieve video recording
13. Video recording URL stream
14. Present event video recording
15. Contact emergency authorities

Figure 28: Automatic detection - high-level interactions

Manual triggering of emergencies

Some lampposts will have a physical panic button which that can be pushed by any citizen in need of assistance. Unlike the previous scenario, the emergency event triggering is done manually by the push of a button which will trigger a chain of events as depicted in the Figure 29. In this scenario, the Operator has also the responsibility of deciding if the reported emergency event is valid. To that end, it also needs to access the real-time video feed from the scene and also the video recording that took place from the time since the moment the button was activated.

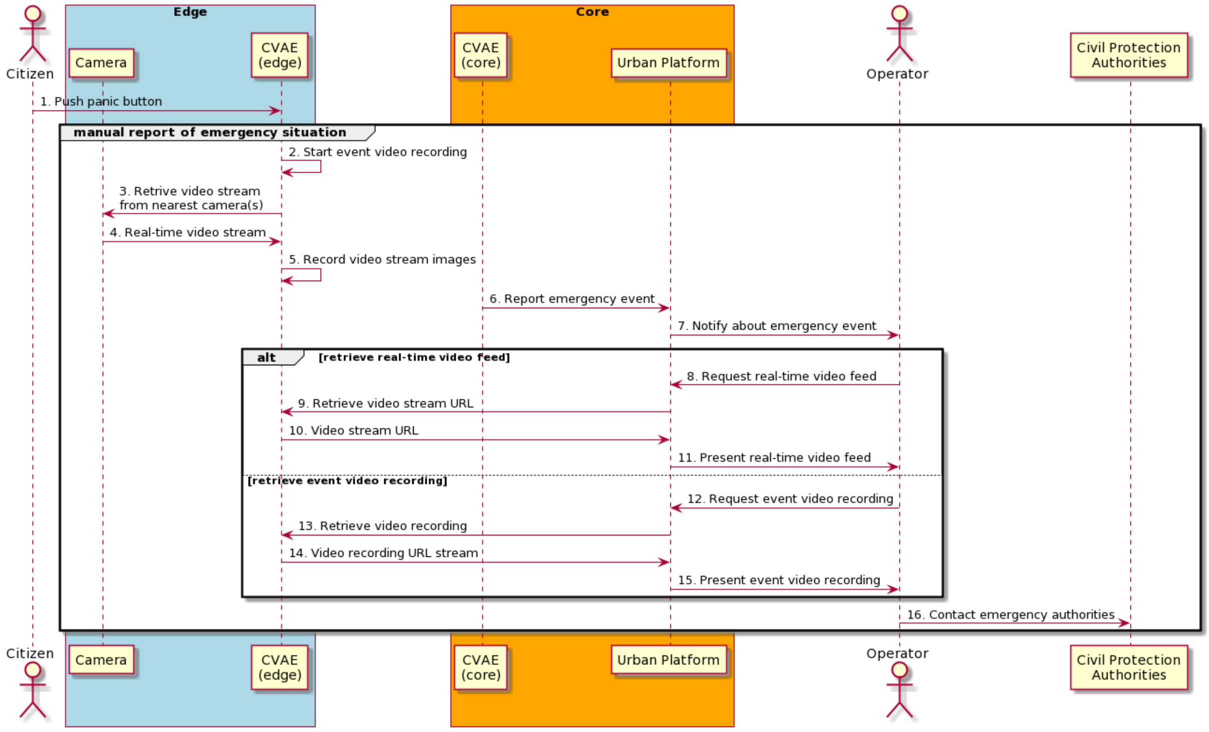
Edge
Core
Citizen
Camera
CVAE (edge)
CVAE (core)
Urban Platform
Operator
Civil Protection Authorities
1. Push panic button
manual report of emergency situation
2. Start event video recording
3. Retrive video stream from nearest camera(s)
4. Real-time video stream
5. Record video stream images
6. Report emergency event
7. Notify about emergency event
alt
[retrieve real-time video feed]
8. Request real-time video feed
9. Retrieve video stream URL
10. Video stream URL
11. Present real-time video feed
[retrieve event video recording]
12. Request event video recording
13. Retrieve video recording
14. Video recording URL stream
15. Present event video recording
16. Contact emergency authorities
Citizen
Camera
CVAE (edge)
CVAE (core)
Urban Platform
Operator
Civil Protection Authorities

Figure 29: Manual triggering steps

UC2: Tracking of targets

The following sequence diagram in Figure 30 represents an example of interactions between two different edges and the core network. Upon the triggering of an emergency event by the CVAE service executing at Edge #1, the CVAE core service will proceed with the already described actions but with an additional action, the dissemination of isolated actors to neighbour edges (step 6). This information may include actor images as well as their partial fingerprints, which will provide vital information for a different edge to be able to positively identify the same actor. If, and upon, the detection of such actor in Edge #2 an emergency event is triggered to the core, similarly to the initial emergency trigger. However, the correlation engine at the core (in this example) will identify that the actor is now located at Edge #2 and will immediately transmit this information to the Urban Platform in order to provide the ability of actor tracking.

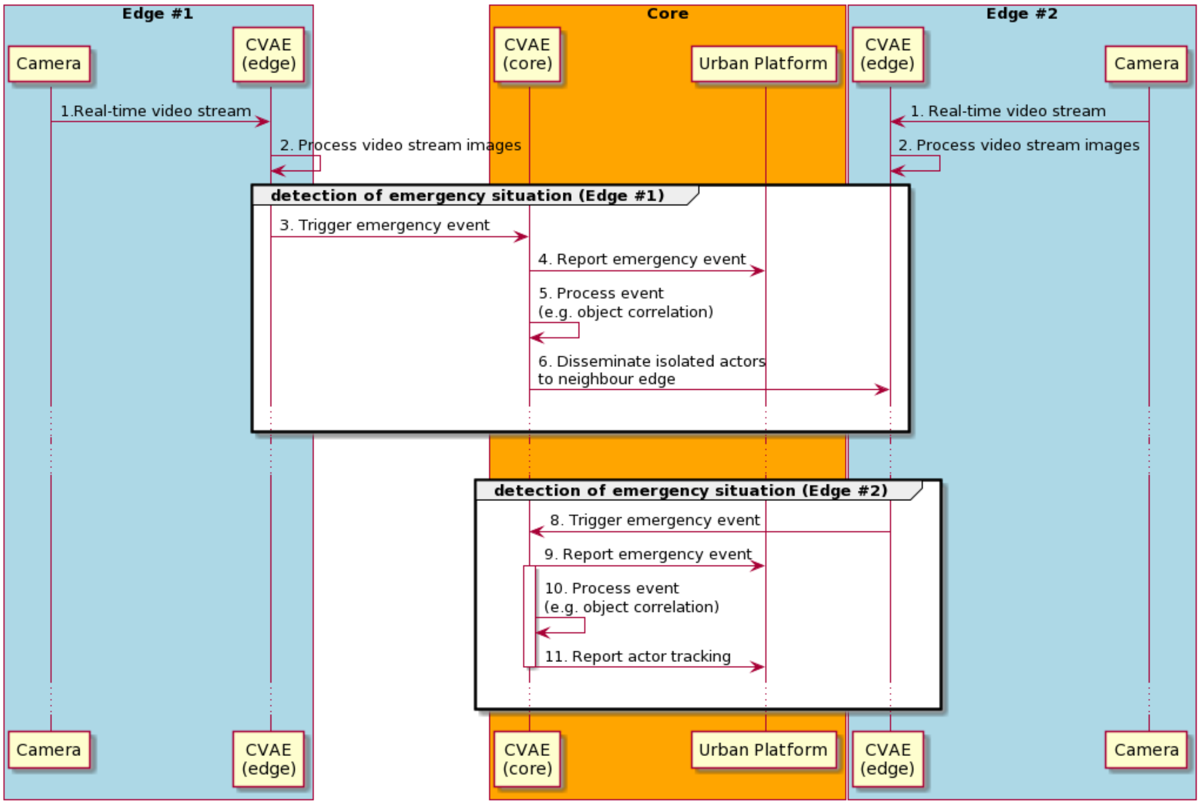
Edge #1
Core
Edge #2
Camera
CVAE (edge)
CVAE (core)
Urban Platform
CVAE (edge)
Camera
1.Real-time video stream
2. Process video stream images
1. Real-time video stream
2. Process video stream images
detection of emergency situation (Edge #1)
3. Trigger emergency event
4. Report emergency event
5. Process event (e.g. object correlation)
6. Disseminate isolated actors to neighbour edge
detection of emergency situation (Edge #2)
8. Trigger emergency event
9. Report emergency event
10. Process event (e.g. object correlation)
11. Report actor tracking
Camera
CVAE (edge)
CVAE (core)
Urban Platform
CVAE (edge)
Camera

Figure 30: Interactions between two edges and the core network

2.2.3.2 HW and SW Components of the Video Analytics Processing / Vision Processing Functionality

The various configuration possibilities of the NEOX IP of THI with custom user instructions, make it flexible to configure key applications such as computer graphics, machine learning, vision/video processing and general-purpose compute. In the context of the project, the NEOX will be mainly used for accelerating the inference part of the CNN models. We will assume that the network training has been happened offline in a cloud-based system. However, since the NEOX SDK will also include an online compiler, the CNN model can be updated periodically. The possibility to make this update on-the-fly (online – without taking down the service) is still being assessed.

The input to the NEOX SDK will be a CNN model provided in an industry standard format e.g., ONNX format. By using an ONNX format, the training and inference parts are actually decoupled i.e., the CNN training can be performed in any well- known framework, while the inference tasks will be based on the deployment engine of THI (that is based on Tensorflow lite for MCUs).

When the CNN-based vision application development is finalised, an important part is to define an appropriate loss function (in terms of frame per second - fps, color depth, color channels, etc.) that is aligned with the specifications of the use cases. The loss function will allow us to employ several optimizations, like model compression/quantization/pruning (part of NEOX SDK), that eventually will enable high performance and low power execution of the inference part.

2.3 Pilot 3: Industrial manufacturing private network

In the initial DoA (Description of Action) of Affordable5G, only the first two pilots were originally defined, along with their implementation plan and procedures. However, at the beginning of the project, the consortium decided that it would be interesting to elaborate an additional third pilot with two deployment scenarios, in the area of industrial and manufacturing environments. In this context, the application of IIoT and related technologies are highly boosted by the deployment of private 5G networks, since timing synchronization among various and diverse procedures along with the provision of zero latency applications are of utmost importance. To this end, as it will be presented in the following sections, two relevant deployment scenarios were selected and described: 1) Management of Autonomous Mobile Robots in construction industry and 2) Sensors deployment in printing facilities. In this pilot, the entities and interactions are described per deployment scenario.

The consortium will assess and decide according to available resources and in agreement with European Commission, the capability to implement and demonstrate some of these deployment scenarios. In any case, the requirements derived from these two scenarios will be taken into consideration towards the definition of the system architecture of the Affordable5G. As initial assessment, this is considered highly beneficial for the technical developments and overall project outcomes, both from a technical, as well as a dissemination and exploitation viewpoint.

2.3.1 Description and goal of the pilot

Manufacturing sector is an indispensable part of the industrial ecosystem of European Union (EU) that is expected to benefit from the innovations introduced in the 5G System and those related to Non-Public Networks (or Private 5G Networks).

The importance of manufacturing in the EU society can be easily realised by the fact that manufacturing contributes around 15% of gross value added (GVA) of the European industry and 40% of EU exports, accounting also for nearly 65% of the total R&D activities of EU companies [53].

Thus, even though manufacturing pilot was not explicitly covered by the time of proposal writing, it remains a critical industrial vertical sector whose requirements must be taken into consideration by the Affordable5G architecture and implementation. In this respect, the consortium decided to analyse and include deployment scenarios from the manufacturing domain that would drive development and innovation on specific parts across the latest 5G System, in accordance to the services specified in the latest Releases (15, 16) of 3GPP.

It is also highlighted that the importance of the vertical domain of the so-called Factory of the Future (FoF) can be judged from the plethora of different documents dealing not only with architectural enhancements related to FoF-related characteristics and services, but also dedicated sections describing use cases, requirements, etc.

Some of the most important 3GPP documents include:

- TR 38.825 that describes NR enhancements to Ultra Reliable Low Latency Communications (URLLC) and Industrial Internet of Things (IIoT);
- TR 21.915 and TR 21.916 that include Work Items related to FoF support as part of Release 15 and 16, respectively;
- TR 22.804 dealing with communications aspects for automation in vertical domain, where a section is dedicated solely to the description of FoF use cases and relevant requirements;

- TS 23.501 and TS 23.502 that provide information on TSN aspects that are considered as an important area of contribution for Affordable5G;
- TS 29.244 that provides specifications on the interfaces used among functions for supporting the TSN concept;
- TR 22.821 that deals with issues related to Feasibility Study on LAN Support in 5G.

Apart from the dedicated documents within the 3GPP constellation, other communities provide useful information on use cases and requirements stemming from real world manufacturing sites, such as those provided by 5G-ACIA:

- Exposure of 5G Capabilities for Connected Industries and Automation Applications transportation [4]
- Integration of Industrial Ethernet Networks with 5G Networks transportation (5G-AGIA, 2019)

In this context, this pilot consists of two use cases covering different parts of the manufacturing process and describes different aspects that must be taken into account for an efficient and functional optimization of all related procedures.

The first use case is dedicated to the benefits arising from the introduction of the TSN concept to manage Autonomous Mobile Robots (AMRs) within a construction site. AMRs move flexibly in a hostile environment such as construction site, recognizing and avoiding obstacles at high safety levels and are easily reprogrammable. This allows AMR movement inside the whole construction in order to perform daily or specific actions. The use of the AMR for construction are quite useful because some jobs for humans can be avoided, the system can work around people and machines at high levels of safety and reduce labour needs. In addition, accident risks are reduced by avoiding risky jobs or heavy tools transport. AMRs need to trade-off operational efficiency (uptime, speed, accuracy) with safety while achieving their aim inside the construction.

