Wireless Personal Communications
https://doi.org/10.1007/s11277-021-08473-5

5G for the Support of Public Safety Services

Ioannis P. Chochliouros[1] · Anastasia S. Spiliopoulou[1] · Pavlos I. Lazaridis[2] · Zaharias D. Zaharis[2] · Maria-Rita Spada[3] · Jordi Pérez-Romero[4] · Bego Blanco[5] · Hicham Khalife[6] · Ehsan Ebrahimi Khaleghi[6] · Michail-Alexandros Kourtis[7]

Accepted: 13 April 2021

Abstract

Next-generation mobile technologies are the enablers for meeting the variable specific requirements of the public safety (PS) community. In particular, due to the development of commercially deployed 5G networks, PS providers look for ways to implement related solutions upon such infrastructures, potentially in a shared use with existing commercial networks. In particular, LTE and 5G NR networks are rapidly gaining recognition as an all-inclusive critical communications platform for the delivery of both mission and business critical applications. Within this scope, we take into account the innovative architectural approach that has been proposed by the 5G ESSENCE project, addressing the paradigms of edge computing and small cell as-a-service that has been realised via a cloud-enabled small cell infrastructure leveraging multi-access technologies in 5G, where we propose a dedicated PS use case, able to offer a mission critical push-to-talk service as well as a Chat and Localisation service. Each one of these services is associated to a dedicated network slice within the scope of the corresponding fundamental 5G ESSENCE architecture and both services are provided via suitable VNFs, thus offering great flexibility to serve PS needs together. We further discuss the overall scenario deployment with the related technical enablers and the proposed functionalities, *per case*. The corresponding end-to-end slicing makes possible to allocate both radio and cloud resources to the involved critical actors, in an automated and elastic way.

Keywords 5G · Cloud enabled small cell (CESC) · Mission-critical (MC) applications · Messaging and localisation service · Mission-critical push-to-talk (MCPTT) · Network function virtualisation (NFV) · Network slicing · Public safety (PS) networks · Software-defined radio (SDN) · Small cell (SC)

1 Introduction

Commercial cellular networks have been driven by the needs of consumer and business users. The success of cellular has led to excellent economies of scale and constant rapid innovation. This environment has produced advanced standards such as LTE (Long Term

✉ Zaharias D. Zaharis
z.zaharis@hud.ac.uk

Extended author information available on the last page of the article

Published online: 20 May 2021

Evolution) that provide multi-megabit per second data rates and multimedia capabilities as well as traditional voice and messaging services. Public Safety (PS) users have traditionally operated with voice-based communication systems and narrowband data services and mission critical (MC) communication systems have been implemented with dedicated networks [1]. However, it has become evident that PS users also need high-speed broadband data services and applications [2]. Although broadband solutions for PS can also be implemented as dedicated systems, in many countries this approach is limited by lack of dedicated spectrum and lack of governmental budgets. In particular, governments and organisations involved in public safety and security (PSS) are devoting great interest in the transition from existing narrowband wireless systems towards broadband [3, 4]. It now appears that the next generations of public safety radio networks are heterogeneous systems that include an LTE core network with multiple subnets and layered services [5]. When planning and building such PS-LTE networks, governments are usually taking into account the following uses and requirements [6]: (1) Converged commercial and dedicated networks that integrate; (2) combined fixed and mobile with the aim of ensuring service continuity and efficiency; (3) broadband mobile intelligent terminals to ensure service boundaries and device security; (4) quality of service (QoS) guarantees to fulfill key roles and services, and; (5) construction policies for dedicated LTE networks to account for limited budgets and guide the expansion of coverage from large, developed cities to smaller, less developed areas with lower risk profiles.

In this scope, PS operators express the need to exchange data, images and video, not only voice. Therefore, the trend is to use both commercial and PS networks to exchange information [7]. Since 2006, the 3GPP has started, in particular with Releases 12, 13 and 14 [8], to include functionalities related to mission-critical (MC) applications [9] as public safety in the mobile networks standards [10]. The term “mission critical” implicates for a certain quality -or characteristic- of a communication activity, application, service or device, that requires low setup and transfer latency, high availability and reliability, ability to handle large numbers of users and devices, strong security and priority and pre-emption handling.