We consider a construction company that owns a few AMRs connected to a network infrastructure that allows some work to be carried out by company engineers for safety and efficiency, and the AMR supplier for maintenance. Although the system is operational, the company has identified a major challenge that limits its full exploitation in their processes, related to the access to areas not reachable by the AMR. The company seeks a solution that adapts to the activities carried out in construction without tedious (re)programming. The AMRs are mostly individual units that plan isolated trajectories, sometimes blocked for an obstacle. This results in missed actions deadlines and stalling of needed results for continuing the work progress. In addition, AMRs are currently unable to recover from system errors and failures internal or external to the AMR, for instance, while positioning at difficult area access or driving with a worn wheel. This results in delays and loss of efficiency and the complexity increases with every new AMR added to the network.

The second use case deals with Process Automation. Since the development and deployment of Factories of the Future (FoF) is inextricably connected with advances in the related fields of wireless mobile communications as well as Internet of Things (IoT) technology, the automation of various procedures, critical for the overall system operation can be supported with advanced wireless features, such as the deployment of 5G mobile networks. To this end, increased data rates and the support of zero latency applications facilitates various aspects of the production procedure.

Large manufacturing companies may have dispersed production units in a territory. In the majority of involved cases, prior to the final production, various intermediate steps have to be included, namely: requirements on demand, feasibility analysis, first materials preparation, intermediate control tests, final production. Even a single failure in one of the above steps may result in product failure and related losses. Hence, product quality should be controlled throughout the production procedure, in order to minimise as much as possible potential failures. In cases of malfunction of a certain production component, feedback to the production unit should be immediate in order to pause all other related procedures.

In addition, this information should also propagate to other production units in order to avoid similar circumstances. In this context, a typical example includes companies in the printing sector since the printing process is quite complex and often requires manual interventions from the personnel. Defects along the manufacturing process have a major impact on the company's financial losses. Therefore, rapid decisions based on immediate feedback are of utmost importance in such a complex environment.

Sensors facilitate the complex task of monitoring an industrial environment to detect malfunctioning and broken elements in the surrounding environment. An appropriate detection approach along with a classification of the anomaly can help choosing a countermeasure or proper action to take in case of predictive maintenance.

2.3.1.1 Deployment scenario 1: Management of Autonomous Mobile Robots in construction industry

We assume one engineer in charge of a large construction site. This construction site has, at least, a control centre where the engineer will control several autonomous mobile robots (AMR) with the ability of performing different actions compliant with TSN requirements. This deployment scenario is based on a private 5G network deployed in a scenario that corresponds to a hostile environment such as a construction site.

The whole architecture is depicted in Figure 31. The left part of the figure (in blue) represents the AMR(s). One AMR will be able to support all elements represented above of itself, such as one or more TSN end stations, an IEEE TSN switch if is necessary and one or more 5G UE with the corresponding TS. In the middle of the figure, known as 5G TSN bridge, there are the gNB (potentially composed by RRH + DRAN + CU) and the edge computing platform to support the 5G core and highlighted the AF responsible of the TSN requirements fulfilment beside a module for learning and network reconfiguration. The modified UPF performs as a translator between 5G network and TSN domain.

The right part of the figure corresponds to the engineer's control centre, composed of CNC+CUC for controlling the TSN deterministic communication, a gPTP server performing as clock grand master for TSN domain. At least, an IEEE TSN switch and one or more TSN end station, since there may be more than one engineer/control centre, this TSN end station is used as a checkpoint or tracking point, where the engineer is able to have a remote control of the AMR. The rack with the required servers for performing the actions above described can be inside a cubicle of the construction site, the gNB can be on the roof of this cubicle.

2.3.1.2 Management of Autonomous Mobile Robots - scenarios

The engineer responsible of the construction site must perform some inspections of different points of the construction.

The engineer, using the checkpoint in the construction site cubicle, gains access to the system, activates the application and performs the daily routine inspection with the AMR. The first part of the daily routine consists of the AMR movement from point A to point B, then a picture will be taken, or a video will be recorded. After that, the picture or the video will be sent to a server located in the cubicle. The second part consists of the movement of tools daily used in the construction site from point C to point D.

The engineer, once per week needs to perform two special inspections. The first special inspection consists of the AMR movement from point A to point B in order to collect a sample using the AMR arm. Once the sample is taken, it will be analysed and returned to the cubicle if at least one parameter is not within the established thresholds. The second special inspection consists of the AMR movement from point C to point D for specific jobs. For instance, the application of a substance that is especially harmful to humans, as anticorrosive for a path or to terminate a weld in a difficult-to-access point using the AMR arm.

2.3.1.3 Entities/resources involved in the deployment scenario

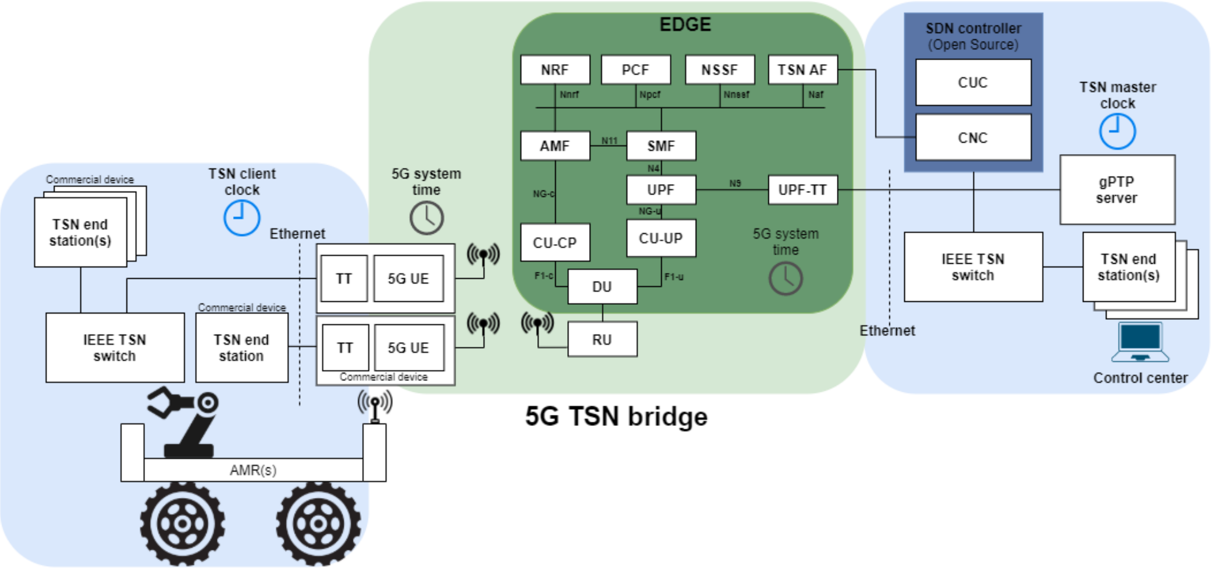

Figure 31: Proposed architectural approach for the 1st use case of the 3rd pilot

This deployment scenario requires the combination of 5G and TSN technologies following the 3GPPP 5G TSN Bridge recommendations. To this aim, the following elements are required:

At the application level, the main hardware elements are the AMRs and the equipment on board of the AMR (cameras, LIDARs, arms, etc.). All the equipment is TSN devices connected to the 5G UE with a TSN switch. For the pilot, the AMR and onboarded equipment will be commercial products, as well as the 5G UE (provided by UMA). The project will enhance ADVA TSN switches to be connected to the 5G UE using the appropriate translators defined by 3GPP. Such translators will be provided by UMA.

For TSN timing domain ADVA will provide the gPTP grandmaster, based on its enhanced version of commercial product *OSA 5405*.

OSA 5405 family comprises both indoor and outdoor variants, including GNSS antenna with integrated receiver.

Since the deployment of gNB might be GNSS-less environment, an additional OSA 5405 will be used as a PTP grandmaster in 5G fronthaul timing domain (O-RU and O-DU).

ADVA TSN switch is based on commercial FSP 150 family. FSP 150 family is FPGA-based, so the initial version with strict priority scheduler will be enhanced by implementing a frame preemption feature for the expedited traffic (802.1Qbu). A novel method for correcting packet delay variation (PDV) of high priority express traffic will be evaluated for adoption in company's TSN products.

ADVA will also provide an enhanced version of *Ensemble Sync Director* software for management and assurance of synchronization quality in both TSN and 5G domains.

The software at the application level, including the engineer front end and the AF, will be adapted, and enhanced from some initial version from commercial or open source (to be identified).

The RAN, originating from different sources, will be enhanced and configured to support TSN requirements in terms of latency and stability. Three different configurations are expected. The 5G emulator available at UMA will be used for first integration and testing. Then, the UMA field 5G deployment will be used for first trials. Finally, the new RAN solution provided in Affordable5G will be used for the final demonstration. This solution will be composed by the remote unit (RU) provided and enhanced by RunEL, the Distributed Unit (DU) developed based on the current solutions by Eurecom and/or RunEL, the Control Unit data (CU-UP) plane by Eurecom, the Control Unit control plane (CU-CP), the O-RAN aligned RIC (RAN Intelligent Controller) near-RT RIC by Accelleran & non-RT RIC by i2CAT as well as by Eurecom.

The 5G core for this deployment scenario will be provided by Athonet. It will implement 5G standalone (SA) features as per 3GPP specifications. Moreover, it will support the ability to deploy part (or the whole) core in the edge plus location support in collaboration with the RAN. The 5GC NFs will exchange monitoring information with the NWDAF module implemented by NKUA to implement machine learning approaches for optimization purposes of the tasks and procedures performed in the industrial environment under consideration (e.g. production quality improvement, minimization of delivery times, etc).

As for the backhaul network, UMA will use its network. UMA will also provide hardware for the Edge NFVI.

2.3.1.4 Interaction of the elements

Three diagrams are presented in this section in order to show the interactions among the system entities at specific times. In Figure 32, a diagram with the initialization process is shown, which contains the first interaction when the AMR are on. The UE on board of the AMR establishes the connection with the gNB, and gNB performs all the message exchange necessary for connection to the network. Once connected to the network the engineer through control end station is able to manage the AMR remotely.

Figure 33 presents a diagram of one of the most important interactions in the system, the time synchronization. This is fundamental in order to use 5G system as a logical bridge within TSN domain. The gPTP server acts as master clock and it is in charge of the time synchronization control with the appropriate entities, in this case CNC,CUC and UPF_TT in the 5G core directly, and TT_UE and AF_TT in the 5G core indirectly.

The last diagram shown in Figure 34 depicts the exchange messages when the engineer performs a remote action to the AMR using the control end station. In this case, the control end station communicates with the AF_app in the 5G core that is able to carry out some predefined actions. The connection between the AF and the AMR is established going through the 5G core, the gNB and the 5G UE; this connection will be used to exchange the corresponding messages to indicate the action chosen by the engineer. The AMR responds using reverse connection path and the engineer gets the results using the control end station.

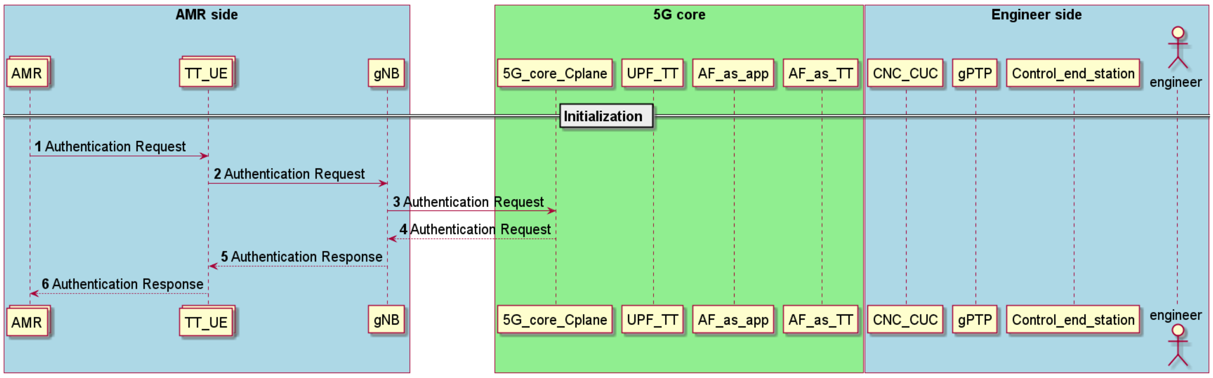

Figure 32: Proposed UML diagram for the 1st use case of the 3rd pilot; initialization

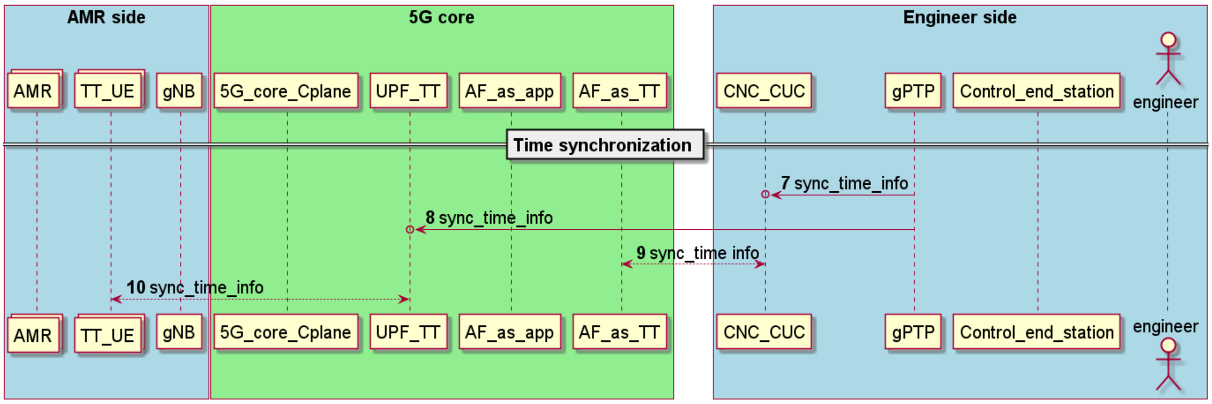

Figure 33: Proposed UML diagram for the 1st use case of the 3rd pilot; time synchronization