With its capabilities able to “meet” the requirements for massive number of connected devices (mMTC), ultra-reliable and low-latency communications (uRLLC) and enhanced mobile broadband (eMBB), 5G is presenting itself as the ideal candidate for a mission-critical and PS solution of the “converged” future [11]. 5G is a multi-radio system built upon both new high capacity and low-latency interfaces and convergence of existing radio technologies such as 5G New Radio (NR), LTE and WiFi to a ubiquitous radio access network [12]. 5G can offer several new technologies which improve the reliability, availability and security of communications; in particular, Mobile Edge Computing (MEC), Software-Defined Networking (SDN), Network Function Virtualisation (NFV), network slicing, cloud computing and seamless integration of different radio technologies [13–15] will furthermore empower 5G to use the common infrastructure for the commercial users to create safety networks within them [10, 16]. Flexible use of radio resources [17] with the multi-connectivity technology also contributes to improved reliability [18].

The paper is organised as follows: Sect. 1 serves as a wider conceptual introduction. Section 2 discusses current PS solutions for the provision of MC applications, especially within the context of the challenges and/or the opportunities arising from the deployment of LTE and 5G infrastructures able to satisfy specific requirements for low latency. Section 3 discusses the fundamental features of the 5G ESSENCE architectural approach aiming to provide a cloud-enabled small cell infrastructure leveraging a variety of multi-access technologies in 5G for the support of multiple tenants. Section 4 discusses a proposed PS use case, based on the context of the 5G ESSENCE original approach; more specifically, we develop two separate services (i.e., a Mission Critical Push-to-Talk (MCPTT) service and a Chat and Localisation service), offered via dedicated network slices. This offers flexibility for dedicated mission critical public safety applications also at the edge of the network and practically establishes an end-to-end (E2E) service for the next generation of edge computing communication scenarios. We discuss the proposed deployment scenario, involved actors, technical enablers and corresponding functionalities. The work concludes with an overview of the proposed innovative features.

2 Current Public Safety Solutions for Mission Critical Applications

PS networks provide communications for services like police, fire and ambulance. In an emergency instant, a reliable and stable communication is the "key" to enable and support successful emergency operations. In this realm, the requirement has been to develop systems that are highly robust and can address the specific communication needs of emergency services. This has fostered public safety standards -such as TETRA and P25-providing for a set of features that were not previously supported in commercial cellular systems. These standards have also been applied to fulfill commercial critical communications needs such as airport operations. Public safety users frequently need to communicate in dynamic groups that might involve both mobile users on the scene and fixed users ("dispatchers") working in a control centre. Often these groups operate in a "push to talk" mode. However, due to their inherent bandwidth and design limitations, even the most sophisticated digital LMR (Land Mobile Radio) networks are unable to support mobile broadband and data-driven industrial IoT applications that have become vital for public safety, military, utilities, transportation, oil and gas, mining and other segments of the critical communications industry. The 3GPP-defined LTE and 5G NR standards [19] have emerged as the leading candidates to fill this void.

Proposed solutions for mission-critical applications include narrowband communication systems, such as terrestrial trunked radio (TETRA) and Tetrapol (TETRA for police) in Europe, and Project 25 (P25) in North America [1] with the related systems designed mainly for the support of voice [20]. These well-defined and largely tested PS communication services can guarantee the provision of advanced security features and of related functionalities, but are not adequately able to support the high data rates required for the growth of data traffic and the general multimedia content transmission when it is related to corresponding MC applications [21]. Mission critical users (such as police officers, border guards, civil protection staff, ambulance personnel, and fire and rescue) need reliable communications, high availability and security, that cannot be matched without multiple technological enablers. With suppliers now offering more LTE solutions, countries building national networks and with law enforcements' changing expectations surrounding their technology usage, it is evident broadband is the future of critical communications [22]. In the scope of the investigation for the potential integration of MC communications within commercially deployed broadband standards, as already performed by various market actors at the global level, the Long Term Evolution-Advanced (LTE-A) mobile radio technology has been assessed as a reference candidate technology, suitable for the development of the committed PS systems [7]. In fact, the 4G/4G+ mobile communications networks can satisfactorily support a variety of technologies for the provision of critical communications such as, inter-alia device-to-device (D2D) communications [23], group communications [24], direct ode communications (also referred to as proximity services (ProSe) [25], mission-critical push-to-talk (MCPTT), video and data (i.e.: MCPTT [9], MCVideo [26], MCData [27]) and end-to-end security. Preserving and/or maintaining these forms of communications within a great variety of emergency circumstances (also in cases of natural disasters or accidents) is the principal action for PS LTE/LTE+ networks [28].