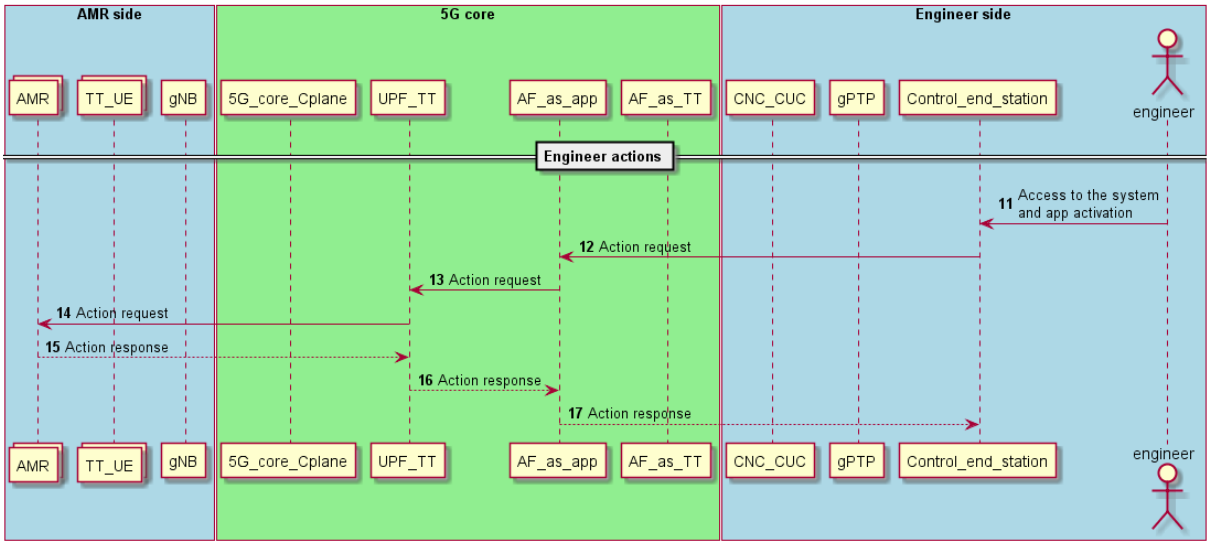

Figure 34: Proposed UML diagram for the 1st use case of the 3rd pilot; engineer actions

2.3.1.5 Deployment Scenario 2: Sensors deployment in printing facilities

This deployment scenario focuses on the requirements of the product manager in an assembly line of a small or medium enterprise. Its main responsibilities include, among others, supervision of the overall process to ensure that all products are delivered on time to the subscribed customers or intermediate companies, as well as quality control check to ensure minimization of potential failures. For this reason, a sensor network has been deployed within the factory premises, that can measure, and report critical parameters related to the overall manufacturing process. These parameters may include, among others, machine temperature (for example, in cases of overheating, severe damages may occur), time of delivery of certain products, as well as advanced features such as object scanning and transmission of either 2D or 3D images to a central processor. These images are post processed with predefined templates of products meeting all specified requirements, in order to ensure that there are no pattern anomalies. In case that such an anomaly is detected, all components in the specific manufacturing line suspend their operation. However, there can be certain cases, such as the printing of brochures, where delay among the detection of the anomaly and production termination should be minimised (zero latency requirement). In this case, edge computing is supported in the sensor nodes, in order to process related metadata on the spot.

Note that in typical manufacturing cases and environments, the production line manager would have to be on the spot of one of numerous production lines and randomly select either final products or intermediate ones. Afterwards, the manager would have to examine the quality of the selected product (possibly in a completely different location), a fact that may result in substantial time spending (for example, in a typical printing procedure, output image processing is performed via spectrography, which is a time-consuming operation). Hence, the automation of such a procedure is expected to significantly reduce overall production times and occurred anomalies, and to minimise profit losses.

The interconnection of sensors in the production line with the central processing unit (CPU) can be made feasible via Ethernet cables. However, a major disadvantage of such an approach is that changes in the overall production chain would also require major modifications in the wired topology. Therefore, an alternate solution would be the wireless communication of sensors with the CPU. Although a public infrastructure can be used, private 5G networks ensure high bandwidth availability on demand (i.e. transmission of high-resolution images from the sensors) as well as latency minimization.

2.3.1.6 Entities/resources involved in the deployment scenario

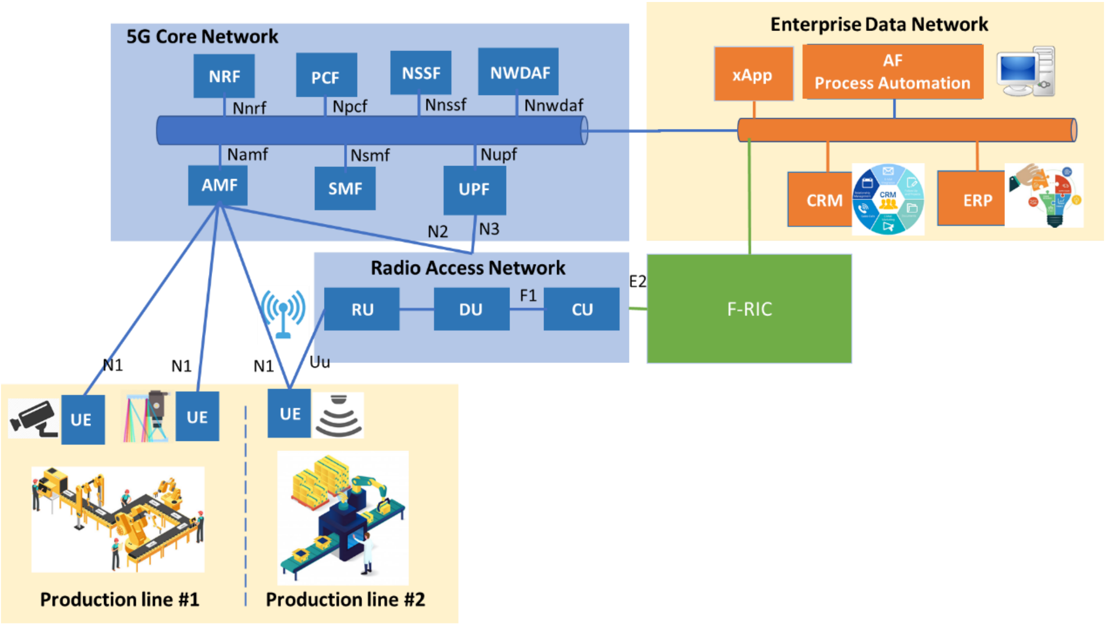

Figure 35: Proposed architectural approach for the 2nd scenario of the 3rd pilot

Our proposed architectural approach is comprised of three sub-networks: The RAN (RU/DU/CU), which also incorporates the Flexible RAN Intelligent Controller (F-RIC), the core network and the enterprise network including network controlled applications (xApps). There are two types of sensors involved: for the first one, a high-resolution camera is embedded on the sensor node, able to capture high resolution images (i.e. either 2D/3D) of the produced intermediate product that is transmitted via a high bandwidth channel to the enterprise network. The second type of sensors are environmental ones, where certain parameters such as the levels of carbon dioxide in the atmosphere, temperature increase due to the simultaneous operation of various machine types as well as humidity, are measured. It is assumed that each node sensor is equipped with a SIM card and acts as a UE. All transmitted data are sent to an RU located in the proximity of the production chain.

In the 5G Core Network, the NWDAF component supports service registration and metadata exposure to NFs/AFs via the generation of notification events. Service registration & discovery is performed by NRF so that different network functions can find each other via APIs.

All operator network slice instances are stored in NSSF and enforced to RAN domain via F-RIC. Network slices are authorised by the AMF, based on the requested service by the sensors. Provision of service may include allocation of high bandwidth channels to the sensor nodes for high resolution image transmission (uplink case) or zero latency transmission from the AF back to the nodes for decision making procedures (e.g. immediate production termination, downlink case). The NSSF collects the load level information of the particular slice from the NWDAF and allocates the sensor node with a different slice from the developed 5G core if required. This is a standard use case in manufacturing environments, where production levels may significantly vary from day to day depending on the amount of daily orders, which, in turn, may vary according to seasonal production characteristics. Based on the day-to-day analysis and history of data, the NWDAF is expected to predict a behavioural pattern which indicates that the expected utilization might get spiked to a certain level during a certain day or period of days. Therefore, according to the NWDAF inputs, NSSF prepares itself to automatically allocate the next available slice in the core network to achieve all the services alike for all active subscriptions.

In addition, NWDAF can store information regarding maximum data used per session and data usage per sensor node at different times of the day. With that information the NWDAF is able to form a data usage pattern for a node. With NWDAF input, PCF can enforce specific rules appropriately for the node according to the usage pattern. This type of proactive decisions by PCF also helps in utilizing the 5G resources appropriately.

Moreover, NWDAF, apart from serving the 5G network functions, can also help potential manufacturing operators to plan their enhancement in infrastructure based on resource utilization. This is useful because, based on the data provided by the NWDAF the NFs can make real time decisions for allocating the resources but are limited to a certain extent (based on hardware resources available).

The F-RIC is an essential component of this deployment scenario, since as explained network slicing will support high bandwidth/zero latency applications to the sensor nodes. In this context, optimization and control of the RAN infrastructure is provided, in conjunction with the data received from the enterprise network.

Finally, in the Enterprise Network, metadata from NWDAF are send to the AF (Process Automation Management) for predictive analysis that helps to proactively manage the 5GS with less human effort.

The main target of this deployment scenario is to provide an OpenSource solution based on the OAI and M5G platforms that would be low-cost, standalone, and operational in support of small and medium enterprises (see components and interfaces as shown in Figure 36). The following technical challenges will be implemented and demonstrated:

- Data mining and analysis by means of xApps and incorporation of NWDAF with the goal to collect and process data from as many 5G functions as possible
- E2E Network Slicing by means of M5G Flexible-RIC platforms (F-RIC)
- RAN intelligent and extensions by means of M5G SDK/xAPPs ecosystems on the top of the network.

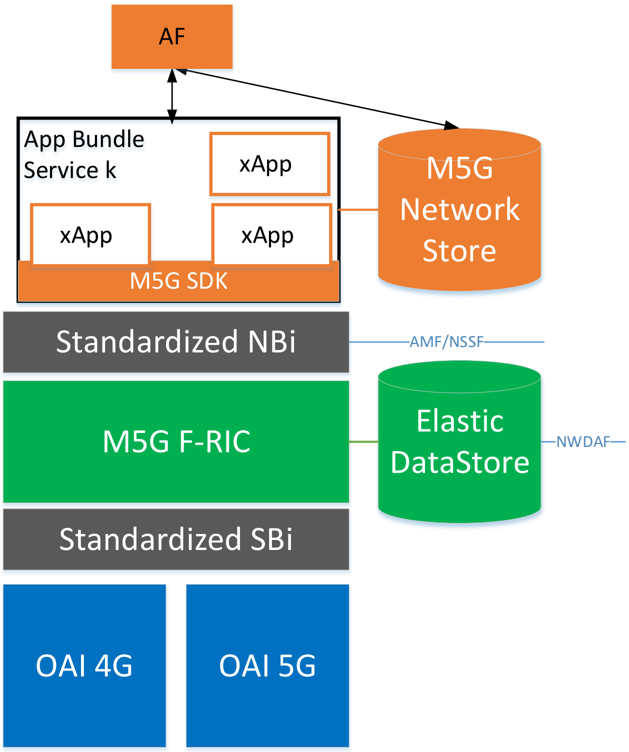

Figure 36: OpenSource low-cost, Standalone, and operational 5G solution for Pilot 3, deployment scenario 2

2.3.1.7 Interactions among entities in the 2nd deployment scenario

In this section, two UML diagrams are presented regarding the interactions among the entities involved in the deployment scenario described in the previous section. In the first case (Figure 37), the NSSF, AMF and RAN components perform discovery requests to the Network Repository Function (NRF) in order to obtain the profiles of the available NF instances and their supported services. Afterwards, the AF in the Enterprise Network performs an event subscription request to the NWDAF, as the goal is to retrieve network related information and to perform local optimization on various parameters of interest (e.g. QoS, availability, etc.) that, in turn, affects industrial performance. Then, the NWDAF sends a service request to the NSSF, to retrieve the information related to the corresponding network slice per service. The NWDAF also performs service requests to the AMF and RAN, to retrieve information on user mobility and network status parameters.

In the second UML diagram, the goal is to further elaborate on the proposed F-RIC and SDK architectural approach that will be adopted for the demonstration of our use case. In this context, a two-level abstraction is performed: logical base stations (BSs), and slices-specific virtual BSs (vBSs). In the first case, each logical BS corresponds to a different access technology in the physical layer. In the second case, each vBS corresponds to a different slice in the network. For the purposes of our use case, a common infrastructure and Radio Access Technology (RAT) have been considered (hence one logical BS). In the second level of abstraction, we consider two slices per vBS: one dedicated to high data rate transmission of 2D/3D images from the sensor nodes to the core network, and the other one dedicated to zero latency transmission of control messages from the core network back to the sensor nodes, in cases where production should be immediately terminated.

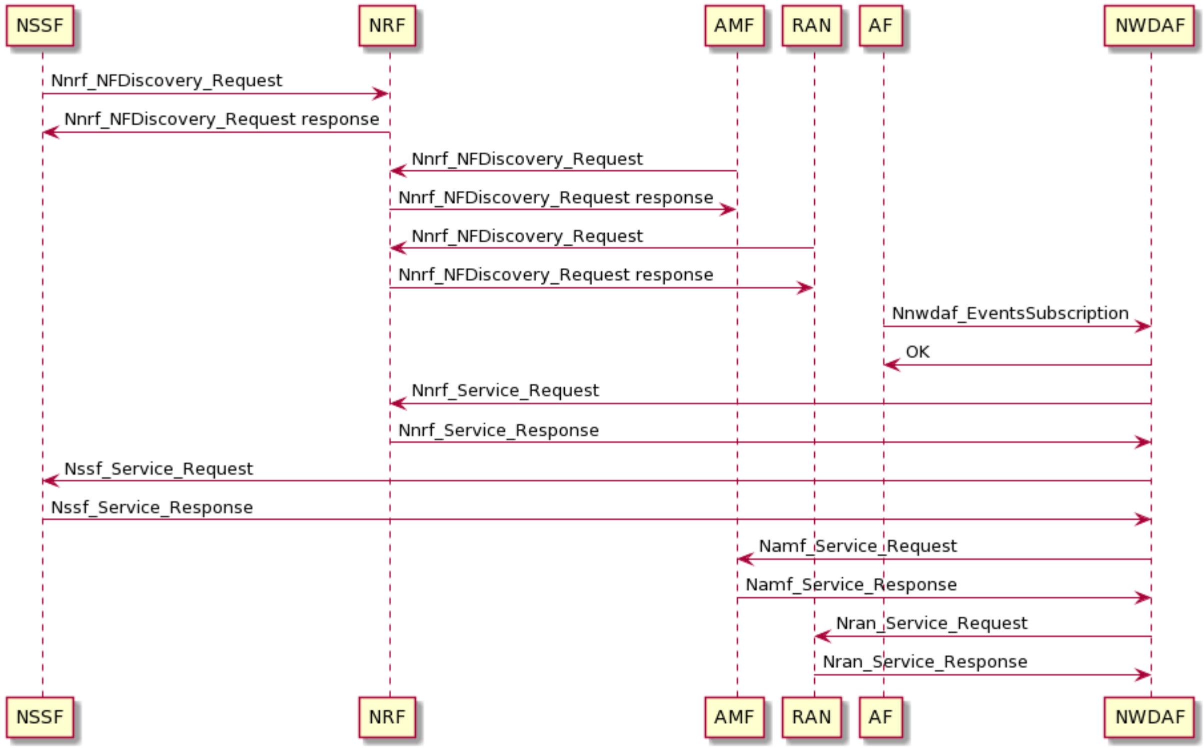

Figure 37: UML diagram of the 2nd deployment scenario of the 3rd pilot (interactions between entities for NF discovery, event subscription and service request)

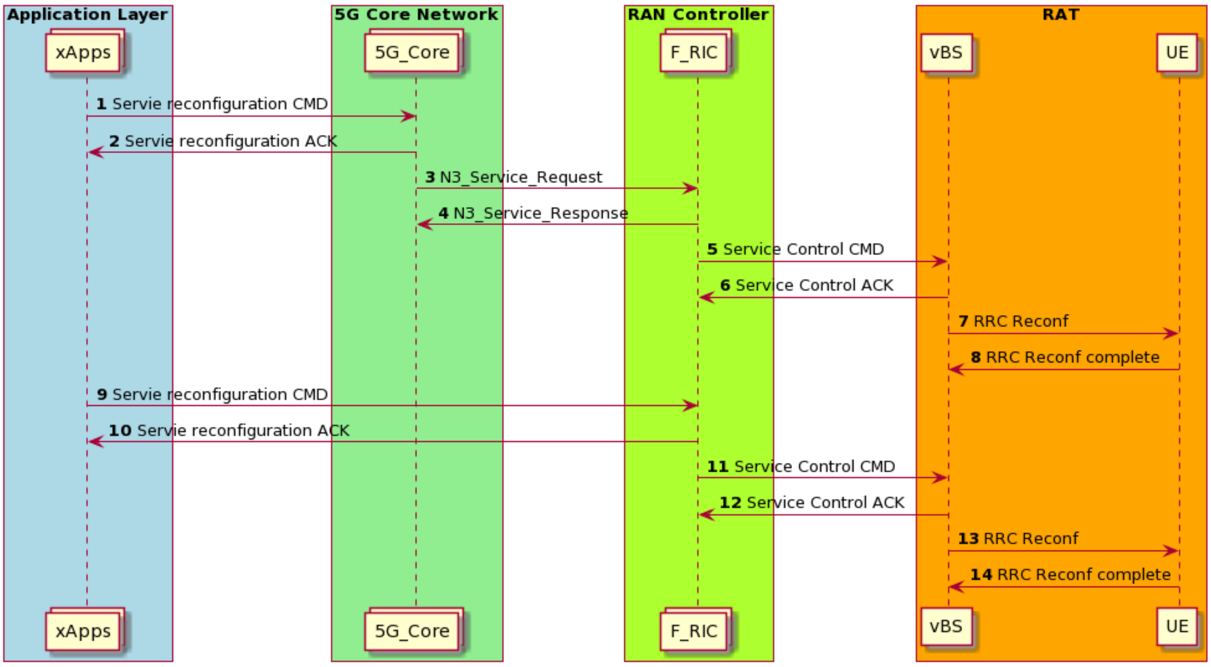

Figure 38: UML diagram of the 2nd deployment scenario of the 3rd pilot (F-RIC interfaces with xApps and 5G Core)

3 SYSTEM REQUIREMENTS

3.1 Approach

From the description in the previous section it is evident that the Affordable5G system aims to support a variety of pilots, applications and use cases with distinct characteristics in terms of throughput, latency, number of supported UEs and sensitivity to timing inaccuracies among others. These use cases, as well as the recent work of the 3GPP, O-RAN, MEC and NFV_MANO communities have been used to derive the Affordable5G system requirements, which will subsequently drive the development of the system architecture.

Additionally, it is clear that requirements for many of the pilots and their use cases overlap, especially in the NG-RAN and 5GC aspects. It was therefore decided to identify a common Affordable5G architecture (that will be elaborated in the subsequent D1.2 deliverable) to consolidate a common set of requirements for that architecture.

Furthermore, the roll-out of such a network requires that efficient cybersecurity mechanisms be in place. These include, for example, requirements to protect the Affordable5G system from internal and external threats, requirements to detect in a timely manner network failures and malfunctions due to malicious activities, and requirements to mitigate security threats and provide minimum system restoration time.

In order to address the requirements for a common Affordable5G architecture and the security considerations that are applicable to all pilots, deployment scenarios and use cases in a more effective manner, we start this section with a presentation of the respective top-level requirements before introducing the detailed system requirements in sections 3.4-3.6.

3.2 Requirements for common Affordable5G architecture

As mentioned above, the pilots and the use cases share many common requirements, and it is also envisaged that these pilots and use cases will consider a minimum common Affordable5G architecture as the basis for their implementation and deployment. The definition of this common Affordable5G architecture is beyond the scope of this document (and will be addressed in deliverable D1.2) but the requirements for that architecture are grouped here. A provisional reference architecture is shown below (placeholder for cross-reference but with specification).

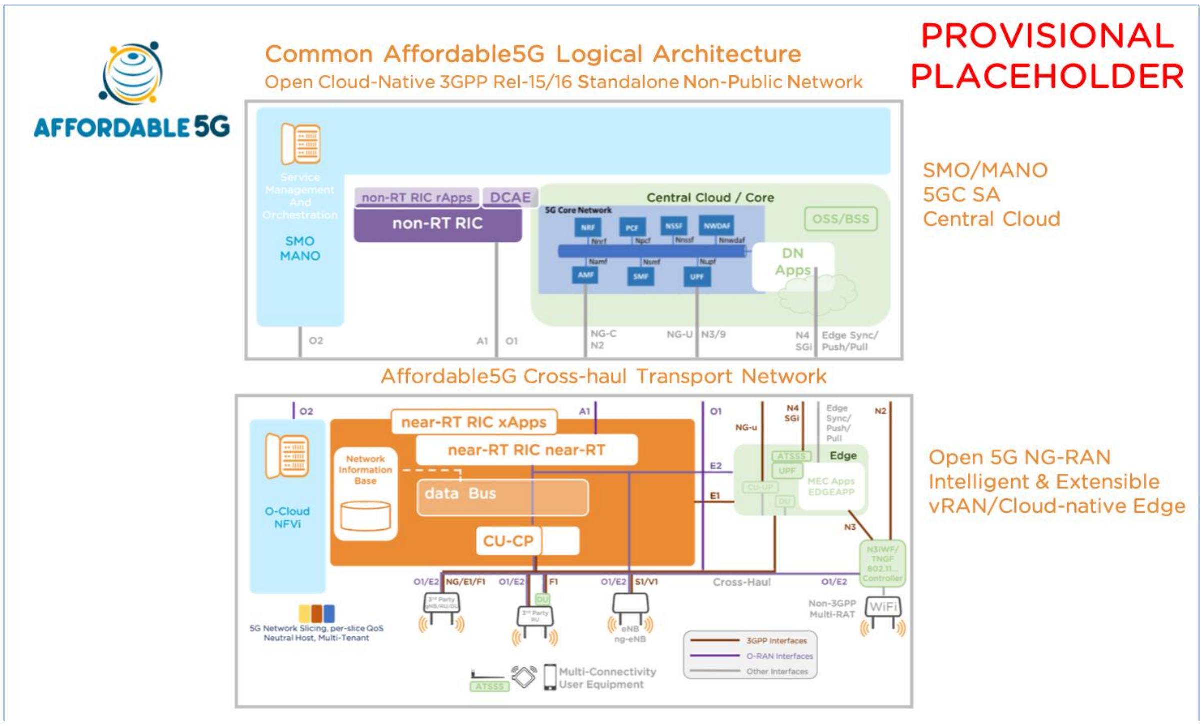

Figure 39: Provisional Affordable5G Reference Architecture (information placeholder only)

3.2.1 Common Affordable5G architecture top-level requirements

Based on the provisional system reference architecture the following major top-level requirements can be identified:

- The Affordable5G network will conform to 3GPP 5G network requirements in both the 5GC and NG-RAN, with the goal to support operation as a 5G Standalone NPN (SNPN). However, the architecture can optionally support additional operation such as Public network integrated NPN (PNI-NPN).
- The architecture will comply with 5G network slicing in the 5GC and NG-RAN to support neutral hosts (e.g., Multi-operator Core Network/Multi-Operator Radio Access Network - MOCN/MORAN) and differentiated QoS slicing such as eMBB, URLLC etc.
- The system will support Control and User Plane Separation (CUPS) in 5GC and NG-RAN including separation of CU-UP and CU-CP and deployment of UPF (and DN) in both core and edge (MEC).
- The NG-RAN will be aligned to the additional O-RAN Alliance requirements, including supporting RIC VNFs. In addition, the NG-RAN edge will support open extensibility and intelligence in both the control-plane (near-RT RIC) and the user-plane (MEC).
- In the NG-RAN, the RU/DU/CU network functions will support Higher-Layer Split/Lower-Layer Split (HLS/LLS) split architecture to support multi-vendor RAN using open interfaces. The choice of deploying integrated RU and DU or split RU and DU will be determined by the use case and the availability of VNFs/PNFs.
- The NG-RAN will support virtualised or cloud-native deployment and orchestration (through the Service Management and Orchestration – SMO / MANO component of the presented provisional architecture) on primarily commodity hardware, potentially with FPGA/GPU/DSP hardware acceleration.

3.3 Affordable5G security considerations and top-level requirements

According to the cybersecurity recommendations of 5G systems proposed by the EU Commission and related technical literature [54] [55] [56], [57], 5G systems should secure the entire network, users and communications effectively against cyber-attacks, and provide flexible security mechanisms tailored to the needs of the different supported use cases. In this sense, 5G systems should provide security mechanisms compliant with local lawful interception laws and regulations covering network protection, authorization, confidentiality, integrity, and availability. Such security mechanisms must be extensible to new algorithms and procedures that could be defined during the lifetime of the specifications.

More precisely, protection and authorization services should be defined for users, devices and networks at bearer and at service levels. Data privacy and protection is one of the key enablers of private 5G deployments, and one of the major concerns for industries and enterprises with certainly valuable data. Hence, confidentiality and integrity services must protect data, voice, video and signalling, as well as subscribers' privacy, and must be ensured through the encryption of end-user plane data as it passes through the mobile network. System availability should be guaranteed by protecting user equipment and the 5G network not only against denial-of-service attacks from external networks such as the Internet, but also against errors and non-malicious unavailability situations that appear due to unusual but expected bad radio conditions and broken links.

From the virtualisation point of view Affordable5G shall also provide security and privacy guarantees. The Affordable5G is designed as a multi-tenant infrastructure being able to manage multiple trusted domains from the edge to the core. For that reason, Affordable5G shall provide security functions across the different trusted domains for protecting the available networks services, following the security and trust guidelines specified in ETSI GS NFV-SEC 003 [58], the security guide detailed in ETSI GS NFV-SEC 0006 [59] and the security management and monitoring analysis defined in ETSI GS NFV-SEC 0013 [60], among others ETSI GSN NFV-SEC specifications and requirements.

Based on the aforementioned information, the following cybersecurity requirements have been defined for Affordable5G*:*

Protection Requirements

The purpose of protection requirements is to strengthen security in the 5G infrastructure by protecting it from internal and external threats. As such, the attack surface of the target infrastructure is expected to be reduced. Protection requirements in Affordable5G include:

- Protecting the networks across their entire lifecycle and covering relevant equipment in the design, development, procurement, deployment, operation and maintenance phases of 5G networks by taking into account cybersecurity vulnerabilities that may be exploited to gain unauthorised access to information (cyberespionage) or for other malicious purposes (cyberattacks aimed at disrupting or destroying systems and data);
- Conducting risk and vulnerability assessments in order to adapt national measures on security requirements and risk management in the light of such assessments;
- Providing a toolbox of appropriate, effective and proportionate possible risk management measures to mitigate the identified cybersecurity risks, including an inventory of the types of security risks potentially affecting the cybersecurity of 5G networks and a list of proactive mitigation measures that would address every type of identified security risks;
- Considering that weak slices isolation and connectivity may compromise the entire 5G security (e.g., sensitive data, managed inside a slice, could be exposed to applications

running in other slices services, through side channel attacks), therefore the system must guarantee strong connection and slice isolation.