However, the systems for the support of public safety as well as for the provision of mission critical facilities have been developed towards satisfying diverse aims and requirements than those that have been considered either for the advance of LTE-A or for other commercially deployed infrastructures [29, 30]. Actual trends persist upon simultaneously exploiting commercially deployed broadband networks also for the provision of MC solutions.

In any case, as the deployed commercial networks do not generally possess the high-level security and reliability that MC applications require, the 3GPP has started "addressing" these requirements as part of the LTE evolution, with the first document concerning public safety published in 3GPP Release 11 [31]. A platform for mission critical communications and MC Services has been a key priority of 3GPP and this is expected to further evolve into the future, by taking more requirements, from different sectors of the global critical communications industry [32]. The 3GPP entered the application domain by standardizing Mission Critical Push to Talk (MCPTT) in Rel-13, completed in 2016. The MCPTT Service can be used for public safety applications as well as for general commercial applications (e.g., utility companies and railways) [33, 34].

A common technological background for both commercial and dedicated public safety networks could offer many advantages and opportunities to both areas. The intended common use and sharing of the network resources can reduce costs and deployment time, while maintaining a single infrastructure supporting both commercial and MC communications [5]. The native support of (edge) cloud computing, SDN and NFV towards the concepts of network softwarisation and slicing promote 5G as the "ideal" proponent so that to "flexibly address" the needs of PS applications. Some interesting examples on how 5G networks can be exploited to realize MC PS services are presented in [10, 16]. The contribution in [16] focuses on the benefits of MEC-based architecture for MCPTT services, by proposing a hierarchical distributed MCPTT architecture that allocates the user plane (UP) at the edge, while keeping the control plane (CP) centralised for synchronisation and assistance purposes [35]. The work in [10] studies and implements the use of commercial technologies for MC services, for two important use cases, that is: (i) the first priority communication use case, where authors apply dynamic QoS management to prioritise the MCPTT application by using policy and charging rules function (PCRF) in the core network, and; (ii) the rapidly deployable network use case, where a distributed LTE network is implemented for the scenarios in which the legacy commercial network might be unavailable. However, 5G with enhanced capabilities can better support PS applications, as described next.

3 The Proposed 5G ESSENCE Approach

The 5G ESSENCE project has been oriented towards the actual demonstration of its results to real life and the vertical industries introduced by the broader 5G-PPP context. The 5G ESSENCE scope addresses the paradigms of edge computing and Small Cell as-a-Service (SCaaS) by fuelling the drivers and removing the barriers in the Small

Cell (SC) market, forecasted to grow at an impressive pace up to 2020 and beyond and to play a “key role” in the 5G ecosystem [36]. The main measurable objectives of the original 5G ESSENCE context include: (1) Full specification of critical architectural enhancements (as described in the 5G-PPP reference architecture [37]); (2) definition of the baseline system architecture and interfaces for the provisioning of a cloud-integrated multi-tenant Small Cell network and a programmable radio resources management (RRM) controller; (3) development of the centralised software-defined radio access network (cSD-RAN) controller to program the radio resources usage in a unified way for all Cloud Enabled Small Cells (CESCs); (4) development of orchestrator’s enhancements for the distributed service management in a multi-tier architecture.

In the 5G ESSENCE approach, the SC concept is evolved as not only to provide multi-operator radio access but also, to achieve an increase in the capacity and the performance of current RAN infrastructures, and to extend the range of the provided services while maintaining its agility [38, 39]. To achieve these ambitious goals, the 5G ESSENCE context leverages the paradigms of RAN scheduling and additionally provides an enhanced, edge-based, virtualised execution environment attached to the small cell, taking advantage and reinforcing the concepts of Multi-Access Edge Computing (MEC) [40] and network slicing [41, 42]. More specifically, the 5G ESSENCE project offers orchestration and CESC infrastructure sharing, which is a novel approach that has never been realised before in the international experience and bibliography. The CESC, which is composed by a SC physical network function (PNF) attached to an execution platform (i.e. micro-server) can “run” several appropriately defined Virtual Network Functions (VNFs) that correlate to the small cell functionality or to specific service-level functions. These can comprise radio specific operations, appearing as advanced scheduling algorithms, as well as network functions appearing in a virtualised form. Furthermore, data sets and metric collection for analysis and optimisation purposes, can also be incorporated.

For our case, the existing 5G architectures act as a “solid reference point” combining the current 3GPP framework for network management in RAN sharing scenarios [43] and the ETSI NFV framework [44] for managing virtualised network functions. The CESC offers virtualised computing, storage and radio resources and the CESC cluster is considered as a cloud. This cloud can also be “sliced” so that to enable multi-tenancy. The execution platform is used to support VNFs that implement the different features of the SCs as well as to support for the mobile edge applications of the end-users. By evolving the high-level architecture of 5G, the technical approach of 5G ESSENCE is presented in Fig. 1 where the working architecture is illustrated, with emphasis on the functional elements and interfaces. The proposed architecture [45–48] allows multiple network operators (tenants) to provide services to their users through a set of CESCs deployed, owned and managed by a third party (i.e., the CESC provider). In this way, operators can extend the capacity of their own 5G RAN in areas where the deployment of their own infrastructure could be expensive and/or inefficient, as it would be the case of, *for example*, highly dense areas where massive numbers of SCs would be needed to provide the expected services.

The 5G ESSENCE architectural approach [49] provides advanced network virtualisation, distributed service management and the full potential of a network embedded cloud, building upon network slicing and isolation and then by providing this capability to multiple operators or tenants [50]. It is worth noting that the abovementioned two-tier architecture of the 5G ESSENCE is well aligned with the current views on 5G architecture described by 5G-PPP, where the infrastructure programmability and the split of control and user planes are identified as two “key” logical architecture design paradigms for 5G.

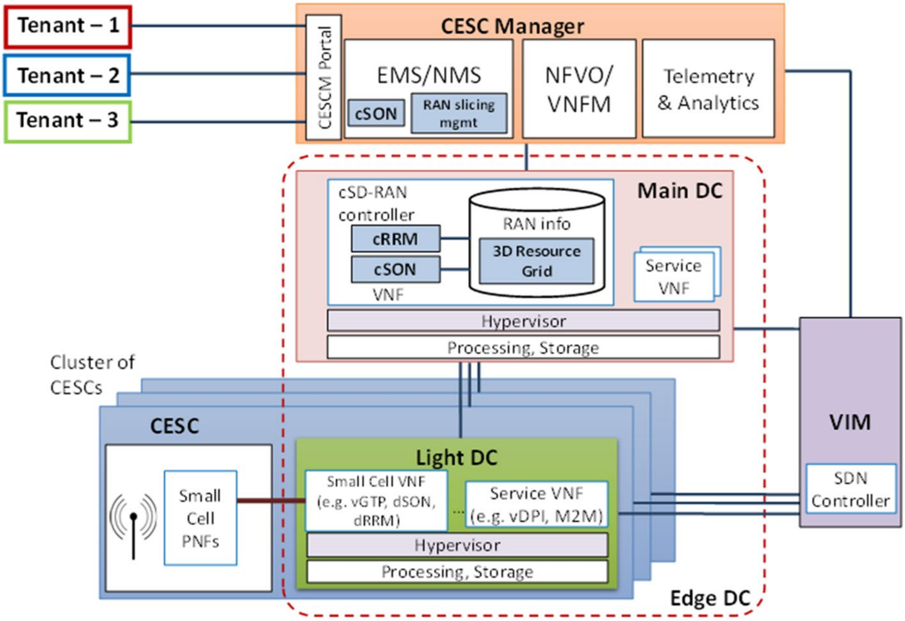

Fig. 1. 5G ESSENCE system architecture

First, 5G ESSENCE achieves infrastructure programmability by leveraging the virtualised computation resources available at the Edge DC. These resources are used for hosting VNFs tailored according to the needs of each tenant, on a per-slice basis. Second, the Main DC allows centralising and softwarising control plane small cell functions to enable more efficient utilisation of radio resources coordinated among multiple CESCs. In addition to the abovementioned aspects, 5G ESSENCE contributes to other 5G architectural concepts such as, *for example,* the realisation of the network slicing concept, which is a fundamental requirement of 5G ESSENCE for enabling that multiple tenants and vertical industries do share the same CESC infrastructure.