- Providing domain isolation between untrusted domains, a security attack on a domain without trust relationships shall not compromise the security of the other domains

Detection Requirements

The purpose of detection requirements is to properly and timely identify security incidents that could not be prevented from the protection phase and that would potentially harm the operations in the 5G infrastructure. Detection requirements in Affordable5G include:

- Supporting the detection of network faults or malfunctions, ideally before those have any drastic impact on system or service performance;
- Supporting the detection of security threats at an early stage by evaluating specially designed algorithms for anomaly detection;
- Ensuring that end-users of the 5G system are authenticated, and the network is also authenticated towards the end-users

Reaction Requirements

The purpose of reaction requirements is to define mitigation measures to react against detected cybersecurity incidents that would harm the operations in the 5G infrastructure. Reaction requirements in Affordable5G include:

- Guaranteeing a minimum restoration time in case of network malfunction during the design phase of the 5G system;
- Providing the ability of isolating security intrusions into given areas by using the concept of security trust zones;
- Providing cybersecurity measures to address security threats affecting the protection of personal data and privacy;
- Providing incident response and incident management plans specific for each threat defined in all use case scenarios.
- Providing domain isolation if a trusted domain has been compromised, the compromised domain should notify the rest of domains and should no longer be trusted

3.4 Common system requirements across all pilots

This section covers the system requirements that are common across all pilots. These are derived after elaborating on the top-level requirements presented in section 3.2.1.

Below, we define basic terms:

A requirement is

(1) A condition or feature needed by an entity to provide a solution to a problem or achieve an objective.

(2) A condition or capability that must be met or integrated in a system/solution to satisfy a contract, standard, specification or other formally imposed documents.

Types of Requirements

In the context of the Affordable5G project, three types provide a suitable approach to distinguish requirements, namely the i) functional requirements, ii) quality requirements and iii) constrains. These are explained as follows.

Functional Requirements (FR)

A functional requirement defines a function or feature to be provided by the system or by a system component. In a first version, functional requirements are described generally and, later on, with the progressing of the specification, a functional requirement describes in detail the inputs and outputs as well as possible failure points.

Quality Requirement (QR)

A quality requirement defines the quality characteristic that can be transversal to the entire system, a system component or merely a function.

Constraint (C)

A constraint represents an organisational or technological requirement that restricts the paradigm that a product is developed.

Quality requirements and constraints form the non-functional requirements, which are used to access the operation of a system.

The Affordable5G system requirements are further categorised as:

- Network layer requirements, which include requirements on the functionality of the Core, the RAN and the Transport networks
- Virtualisation infrastructure, management and orchestration layer requirements, which cover requirements on the NFVI, the NFV MANO, as well as requirements on slicing and edge computing
- Application layer requirements, which address the needs of the particular applications involved in the use cases.

In the description of the requirements, specific verbs, namely “shall”, “should” and “may”, are used. The meaning of these verbs (key words) is as follows:

- shall – it is used to express a mandatory (absolute) requirement
- should – it is used to express recommendations, i.e., provisions that an implementation is expected to follow unless there exist strong reasons in particular circumstances to ignore them
- may – it is used to express an optional requirement.

Each one of the requirements presented in the following sections is associated with an identifier (ID) and complemented by a short explanation or reference to relevant source.

3.4.1 Network layer requirements

The common network layer requirements are presented in Table 1.

Table 1: Network layer requirements common to all pilots

Functional Requirements		
ID	**Requirement**	**Comments**
REQ-NET-01	The network shall conform to 3GPP 5G network requirements, architectures and interfaces in both the 5GC and NG-RAN	Affordable5G aims to deliver a complete 5G system offering for private and enterprise networks
REQ-NET-02	The system shall support operation as a 5G SNPN	Support for the realization of a Standalone private (non-public) network will be provided

REQ-NET-03	The system shall support O-RAN standard architecture & interfacing including the support of RIC VNFs	The system will support open solutions like O-RAN to allow flexible and cost-efficient 5G deployments in private and enterprise networks
REQ-NET-04	The system shall support 3GPP release Rel 15 SA	The baseline for the system architecture will be Rel. 15 (first phase of 3GPP 5G specifications)
REQ-NET-05	The system may support 3GPP release Rel 16 SA	Features from the second phase of 3GPP 5G specifications (Rel. 16) will also be considered
REQ-NET-06	The system shall support control and user plane separation in the 5GC and deployment of the UPF (and DN) in both core and edge (MEC).	Separation between control and user plane functions in the core network is specified for 5G systems in Rel. 15. User Plane Function (UPF) will be deployed as an NFV service in the core as well as in edge locations (exploiting MEC) to support traffic routing to local DN.
REQ-NET-07	The system shall support control and user plane separation in the NG-RAN	Separation of CU-UP and CU-CP will be supported.
REQ-NET-08	The system shall support configuration and placement of the CU-UP, UPF and DN per slice	The placement of these network functions and of the DN will be done according to the QoS requirements of the particular slice. For example, a slice for URLLC may terminate the User Plane at a DN in the edge cloud while an eMBB slice may terminate the User Plane at a DN in Metro or in the core cloud.
REQ-NET-09	The system shall support Multi-Operator CU and DU HW and NFVi	CU and DU HW and NFVI hosted by the Neutral Host will be able to support multiple operators
REQ-NET-10	The system shall support several synchronization means: GNSS, PTP and SyncE	For the synchronization (time, frequency and phase) of the equipment in the 5G network different technologies will be used like GNSS, PTP and SyncE
REQ-NET-11	The system shall support MIMO functionality	For improving spectral and energy efficiency, the system will use MIMO techniques
REQ-NET-12	The system shall support virtualised RAN functions	The system will support the deployment of RAN functions as software running on commodity hardware
REQ-NET-13	The system shall support virtualised CN functions	The system will support the deployment of Core Network functions as software running on commodity hardware
REQ-NET-14	The system shall support Multi Band and Multi Operator RRU (MORAN & MOCN)	RAN sharing with MORAN or MOCN solutions will be facilitated through slicing at the RAN level which will support neutral hosts

REQ-NET-15	The core network should be able to respond to any QoS solicitation from the Application Function to assure the service performance.	The Application Function (AF) should be able to request that necessary QoS resources be available to the user and influence traffic routing
REQ-NET-16	The Core Network should report System KPI to the monitoring system.	For the efficient performance management of the system the Core Network should report KPI values to the monitoring component
REQ-NET-17	The system shall support inter 5G cells mobility	Classical mobility between 5G cells will be supported in various operational environments
REQ-NET-18	The system shall support virtualised or cloud-native deployment & orchestration on open COTS hardware for NG-RAN	Deployment of CU/DU on COTS will be supported potentially complemented by FPGA/GPU/DSP hardware acceleration
REQ-NET-19	The system shall support Ethernet based fronthaul with TSN functionality	Ethernet-based mobile fronthaul using Time Sensitive Networking (TSN) can simplify deployment and reduce cost compared to WDM-based solutions
REQ-NET-20	The system shall support operation in the TS 38.101-1 Frequency Range 1 FR1 (410-7125 MHz) bands including support for bands n77 and n78.	The system will use frequency bands in the FR1, i.e., sub-6GHz frequency bands also extended to support new spectrum from 410 MHz to 7125 MHz, including band n77 (3700 MHz) and n78 (3500 MHz)
REQ-NET-21	The system may support operation in the TS 38.101-2 FR2	Operation in bands in the FR2 (28-42 GHz) may be supported
REQ-NET-22	In the NG-RAN, the RU/DU/CU network functions shall support HLS/LLS split architecture to support multi-vendor RAN using open interfaces.	The choice of deploying integrated RU+DU or split RU and DU will be determined by the use case and availability of VNFs/PNFs. HLS will be Split 2 F1 (F1-c & F1-u) and baseline for the LLS will be the O-RAN fronthaul at Split7.2 but additional options including support of Split 6 FAPI/nFAPI may be considered
REQ-NET-23	Security mechanisms shall span across the CN and RAN and shall be compliant to 5G security architecture	5G Security architecture and procedures compliant to 3GPP TS 33.501
REQ-NET-24	The system shall support authentication of the UEs and authentication of the network towards the user	Mutual authentication between the UE and the network will be supported
REQ-NET-25	Access to the private 5G network shall be restricted to authorised UEs and processes only.	The 5GC infrastructure shall enforce access control policies to restrict access only to authorised (certified) devices.

REQ-NET-26	O-RAN Operations and Maintenance Interface (O1) shall be protected	O1 interface protected with authentication, integrity, confidentiality. Use of TLS instead of SSH.
REQ-NET-27	O-RAN Management A1 interface shall be protected	A1 interface protected with authentication, integrity, confidentiality
REQ-NET-28	Open Fronthaul M-Plane interface shall be protected	Interface protected with authentication, integrity, confidentiality
REQ-NET-29	3GPP E1 interface shall be protected	Confidentiality, integrity, replay protection
REQ-NET-30	3GPP F1 interface shall be protected	Confidentiality, integrity, replay protection
REQ-NET-31	The system shall be able to detect network failures and malfunctions	Failures related to network devices, functions and communication links should be detected in a timely manner
Quality Requirements (Non-functional)		
ID	**Requirement**	**Comments**
REQ-NET-32	The transport network shall provide failure recovery mechanisms	The transport network (backhaul, between the edges and the core) will provide mechanisms for network failure recovery
REQ-NET-33	The transport network shall provide a delay less than 10 ms.	The backhaul network will have a delay of less than 10 ms (this is a typical latency requirement for a 5G backhaul)
REQ-NET-34	The transport network shall provide at least a throughput of 100 Mbps.	The backhaul will provide a throughput of at least 100 Mbps in order to support the envisaged applications
REQ-NET-35	The transport network shall guarantee high availability	The uninterrupted support of the different applications requires high availability of the backhaul network
REQ-NET-36	The NG-RAN may support Real time security Event Logging	RAN may support "Real time security Event Logging" with purpose to capture real-time security events that occur in the network and report these for further handling in a comprehensive way. The security events should be sent in a standardised way from the node to an external Syslog server, compliant with the standard RFC5424 (Syslog). This gives real-time feedback, making it possible for an Intrusion Detection System (IDS) to detect threats towards the system. This is done by collecting security events from all nodes.
REQ-NET-37	The system shall be able to detect security threats	Security threats like denial-of-service attacks should be detected in a timely

		manner possibly using anomaly detection algorithms

3.4.2 Virtualisation infrastructure, management and orchestration layer requirements

The common Virtualisation infrastructure, management and orchestration layer requirements across all pilots are presented in Table 2.

Table 2: Virtualisation infrastructure, management and orchestration layer requirements common to all pilots

Functional Requirements		
ID	**Requirement**	**Comments**
REQ-MAN-01	The architecture shall provide 5G network slicing to support services with diverse QoS requirements	There can be various and diverse requirements, such as high data rate transmission or zero latency applications
REQ-MAN-02	The solution should be able to establish network slices that are extended from the RAN (ingress point) up to the Core of the network (egress point).	It is vital to be able to establish a slice, for a particular service, that guarantees the SLA throughout the whole network components that are used by the service, including the RAN, Edge network, and the Core network.
REQ-MAN-03	The system shall provide a way to create, instantiate, update and delete Network Slices	The management component will be responsible for the creation, instantiation, update and deletion of the Network Slices (Network Slice Life Cycle Management)
REQ-MAN-04	The system shall support several slices over the same infrastructure	Several slices will be supported to cope with applications with diverse QoS requirements
REQ-MAN-05	The system shall support management of slices in an end-to-end fashion	The Network Slices will extend from the RAN to the Core Network and will be managed in an end-to-end fashion
REQ-MAN-06	The system shall support Multi-Access Edge Computing (MEC)	Support of edge computing will be provided to address applications requiring processing and/or storage close to the endpoints.
REQ-MAN-07	The system shall support MEC deployment topology in the RAN	It will be possible to deploy edge computing servers in the cloud RAN
REQ-MAN-08	The system shall support the provision of the MEC stack installation and configuration.	It will be possible to install and configure a MEC platform for distributed edge computing
REQ-MAN-09	The system shall support orchestration of services as well as lifecycle management.	The dynamics of deployed services demand their management using an orchestrator which is capable of instantiation, termination, scaling and pausing of services.

REQ-MAN-10	The service orchestrator shall be connected to the system monitoring and to the infrastructure involved in the necessary actions.	The service orchestrator will trigger the allocation of Virtualisation infrastructure resources needed for the connectivity of services and this will be done using information from the service monitoring component.
REQ-MAN-11	The system shall provide an interface to manage the lifecycle of the edge server	Edge server lifecycle management may include initial deployment, monitoring, decommissioning
REQ-MAN-12	The system shall be able to configure the HW for specific workloads	Configuration includes Enable/Disable CPU/memory settings etc.
REQ-MAN-13	The system shall provide an interface to manage the lifecycle of the VNF	Lifecycle management may include Fault, Configuration, Accounting, Performance and Security (FCAPS) management
REQ-MAN-14	The system shall support VNF lifecycle management at cloud-level platforms as well as low-end devices	It will be possible to support VNF instantiation, management, scaling up/down, and termination not only at the main cloud platform but also at low-end devices
REQ-MAN-15	The Network Service lifecycle manager shall guarantee the sequencing of the instantiation actions.	The lifecycle manager will perform all required steps to start the Network Service
REQ-MAN-16	The Network Service Lifecycle manager shall monitor the instances.	It will be possible to monitor the operating state of the Network Service instances
REQ-MAN-17	Network Service Lifecycle shall follow up the instantiation phases, network configuration and final up and running.	It will be possible to use the Lifecycle manager to deploy a Network Service dynamically by following the steps of instantiation, network configuration and service execution
REQ-MAN-18	The solution should provide an environment for running software for data processing and service provisioning of multiple NFV services.	The system will be able to handle multiple NFV-based services
REQ-MAN-19	The solution should be able to provide real-time KPIs to the Orchestration platform mainly related to the QoS of services in order to guarantee SLAs.	The Orchestration platform should be able to monitor the services instantiated under its realm, using KPIs, in order to provide means of ensuring that SLAs are met. This will allow the triggering of scale up/down of services, according to the rules provided in NFV service descriptors.
REQ-MAN-20	The slice shall respond to application service requirements	The provisioning of Network slices will be done in a way that will take into account the requirements of the application services

REQ-MAN-21	The system shall provide monitoring mechanisms to continuously check the performance and status of the active slices	The monitoring system will be able to monitor the state of all components (dedicated and/or shared resources) of a Network Slice
REQ-MAN-22	The system shall provide monitoring mechanisms to continuously check the performance and status of the active VNFs	It will be possible for the system to collect data regarding KPIs of a VNF (e.g., memory, CPU, bandwidth, packet loss, jitter etc.)
REQ-MAN-23	The system shall provide monitoring mechanisms to continuously check the performance and status of the active edge servers	It will be possible for the system to collect data regarding KPIs of an edge server including for example hardware utilization (processor, memory, disk usage), throughput, response time etc.
REQ-MAN-24	The system shall provide monitoring mechanisms to continuously check the performance and status of the VIMs	It will be possible to monitor the state and performance of the Virtualised Infrastructure Managers (e.g., response time, service daemons, instance reachability, etc.)
REQ-MAN-25	The system shall provide monitoring mechanisms to continuously check the performance and status of its own system health.	It will be possible to monitor the system's health with respect to parameters like real-time disk usage, memory usage, CPU load, network IO and virtual IO usage / loss rate, available vCPUs, virtual memory etc.
REQ-MAN-26	The system shall ensure the isolation of the slices	The architecture must be able to instantiate several slices and provide them with the appropriate strong isolation to deliver slice security and privacy
Quality Requirements (Non-functional)		
ID	**Requirement**	**Comments**
REQ-MAN-27	The system shall support the provision of different bare metal OS to the edge servers	The system will support interoperability across platforms running different OSs
REQ-MAN-28	The system shall detect VNF health-issues and trigger pre-defined recovery actions	When the performance of a VNF is below a pre-defined threshold the system will be able to take mitigation / recovery actions (e.g., alert, migration etc)
REQ-MAN-29	The system may support HW and SW security hardening	All hardware and software (e.g. VNFs) used may be security hardened at rollout. The hardening guideline is a process to reduce the security risks by eliminating known vulnerabilities during installation. Examples include, removal of unnecessary software, or disabling insecure/un-used services. The hardening guideline also includes what ports

		and listening services that needs to remain open/running to minimise the risk for unused ones not been used for vulnerability exploitation (i.e. disable unused ports/interfaces).
Constraints (Non-functional Requirements)		
ID	**Requirement**	**Comments**
REQ-MAN-30	Edge Infrastructure shall host lightweight version of instances deployed in the main core.	At the edge nodes compute and storage resources are limited
REQ-MAN-31	The system should support services running in lightweight VMs or Docker containers.	Given the limited physical space for computational resources and thus limited processing capacity the current implementation should be based on lightweight virtualised infrastructure managers (VIM), such as Docker based managers, e.g., Kubernetes and Openshift.
REQ-MAN-32	The solution should allow the deployment of end-to-end slices able to accommodate the requirements imposed.	Providing services in an end-to-end manner requires to set up all the resources necessary to make sure that the SLA in the slice descriptors are met (compute, networking, and storage in an end-to-end fashion).

3.5 Pilot-specific requirements

For the presentation of the requirements that are derived from different Pilots we use the same categorization used for the requirements that are common to all Pilots. In the following tables we also indicate the Pilot that each requirement has been derived from.

3.5.1 Network layer requirements

Table 3 summarises the additional network layer requirements per pilot.

Table 3: Additional network layer requirements per pilot

Functional Requirements			
ID	**Requirement**	**Comments**	**Derived from**
REQ-NET-38	The system may support operation as PNI-NPN	It may be possible to have a private network deployed with the support of a PLMN (Public network integrated NPN)	P1
REQ-NET-39	The system shall support small outdoor cells capabilities	Castellolí test platform in which Pilot1 is being carried out shall be based on outdoor small cells	P1
REQ-NET-40	The system shall support remote management and	5GCore, IMs and MCS instances should be remotely accessible and independent from the different	P1

	separate management domain per operator.	domains. Also, services should be instantiated in an NFVI out of each operator´s orchestrator operating environment.	
REQ-NET-41	The system shall support national roaming functionality	In case visitors' (external emergency authority´s) 5GC could not be hosted in the neutral host operator domains, roaming agreement should be supported.	P1
REQ-NET-42	The system may provide integrity protection of the user data between the UE and the gNB	User data may be integrity protected (specified as optional in 3GPP TS 33.501)	P1
REQ-NET-43	The system shall prevent the user terminal from connecting to lower security networks	Method for preventing the user terminal from connecting to lower security networks (e.g., GSM, UMTS, LTE) to avoid attacks, such as, rogue base stations.	P1
REQ-NET-44	The system should support data collection from NFs residing on the core and access part of the 5GS	The NG-RAN infrastructure and the 5GC NFs should route monitoring information towards the NWDAF.	P3
REQ-NET-45	NWDAF should be supported for network load performance computation and future load prediction	The NWDAF will be able to provide analytics regarding the network load and future load prediction	P3
REQ-NET-46	The NWDAF should support subscriptions from multiple network elements and entities	Multiple Network Functions and similar entities will be able to subscribe to the NWDAF for information obtained from data analytics	P3
REQ-NET-47	The NWDAF should deliver event information and predictions to its subscribers	Different entities (including Network Functions) will subscribe to the NWDAF to get information from other entities and analytics	P3
REQ-NET-48	The system should support intelligent processing of collected data	The NWDAF should processes the gathered monitoring data for learning purposes	P3
REQ-NET-49	The system shall support interconnection of the AF with the NWDAF	The AF will provide service data to the NWDAF and will subscribe to NWDAF to receive network analytics info	P3
REQ-NET-50	The 5G system shall support prioritisation of critical messages	The network will be able to provide different levels of traffic prioritization in order to support applications with different QoS requirements	P3

REQ-NET-51	The 5G system should be totally compatible with TSN domain	The 5G system should be able to provide a TSN bridge transport service	P3
REQ-NET-52	The infrastructure shall support high performance Ethernet applications	The Ethernet transport service will support traffic filtering and prioritization based on information extracted from the Ethernet header information created based on 802.1Qbv. Also, the 3GPP system will support clock synchronization defined by IEEE 802.1AS across 5G-based Ethernet links with PDU-session type Ethernet.	P3
REQ-NET-53	The 5G system shall support dense UE deployment	Various sensor nodes are required in industrial environments	P3
REQ-NET-54	A large number of AMRs should be supported in a limited geographical area (dense deployment)	Could have more than one AF residing on the core part of the 5G	P3
Quality Requirements (Non-functional)			
ID	**Requirement**	**Comments**	**Derived from**
REQ-NET-55	The system shall provide confidentiality protection of user data between the UE and the gNB	User data will be confidentiality protected (specified as optional in 3GPP TS 33.501)	P1
REQ-NET-56	A centralised solution should allow to register specific users (authentication) under specific roles (authorisation), while keeping a log of all access attempts to external reference points	Authentication and authorization will be provided by a centralised mechanism while logs of access attempts will be available through different mechanisms (RESTful APIs, RPC daemons, etc.)	P2
REQ-NET-57	The solution shall guarantee the data transport between the CN and the Edge network within pre-determined levels of goodput and latency that suite the service.	The link quality between the core network and edge networks must be somehow guaranteed. Particularly on critical services, minimum latency and bandwidth requirements must be ensured by the system.	P2
REQ-NET-58	The 5G system shall support high-bandwidth streams from a massive set of devices with a user experienced data rate of up to 100 Mbit/s	Wireless sensor nodes should be able to transmit high resolution 2D/3D images at a high rate	P3

Constraints (Non-functional Requirements)			
ID	**Requirement**	**Comments**	**Derived from**
REQ-NET-59	RUs and DUs should be deployed according to the scheduled task that may require communication either with distant AMRs or link establishment in harsh conditions	Harsh conditions may include, for example, cubicles, control centre, etc.	P3
REQ-NET-60	RU and DUs should be deployable in GNSS-less environment	GNSS-less environment without access to the sky area	P3

3.5.2 Virtualisation infrastructure, management and orchestration layer requirements

Table 4 presents the additional requirements per pilot regarding the support of the Virtualisation infrastructure, the management and the orchestration.

Table 4: Additional Virtualisation infrastructure, management and orchestration requirements per Pilot

Functional Requirements			
ID	**Requirement**	**Comments**	**Derived from**
REQ-MAN-33	The system shall support QoS solicitations from the MCS	The core network should be able to respond to any QoS solicitation from the Application Function to assure the service performance.	P1
REQ-MAN-34	The solution should be able to provide pre-determined KPIs directly to the virtualised functions of NFV services.	The access of certain KPIs related to the functioning of a service should be fed to its virtualised functions. This is particularly necessary when functions require to change their configurable parameters dynamically (tunning) while keeping their efficiency. For instance, the transmission fps of a video may be decreased if necessary, within a certain limit, while still maintaining the proper service performance.	P2
Quality Requirements (Non-functional)			
ID	**Requirement**	**Comments**	**Derived from**
REQ-MAN-35	The system shall provide uninterrupted connection	In an emergency scenario availability of the service is a key	P1

	between the MC service components	requirement for the communications.	
REQ-MAN-36	The system shall support specific VNF scale up or down	Service scale-up or down shall be necessary if the service initial sizing does not respond to the current number of solicitations and the traffic type.	P1, P2
REQ-MAN-37	The system shall support multiple NFVI geographically distributed PoP	The distributed Point of Presence will be deployed at the main and the edge cores	P1, P2
REQ-MAN-38	The system shall on-board and provision off-the-shelf edge servers with minimal intervention	When new infrastructure needs to be brought online, automation can be facilitated by near zero-touch provisioning using iPXE	P1
REQ-MAN-39	The slice manager should envision optimizations for proactive resource management.	The dynamics of resource demand should be modelled and optimised to anticipate to changes in its trend and proactively perform resource allocation to guarantee SLA and service continuity.	P2
REQ-MAN-40	The solution should be highly efficient in terms of energy consumption, computing resources and bandwidth.	IoT devices and edge computing nodes have limited computational capacity, limited battery power and limited network bandwidth which significantly narrows the solution space.	P2, P3
Constraints (Non-functional Requirements)			
ID	**Requirement**	**Comments**	**Derived from**
REQ-MAN-41	The system may use IPMI for remote edge server management	The Intelligent Platform Management Interface (IPMI) provides a solution to manage servers in remote physical locations regardless of the installed operating system	P1

3.5.3 Application layer requirements

Table 5 presents the application layer requirements derived from the different pilots.

Table 5: Application layer requirements

Functional Requirements			
ID	**Requirement**	**Comments**	**Derived from**
REQ-APP-01	The MC service shall support individual and group voice calls	The MC system should support a way of configuring each user profile with selected contacts and	P1

		talk groups that later on by selecting on them from the client a call will be initiated. Depending on the call type the call invitation will be either forwarded to one individual (private calls) or a group of affiliated members of the selected group (group call).	
REQ-APP-02	The MC service shall support individual and group video transmission	The MC system should support a way of configuring each user profile with selected contacts and video groups that later on by selecting on them from the client a call will be initiated. Depending on the video call type the invitation will be either forwarded to one individual (one to one video calls) or a group of affiliated members of the selected group (group video call).	P1
REQ-APP-03	The MC service shall support individual and group data transmission	The MC system should support data transmission among user profiles following the individual and group configurations.	P1
REQ-APP-04	The MC service shall support the service migration from Core to Edge and vice-versa	Whenever Edge MCS instantiation occurs, MCS Service should be operational (during migration, service continuity may not occur)	P1
REQ-APP-05	The MC service shall support the possibility to provide OTT service over private or more basic public networks	MCS may work regardless the communication QoS, using the 5G connectivity as an IP pipe.	P1
REQ-APP-06	The MC service shall support the logic for switching between unicast and multicast transmissions based on the location information provided by the different UEs.	The MC Service shall be capable of providing multicast transmission only if network does support it.	P1
REQ-APP-07	The MC service shall support affiliation procedures providing the capability to allow the user to select the active groups	Once the user profile´s contacts and talk groups are configured, the user should be able to operate within the desired group and contacts selecting them from the application GUI or by default configuration.	P1
REQ-APP-08	The MC service shall support mechanisms for traffic priority, queueing and QoS	When multiple requests occur, the determination of which user's request is accepted, and which	P1

		users' requests are rejected or queued is based upon a number of characteristics. There shall exist mechanisms at network level to prioritise between flows depending on QPP parameters and the MC service shall prioritise user-specific priority for floor control.	
REQ-APP-09	The MC service shall be able to dynamic change the traffic priority in real time depending on the urgency of the emergency situation	MC Service shall provide a mechanism for a user to either take over the floor control or upgrade the current call to a higher priority state. With both actions the user will have higher priority (e.g., MCPTT Emergency condition) to override (interrupt) the current talker. MCPTT Service also supports a mechanism to limit the time a user talks (hold the floor) thus permitting users of the same or lower priority a chance to gain the floor.	P1
REQ-APP-10	The service shall provide monitoring mechanisms to continuously check the performance and status of the service specific KPI	The service shall be able to provide KPI-related information to the monitoring module. Afterwards, the monitoring module shall send the appropriate message to the orchestrator in order to trigger the specific actions whenever the service KPI vary from their nominal values.	P1
REQ-APP-11	The MC service shall support dynamic instantiation and operation in Cloud and Edge platforms depending on the service requirements (latency, throughput, number of users, etc)	The MC VNF shall support to be run in various geographically distant NFVI hosting the service to cope with service KPI requirements.	P1
REQ-APP-12	The MC service shall support the dynamic scaling of resources during the VNF lifecycle	Service scale-up or scale-down shall be necessary if the service initial sizing does not respond to the current number of solicitations and the traffic type and the monitoring and alarm system prompt a necessity for it. This scale consists of adding or removing instances of the MC VNF.	P1
REQ-APP-13	The MC service shall protect the confidentiality and integrity	The MC service will follow 3GPP specifications in order to provide	P1

	of the data stored and transmitted	confidentiality and integrity though the integration of the Key Management server (MKS). The AES-256 key wrap algorithm as defined in RFC 3394 shall be supported for encryption of the XML key material downloaded from the KMS. Integrity protection of XMLs: It is based on XML signatures (xmlsig) and the HMAC-SHA256 signature method shall be supported	
REQ-APP-14	The MC service shall provide authentication and access control to the MCS UEs	The Identity Management Server within the MC system will provide the main point of identity, thus acts as the first entry point for the MCS authorisation and authentication.	P1
REQ-APP-15	The MC service shall provide end-to-end call and data encryption protecting the data stored and transmitted	To avoid malicious modification of the data transmitted, encryption mechanisms will be applied. Following TS 33180 definition, the media is protected with distribution of MIKEY-SAKKE I_MESSAGEs and confidentiality and data authentication are provided with AEAD_AES_128_GCM (IETF RFC 7714) in SRTP packets.	P1
REQ-APP-16	The system shall support user-to-application encryption of user data while in transit through an inner tunnel	On top of the security provided by the 5G network, there should be additional protection for the user data while in transit (voice, video or data). The security solution should include two layers of encryption terminated at the User Equipment, consisting of two nested, independent tunnels. The inner encryption component could be IPSec, TLS or SRTP, provided by VPN client, TLS-Protected server/client, SRTP endpoint/client respectively.	P1
REQ-APP-17	The system may support user-to-application encryption of user data while in transit through an outer tunnel	The outer encryption component should be a secure enough tunnel providing device authentication, confidentiality and maintaining the integrity of information, terminated at the User Equipment.	P1