Latest 3GPP releases address the key requirements expressed from the Public Safety (PS) domain for next generation broadband public safety networks [51]. Further improvements to the 3GPP standards to cope with mission critical communications requirements are considered as a "central topic" in the 3GPP requirements study for 5G [52]. Regarding PS service delivery models, there is a clear trend towards different forms of network sharing models as opposed to building out dedicated PS networks [53]. Blue Light Mobile [54] service by PS operator Astrid in Belgium offers access through roaming agreements with commercial operators; FirstNet in the US, while it counts with spectrum dedicated to PS, is expected to enable secondary use by commercial applications [55]. In this context, multitenancy becomes a cornerstone challenge.

The 5G ESSENCE's common orchestration of radio, network and cloud resources can considerably support the intended implementation of the exact needs that are requested -and set- by the public safety sector, as the corresponding scope supports the use of modern tools and of related facilities for effectively sharing radio and edge computing capabilities in both localised and temporary network deployments between the PS and the commercial users. The core objective is about the suitable allocation of radio, network and cloud resources to the involved critical "actors" (like the first responders) who, by nature, necessitate for the provisioning of fully prioritised and high-quality services. Thus, the involved PS operators are shifting their their business activities from a fully owned infrastructure model to specific one where they can "act" as a Mobile Virtual Network Operator (MVNO) between various parties owning and operating mobile networks and the intended public safety end-users. This way of network deployment can also be seen as the "equivalent" of a corresponding MC slice that can be used in a variety of operators' domains. The proposed scope implicates that the involved PS operator can "purchase" connectivity to multiple legacy mobile operators aiming to provide adequate assurance and/or guarantee to his specific PS customers about the provision of a certain level of connectivity, resilience and of suitable defined QoS for the intended public safety operations. This approach can be beneficial of the participating PS operators for a variety of reasons: That is, the proposed model results to costs reduction as of buying, installing and maintaining dedicated infrastructures; in addition, adopting such solutions offers greater flexibility to the involved MVNOs to dynamically adapt their offers to their customers. In any case, this framework comes at the price of pre-negotiated contracts between MVNOs and involved legacy providers, to ensure a high availability and a guaranteed level of throughput for the participating PS users.

The 5G ESSENCE project targets the development and demonstration of an innovative architecture [45], capable of providing SC coverage to multiple operators "as-a-Service", enriched with 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 applications. To that end, 5G ESSENCE envisages to virtualize and to partition SC capacity while, *at the same time*, it aims to support enhanced edge cloud services by enriching the network infrastructure with an edge cloud. In particular, the 5G ESSENCE framework combines the MEC and NFV concepts with SC virtualisation in 5G networks [56] and enhances them for supporting multi-tenancy and for increasing the network capacity and the available computational resources at the edge [38].

At the network's edge, each CESC is able to host one or more service VNFs, directly applying to the users of a specific operator. Similarly, VNFs can be instantiated inside the Main DC (Data Centre) and be parts of a Service Function Chaining (SFC) procedure. The Light DC can be used to implement different functional splits of the SCs as well as to support the mobile edge applications of the end-users. At the same time, the 5G ESSENCE proposes the development of small cell management functions as VNFs, which run in the Main DC and coordinate a fixed pool of shared radio resources, instead of considering that each small cell station has its own set of resources. The CESC offers virtualised computing, storage and radio resources and the CESC cluster is considered as a cloud from the upper layers. This cloud can also be "sliced" to enable multi-tenancy. The execution platform is used to support VNFs that implement the different features of the SCs as well as to support for the mobile edge applications of the end-users [39].