REQ-APP-18	The solution should allow monitoring of security-related events	Risk management tools need ways to determine the trustworthiness of network segments, devices and processes. Monitoring data like network traffic connections and loads per source and destination, presence of known attack signatures, failure to authenticate, etc. will be used for this purpose in the network analytics.	P2
REQ-APP-19	The system should support interconnection of the AF with business-oriented applications	In an industrial environment, interconnection of the AF with business applications like CRM and ERP should be supported for a complete quality analysis	P3
REQ-APP-20	The solution should support autonomous driving capacity from point A to B.	The application is able to use images for detecting and avoiding obstacles in order to reach the point B	P3
REQ-APP-21	The solution should support real-time operation of an actuator	The application is able to operate a) Articulated arm, b) Camera with zoom, c) Probe for taking samples	P3
REQ-APP-22	The solution should support video capacity in 360º 4k 30fps	The required quality of the video is 4k (resolution) at 30fps	P3
REQ-APP-23	The solution should support at least 3 vehicles active simultaneously avoiding collisions	3 AMRs are needed to support the application. The movement of the vehicles should be coordinated so as to avoid collisions	P3
REQ-APP-24	The system should be able to terminate immediately the production procedure in case a malfunction occurs	Upon trigger from the sensor nodes regarding a malfunction, the production procedure should be terminated immediately	P3
REQ-APP-25	The system should allow monitoring of the energy status of the wireless sensor nodes	Measuring the energy levels of the sensor nodes is important to prevent node failures	P3
Quality Requirements (Non-functional)			
ID	**Requirement**	**Comments**	**Derived from**
REQ-APP-26	The MC service shall support redundant instantiation with master-slave synchronization to prevent sudden outages or infrastructure failures	When the MC service instance is present in more than one NFVI, they should synchronise to define the operating hierarchy	P1
REQ-APP-27	MCPTT Service shall provide an End-to-end MCPTT Access time less than 1000 ms for	In prearranged group call, when the voice call has to be picked up	P1

	users under coverage of the same network.	by the users, the access time should be less than one second.	
REQ-APP-28	For group and private calls where the call is already established, the MCPTT Service shall provide an MCPTT Access time less than 300 ms for 95% of all MCPTT PTT Requests.	For group calls that do not need the call to be picked up by the user, the access time should be less than 300ms.	P1
REQ-APP-29	The MCPTT Service shall provide a Mouth-to-ear latency that is less than 300 ms for 95% of all voice bursts.	Once the call stablished, the time elapsed from the emitter speaking to the receiver hearing should be less than 300ms.	P1
REQ-APP-30	AMR should not exceed more than 1 minute taking the sample	The solution should be efficient in terms of time for taking samples	P3
Constraints (Non-functional Requirements)			
ID	**Requirement**	**Comments**	**Derived from**
REQ-APP-31	AMR maximum speed of 1 m/s	The solution should be efficient in terms of speed	P3
REQ-APP-32	AMR run time maximum 3 hours	The solution should be efficient in terms of consumption	P3
REQ-APP-33	AMR capacity to load is at least 50kg	The solution should be robust enough	P3
REQ-APP-34	AMR maximum dimensions are 1x1m	The solution should be compact size	P3

3.6 Mapping of requirements on pilots and use cases

The complete list of the system requirements is presented in the following Table. The category the requirements belong to can be identified by the requirement ID. Furthermore, the particular use cases in the pilots that facilitated the derivation of the requirements are also mentioned.

Table 6: Affordable5G system requirements

No.	**ID**	**Requirement**	**Derived from**	
			Pilot	**Use case**
1	REQ-NET-01	The network shall conform to 3GPP 5G network requirements, architectures and interfaces in both the 5GC and NG-RAN	ALL	ALL
2	REQ-NET-02	The system shall support operation as a 5G SNPN	ALL	ALL
3	REQ-NET-03	The system shall support O-RAN standard architecture & interfacing including the support of RIC VNFs	ALL	ALL

4	REQ-NET-04	The system shall support 3GPP release Rel 15 SA	ALL	ALL
5	REQ-NET-05	The system may support 3GPP release Rel 16 SA	ALL	ALL
6	REQ-NET-06	The system shall support control and user plane separation in the 5GC and deployment of the UPF (and DN) in both core and edge (MEC).	ALL	ALL
7	REQ-NET-07	The system shall support control and user plane separation in the NG-RAN	ALL	ALL
8	REQ-NET-08	The system shall support configuration and placement of the CU-UP, UPF and DN per slice	ALL	ALL
9	REQ-NET-09	The system shall support Multi-Operator CU and DU HW and NFVi	ALL	ALL
10	REQ-NET-10	The system shall support several synchronization means: GNSS, PTP and SyncE	ALL	ALL
11	REQ-NET-11	The system shall support MIMO functionality	ALL	ALL
12	REQ-NET-12	The system shall support virtualised RAN functions	ALL	ALL
13	REQ-NET-13	The system shall support virtualised CN functions	ALL	ALL
14	REQ-NET-14	The system shall support Multi Band and Multi Operator RRU (MORAN & MOCN)	ALL	ALL
15	REQ-NET-15	The core network should be able to respond to any QoS solicitation from the Application Function to assure the service performance.	ALL	ALL
16	REQ-NET-16	The Core Network should report System KPI to the monitoring system.	ALL	ALL
17	REQ-NET-17	The system shall support inter 5G cells mobility	ALL	ALL
18	REQ-NET-18	The system shall support virtualised or cloud-native deployment & orchestration on open COTS hardware for NG-RAN	ALL	ALL
19	REQ-NET-19	The system shall support Ethernet based fronthaul with TSN functionality	ALL	ALL
20	REQ-NET-20	The system shall support operation in the TS 38.101-1 Frequency Range 1 FR1 (410-7125 MHz) bands including support for bands n77 and n78.	ALL	ALL
21	REQ-NET-21	The system may support operation in the TS 38.101-2 FR2	ALL	ALL

22	REQ-NET-22	In the NG-RAN, the RU/DU/CU network functions shall support HLS/LLS split architecture to support multi-vendor RAN using open interfaces.	ALL	ALL
23	REQ-NET-23	Security mechanisms shall span across the CN and RAN and shall be compliant to 5G security architecture	ALL	ALL
24	REQ-NET-24	The system shall support authentication of the UEs and authentication of the network towards the user	ALL	ALL
25	REQ-NET-25	Access to the private 5G network shall be restricted to authorised UEs and processes only.	ALL	ALL
26	REQ-NET-26	O-RAN Operations and Maintenance Interface (O1) shall be protected	ALL	ALL
27	REQ-NET-27	O-RAN Management A1 interface shall be protected	ALL	ALL
28	REQ-NET-28	Open Fronthaul M-Plane interface shall be protected	ALL	ALL
29	REQ-NET-29	3GPP E1 interface shall be protected	ALL	ALL
30	REQ-NET-30	3GPP F1 interface shall be protected	ALL	ALL
31	REQ-NET-31	The system shall be able to detect network failures and malfunctions	ALL	ALL
32	REQ-NET-32	The transport network shall provide failure recovery mechanisms	ALL	ALL
33	REQ-NET-33	The transport network shall provide a delay less than 10 ms.	ALL	ALL
34	REQ-NET-34	The transport network shall provide at least a throughput of 100 Mbps.	ALL	ALL
35	REQ-NET-35	The transport network shall guarantee high availability	ALL	ALL
36	REQ-NET-36	The NG-RAN may support Real time security Event Logging	ALL	ALL
37	REQ-NET-37	The system shall be able to detect security threats	ALL	ALL
38	REQ-NET-38	The system may support operation as PNI-NPN	P1	ALL
39	REQ-NET-39	The system shall support small outdoor cells capabilities	P1	ALL
40	REQ-NET-40	The system shall support remote management and separate management domain per operator.	P1	ALL

41	REQ-NET-41	The system shall support national roaming functionality	P1	ALL
42	REQ-NET-42	The system may provide integrity protection of the user data between the UE and the gNB	P1	ALL
43	REQ-NET-43	The system shall prevent the user terminal from connecting to lower security networks	P1	ALL
44	REQ-NET-44	The system should support data collection from NFs residing on the core and access part of the 5GS	P3	UC1
45	REQ-NET-45	NWDAF should be supported for network load performance computation and future load prediction	P3	UC2
46	REQ-NET-46	The NWDAF should support subscriptions from multiple network elements and entities	P3	UC2
47	REQ-NET-47	The NWDAF should deliver event information and predictions to its subscribers	P3	UC2
48	REQ-NET-48	The system should support intelligent processing of collected data	P3	UC1
49	REQ-NET-49	The system shall support interconnection of the AF with the NWDAF	P3	UC2
50	REQ-NET-50	The 5G system shall support prioritisation of critical messages	P3	UC2
51	REQ-NET-51	The 5G system should be totally compatible with TSN domain	P3	UC1
52	REQ-NET-52	The infrastructure shall support high performance Ethernet applications	P3	UC1
53	REQ-NET-53	The 5G system shall support dense UE deployment	P3	UC2
54	REQ-NET-54	A large number of AMRs should be supported in a limited geographical area (dense deployment)	P3	UC1
55	REQ-NET-55	The system shall provide confidentiality protection of user data between the UE and the gNB	P1	ALL
56	REQ-NET-56	A centralised solution should allow to register specific users (authentication) under specific roles (authorisation), while keeping a log of all access attempts to external reference points	P2	ALL
57	REQ-NET-57	The solution shall guarantee the data transport between the CN and the Edge network within pre-determined levels of goodput and latency that suite the service.	P2	ALL

58	REQ-NET-58	The 5G system shall support high-bandwidth streams from a massive set of devices with a user experienced data rate of up to 100 Mbit/s	P3	UC2
59	REQ-NET-59	RUs and DUs should be deployed according to the scheduled task that may require communication either with distant AMRs or link establishment in harsh conditions	P3	UC1
60	REQ-NET-60	RU and DUs should be deployable in GNSS-less environment	P3	UC1
61	REQ-MAN-01	The architecture shall provide 5G network slicing to support services with diverse QoS requirements	ALL	ALL
62	REQ-MAN-02	The solution should be able to establish network slices that are extended from the RAN (ingress point) up to the Core of the network (egress point).	ALL	ALL
63	REQ-MAN-03	The system shall provide a way to create, instantiate, update and delete Network Slices	ALL	ALL
64	REQ-MAN-04	The system shall support several slices over the same infrastructure	ALL	ALL
65	REQ-MAN-05	The system shall support management of slices in an end-to-end fashion	ALL	ALL
66	REQ-MAN-06	The system shall support Multi-Access Edge Computing (MEC)	ALL	ALL
67	REQ-MAN-07	The system shall support MEC deployment topology in the RAN	ALL	ALL
68	REQ-MAN-08	The system shall support the provision of the MEC stack installation and configuration.	ALL	ALL
69	REQ-MAN-09	The system shall support orchestration of services as well as lifecycle management.	ALL	ALL
70	REQ-MAN-10	The service orchestrator shall be connected to the system monitoring and to the infrastructure involved in the necessary actions.	ALL	ALL
71	REQ-MAN-11	The system shall provide an interface to manage the lifecycle of the edge server	ALL	ALL
72	REQ-MAN-12	The system shall be able to configure the HW for specific workloads	ALL	ALL
73	REQ-MAN-13	The system shall provide an interface to manage the lifecycle of the VNF	ALL	ALL
74	REQ-MAN-14	The system shall support VNF lifecycle management at cloud-level platforms as well as low-end devices	ALL	ALL

75	REQ-MAN-15	The Network Service lifecycle manager shall guarantee the sequencing of the instantiation actions.	ALL	ALL
76	REQ-MAN-16	The Network Service Lifecycle manager shall monitor the instances.	ALL	ALL
77	REQ-MAN-17	Network Service Lifecycle shall follow up the instantiation phases, network configuration and final up and running.	ALL	ALL
78	REQ-MAN-18	The solution should provide an environment for running software for data processing and service provisioning of multiple NFV services.	ALL	ALL
79	REQ-MAN-19	The solution should be able to provide real-time KPIs to the Orchestration platform mainly related to the QoS of services in order to guarantee SLAs.	ALL	ALL
80	REQ-MAN-20	The slice shall respond to application service requirements	ALL	ALL
81	REQ-MAN-21	The system shall provide monitoring mechanisms to continuously check the performance and status of the active slices	ALL	ALL
82	REQ-MAN-22	The system shall provide monitoring mechanisms to continuously check the performance and status of the active VNFs	ALL	ALL
83	REQ-MAN-23	The system shall provide monitoring mechanisms to continuously check the performance and status of the active edge servers	ALL	ALL
84	REQ-MAN-24	The system shall provide monitoring mechanisms to continuously check the performance and status of the VIMs	ALL	ALL
85	REQ-MAN-25	The system shall provide monitoring mechanisms to continuously check the performance and status of its own system health.	ALL	ALL
86	REQ-MAN-26	The system shall ensure the isolation of the slices	ALL	ALL
87	REQ-MAN-27	The system shall support the provision of different bare metal OS to the edge servers	ALL	ALL
88	REQ-MAN-28	The system shall detect VNF health-issues and trigger pre-defined recovery actions	ALL	ALL
89	REQ-MAN-29	The system may support HW and SW security hardening	ALL	ALL

90	REQ-MAN-30	Edge Infrastructure shall host lightweight version of instances deployed in the main core.	ALL	ALL
91	REQ-MAN-31	The system should support services running in lightweight VMs or Docker containers.	ALL	ALL
92	REQ-MAN-32	The solution should allow the deployment of end-to-end slices able to accommodate the requirements imposed.	ALL	ALL
93	REQ-MAN-33	The system shall support QoS solicitations from the MCS	P1	ALL
95	MAN-34	The solution should be able to provide pre-determined KPIs directly to the virtualised functions of NFV services.	P2	ALL
96	MAN-35	The system shall provide uninterrupted connection between the MC service components	P1	ALL
97	MAN-36	The system shall support specific VNF scale up or down	P1	UC1
98	MAN-37	The system shall support multiple NFVI geographically distributed PoP	P1	UC2/UC3
99	MAN-38	The system shall on-board and provision off-the-shelf edge servers with minimal intervention	P1	UC2/UC3
100	MAN-39	The slice manager should envision optimizations for proactive resource management.	P2	ALL
101	REQ-MAN-40	The solution should be highly efficient in terms of energy consumption, computing resources and bandwidth.	P2	ALL
			P3	UC2
101	REQ-MAN-41	The system may use IPMI for remote edge server management	P1	UC2/UC3
102	REQ-APP-01	The MC service shall support individual and group voice calls	P1	ALL
103	REQ-APP-02	The MC service shall support individual and group video transmission	P1	ALL
104	REQ-APP-03	The MC service shall support individual and group data transmission	P1	ALL
105	REQ-APP-04	The MC service shall support the service migration from Core to Edge and vice-versa	P1	UC2/UC3
106	REQ-APP-05	The MC service shall support the possibility to provide OTT service over private or more basic public networks	P1	ALL

107	REQ-APP-06	The MC service shall support the logic for switching between unicast and multicast transmissions based on the location information provided by the different UEs.	P1	ALL
108	REQ-APP-07	The MC service shall support affiliation procedures providing the capability to allow the user to select the active groups	P1	ALL
109	REQ-APP-08	The MC service shall support mechanisms for traffic priority, queueing and QoS	P1	ALL
110	REQ-APP-09	The MC service shall be able to dynamic change the traffic priority in real time depending on the urgency of the emergency situation	P1	ALL
111	REQ-APP-10	The service shall provide monitoring mechanisms to continuously check the performance and status of the service specific KPI	P1	ALL
112	REQ-APP-11	The MC service shall support dynamic instantiation and operation in Cloud and Edge platforms depending on the service requirements (latency, throughput, number of users, etc)	P1	ALL
113	REQ-APP-12	The MC service shall support the dynamic scaling of resources during the VNF lifecycle	P1	ALL
114	REQ-APP-13	The MC service shall protect the confidentiality and integrity of the data stored and transmitted	P1	ALL
115	REQ-APP-14	The MC service shall provide authentication and access control to the MCS UEs	P1	ALL
116	REQ-APP-15	The MC service shall provide end-to-end call and data encryption protecting the data stored and transmitted	P1	ALL
117	REQ-APP-16	The system shall support user-to-application encryption of user data while in transit through an inner tunnel	P1	ALL
118	REQ-APP-17	The system may support user-to-application encryption of user data while in transit through an outer tunnel	P1	ALL
119	REQ-APP-18	The solution should allow monitoring of security-related events	P2	ALL
120	REQ-APP-19	The system should support interconnection of the AF with business-oriented applications	P3	UC2
121	REQ-APP-20	The solution should support autonomous driving capacity from point A to B.	P3	UC1

122	REQ-APP-21	The solution should support real-time operation of an actuator	P3	UC1
123	REQ-APP-22	The solution should support video capacity in 360º 4k 30fps	P3	UC1
124	REQ-APP-23	The solution should support at least 3 vehicles active simultaneously avoiding collisions	P3	UC1
125	REQ-APP-24	The system should be able to terminate immediately the production procedure in case a malfunction occurs	P3	UC2
126	REQ-APP-25	The system should allow monitoring of the energy status of the wireless sensor nodes	P3	UC2
127	REQ-APP-26	The MC service shall support redundant instantiation with master-slave synchronization to prevent sudden outages or infrastructure failures	P1	UC2/UC3
128	REQ-APP-27	MCPTT Service shall provide an End-to-end MCPTT Access time less than 1000 ms for users under coverage of the same network.	P1	ALL
129	REQ-APP-28	For group and private calls where the call is already established, the MCPTT Service shall provide an MCPTT Access time less than 300 ms for 95% of all MCPTT PTT Requests.	P1	ALL
130	REQ-APP-29	The MCPTT Service shall provide a Mouth-to-ear latency that is less than 300 ms for 95% of all voice bursts.	P1	ALL
131	REQ-APP-30	AMR should not exceed more than 1 minute taking the sample	P3	UC1
132	REQ-APP-31	AMR maximum speed of 1 m/s	P3	UC1
133	REQ-APP-32	AMR run time maximum 3 hours	P3	UC1
134	REQ-APP-33	AMR capacity to load is at least 50kg	P3	UC1
135	REQ-APP-34	AMR maximum dimensions are 1x1m	P3	UC1

4 CONCLUSIONS

The deliverable presented the approach that has been followed in T1.1 “Pilots description and Technical requirements” for specifying the functionality that the Affordable5G system should provide in order to enable cost-efficient roll-out of 5G private and enterprise networks. Towards this end, analysis of the 5G private networks was provided, three relevant pilots and associated use cases were described, and the requirements that the Affordable5G system should fulfil with respect to the support of 5G private networks were presented.

The analysis of the 5G networks addressed issues regarding their deployment and limitations, as well as their potential to drive innovation of private internet services. In addition, business opportunities for private 5G networks solutions were discussed and relevant developments and activities in the context of 5G PPP projects, alliances, fora and working groups were described.

The potential of private and enterprise networks to support a variety of services and applications was presented through carefully selected pilots and use cases, which will be used to validate and demonstrate the technical developments that will take place in the project. The three pilots addressed different deployment scenarios and system capabilities with the goal to support emergency communications, smart city edge-related services and applications relevant to industrial and manufacturing environments.

The elaboration on the use cases and pilots’ elements, as well as the recent work of the 3GPP, O-RAN, MEC and NFV MANO communities, was exploited for the derivation of the Affordable5G system requirements. Also, security considerations were addressed to elicit top-level requirements. The analysis of these requirements showed that several of them are common across the three pilots and the respective use cases and deployment scenarios. This set of system requirements will provide the basis for the development of the common Affordable5G architecture that will take place in the context of T1.2. The specification of the requirements also provides a guide for the initial work that is being performed in WP2 regarding the hardware equipment optimization and resource sharing, as well as in WP3 on open software platforms.

REFERENCES

[1] 3GPP TR 38.825, “Study on NR industrial Internet of Things (IoT),” 2018.

[2] 3GPP TR 23.791, “Study of enablers for Network Automation for 5G,” 2017.

[3] 3GPP TS 22.280, “Mission Critical Services Common Requirements (MCCoRe); Stage 1,” 2016.

[4] 3GPP TR 22.804, “Study on Communication for Automation in Vertical domains (CAV),” 2017.

[5] 3GPP TS 33.501, “Security architecture and procedures for 5G System,” 2017.

[6] 3GPP TR 21.915, “Release description; Release 15,” 2019.

[7] 3GPP TR 21.916, “Release description; Release 16,” 2018.

[8] 3GPP TR 28.807, “Study on management aspects of Non-Public Networks (NPN),” 2019.

[9] ETSI, “Network Functions Virtualisation (NFV) Release 3; Management and Orchestration; Functional requirements specification,” ETSI GS NFV-IFA010, 2019.

[10] O-RAN alliance, “Operator Defined Open and Intelligent Radio Access Networks,” 2019. [Online]. Available: https://www.o-ran.org/.

[11] LF EDGE, “Akraino,” [Online]. Available: https://www.lfedge.org/projects/akraino/.

[12] KubeEdge, “KubeEdge,” [Online]. Available: https://kubeedge.io.

[13] OSM, “Open Source MANO,” [Online]. Available: https://osm.etsi.org/.

[14] 3GPP TS 23.251, “Network sharing; Architecture and functional description,” 2015.

[15] 5GCity, “5GCity,” 2017. [Online]. Available: https://5g-ppp.eu/5g-city/.

[16] 5G-ESSENCE, 2017. [Online]. Available: https://www.5g-essence-h2020.eu/.

[17] 5G-MoNArch, 2017. [Online]. Available: https://5g-monarch.eu/.

[18] 5G-PICTURE, 2017. [Online]. Available: https://www.5g-picture-project.eu/.

[19] 5G-SMART, 2019. [Online]. Available: https://5g-ppp.eu/5g-smart/.

[20] 5Growth, 2019. [Online]. Available: https://5g-ppp.eu/5growth/.

[21] 5Growth, “Deliverable D3.2: Specification of ICT17 in-house deployment,” 2020. [Online]. Available: https://5growth.eu/wp-content/uploads/2020/04/D3.2-Specification_of_ICT17_in-house_deployment.pdf.

[22] 5G-Clarity, 2019. [Online]. Available: https://5g-ppp.eu/5g-clarity/.

[23] 5GZORRO, 2019. [Online]. Available: https://www.5gzorro.eu/.

[24] Fudge-5G, 2020. [Online]. Available: https://5g-ppp.eu/fudge-5g/.

[25] 5G-Records, 2020. [Online]. Available: https://5g-ppp.eu/5g-records/.

[26] 5G-ACIA, 2020. [Online]. Available: https://www.5g-acia.org/.

[27] 5G-ACIA, "5G Non-Public Networks for Industrial Scenarios (White Paper)," 2019.

[28] 5G-ACIA, "Security Aspects of 5G for Industrial Networks (White Paper)," 2020.

[29] 5G-ACIA, "Exposure of 5G Capabilities for Connected Industries and Automation Applications," 2020.

[30] 3GPP TS 23.501, "System Architecture for 5G System; Stage 2 (clauses 4.4.8, 5.27, 5.28, Annex H, Annex I on support for TSN and clauses 5.6.10.2, 5.7.6.3, 5.8.2.5.3 on Ethernet forwarding)," 2017.

[31] 3GPP TS 23.502, "Procedures for the 5G System (version 15.2.0 Release 15)," 2017.

[32] 3GPP TS 22.261, "Service requirements for next generation new services and markets (version 15.5.0 Release 15)," 2017.

[33] 3GPP TS 23.503, "Policy and charging control framework for the 5G System (5GS); Stage 2," 2017.

[34] O-RAN, "O-RAN specifications lead the telecom industry towards Open and Intelligent Radio Access Networks," 2020. [Online]. Available: https://www.o-ran.org/specifications.

[35] TIP, "Telecom Infra Project," 2016. [Online]. Available: https://telecominfraproject.com/.

[36] O-RAN-SC, "O-RAN Software Community," 2020. [Online]. Available: https://o-ran-sc.org/.

[37] SmallCellForum, "Small Cell Forum," 2020. [Online]. Available: https://www.smallcellforum.org/.

[38] SmallCellForum, "Private Cellular Networks with Small Cells," 2020.

[39] OpenAirInterface, "5G software alliance for democratising wireless innovation," 2020. [Online]. Available: https://www.openairinterface.org/.

[40] Open5GCore, "Open5GCore – The Next Mobile Core Network Testbed Platform," 2020. [Online]. Available: https://www.open5gcore.org/.

[41] TCCA, "Critical Communications Association," 2020. [Online]. Available: https://tcca.info/.

[42] GSMA, "GSMA," 2020. [Online]. Available: www.gsma.com.

[43] GSMA, "Mobile Networks for Industry Verticals: Spectrum Best Practice," 2020.

[44] CBRS Alliance, "CBRS Alliance," 2020. [Online]. Available: https://www.cbrsalliance.org/.

[45] IEEE Future Networks, "IEEE Future Networks : Enabling 5G and Beyond," 2020. [Online]. Available: https://futurenetworks.ieee.org/.

[46] IEEE, "IEEE Future Directions," 2020. [Online]. Available: ieee.org/futuredirections.

[47] 5G Americas, "5G Americas: The Voice of 5G & LTE for the Americas," 2020. [Online]. Available: https://www.5gamericas.org/.

[48] 5G Americas, "5G Technologies in Private Networks," 2020.

[49] Ericsson, “5G for business a 2030 market compass,” 2019.

[50] Forbes, “The Mobile industrial revolution,” 2016.

[51] KPMG, “Unlocking the benefits of 5G for enterprise customers,” 2019.

[52] Mosaic5G, “Mosaic5G Initiative, Agile 5G service platforms,” [Online]. Available: https://mosaic5g.com.

[53] European Cyber Security Organisation, “Cyber security for the Industry 4.0 and ICS sector,” 2018.

[54] European Commission, “5G PPP phase 1 Security Landscape,” 5G PPP security WG, 2017.

[55] European Commission, “Commission Recommendation Cybersecurity of 5G networks,” 2019.

[56] 5G-MoNArch, “D6.1 – Documentation of Requirements and KPIs and Definition of Suitable Evaluation Criteria,” 2017.

[57] Ericsson, “A guide to 5G network security. Conceptualizing security in mobile communications – how does 5G fit in?,” 2018.

[58] ETSI, “NFV, Network Functions Virtualisation.,” ETSI GS NFV-SEC 003 V1.1.1 (2014-12), 2014.

[59] ETSI, “NFV, Network Functions Virtualisation,” ETSI GS NFV-SEC 006 V1.1.1 (2016-04), 2016.

[60] ETSI, “NFV, Network Functions Virtualisation,” ETSI GS NFV-SEC 013 V3.1.1 (2017-02), 2017.

[61] ETSI, “Multi-access Edge Computing (MEC); Radio Network Information API,” ETSI GS MEC 012, 2019.