In the context of the deployed 5G ESSENCE architectural framework [47, 48] the corresponding NFVI (Network Function Virtualisation Infrastructure) is realised across two dedicated tiers (i.e.: the Main DC and the Light DC), thus dealing with wider distribution and heterogeneity-related features. The first tier which is the Light DC hosted inside the CESCs, is used for supporting the implementation of related VNFs, thus realising the intended virtualisation features of the small cell access. This purely implicates that several suitable network functions that can support traffic interception, GTP (General Packet radio Service (GPRS) Tunneling Protocol) encapsulation/decapsulation and some distributed RRM (Radio Resource Management) / SON (Self-Organising Networks) functionalities [47] can take place therein. In addition, other potential VNFs that necessitate for lower processing power (such as a Deep

Packet Inspection (DPI), a Machine-to-Machine (M2M) Gateway and others), can be accommodated here. The linking between the SC Physical Network Functions (PNFs) and the SC VNFs can be performed through the network Functional Application Platform Interface (nFAPI). The second tier proposed by the corresponding architecture (i.e., the Main DC), can accommodate more computation-intensive tasks and processes that have to be centralised with the intention of realising a broader view of the underlying infrastructure.

This involves the cSD-RAN (centralised Software-Defined Radio Access Network) controller which is delivered as a dedicated VNF running in the Main DC and makes control plane decisions for all the radio elements in the geographical area of the CESC cluster, including the centralised Radio Resource Management (cRRM) over the entire CESC cluster, also in a multi-RAT environment. As the geographic area of the cell cluster is at the edge of the 5G network, both main and light DCs can be logically grouped together to form an edge DC. The legacy DC can be distinguished from the edge DC, being at the core of the cellular network.

The 5G ESSENCE system presents a high degree of dynamicity, due to the constantly changing behaviour of services and workloads to be supported by the radio and cloud infrastructure. From this perspective, a proper monitoring system able to adapt to the different supported scenarios is required. The data collected by the monitoring system is used for visualisation purposes (for human consumption) and it is also provided to a set of analytics techniques capable of extracting insights from the data and, via feedback loop, enabling the realisation of efficient resource allocation across the infrastructure, through the orchestration system. These are the functionalities provided by the 5G ESSENCE CESC Manager (CESCM). This module includes the components of the ETSI NFV MANO (Management and Orchestration) framework, that is the NFVO and Virtual Network Function Manager (VNFM) for carrying out the lifecycle management of network services and VNFs, the Element Management System (EMS) / Network Management System (NMS) for carrying out the management of the deployed CESCs in terms of Fault, Configuration, Accounting, Performance, Security (FCAPS) operations, and a telemetry and analytics module that collects and analyses relevant indicators of the network operation [46]. The CESCM is responsible for coordinating and supervising the use, the performance, and the delivery of both radio resources and services. It controls the interactions between the infrastructure (CESCs, Edge DC) and the network operators. In addition, it handles Service Level Agreements (SLAs) while, *on an architectural basis*, the CESCM encompasses telemetry and analytics as fundamental tools for efficiently managing the overall network.

The Virtualised Infrastructure Manager (VIM) is responsible for controlling and optimising the operation of the NFV Infrastructure (NFVI), which includes the computing, storage and network resources of the Edge DC.

The Orchestration module includes the Service Orchestrator (SO) and the Resource Orchestrator (RO) as part of Open Source MANO (MANagement and Orchestration) [57], in charge of configuring in one go, both the compute resources and the network resources, and the Virtual Infrastructure Manager (VIM) in combination with OpenStack [58], taking care of the computing resources, and OpenDaylight [59], taking care of flows, connections and communication between VNFs (and maybe other resources).

4 Use Case Description

4.1 Conceptual Approach

The 5G ESSENCE aims at significantly contributing to the achievement of the requirement of the PS sector by providing a highly flexible and scalable platform, based on edge cloud computing and small cells. Therefore, instead of owning a dedicated infrastructure to provide PS services, which entails high costs of buying, installing and maintaining infrastructure elements, PS operators have already started moving their business to a Mobile Virtual Network Operator (MVNO) paradigm. This can manage the allocation of resources to the critical actors, requiring prioritised and high-quality services. Therefore, the proposed use case has special requirement reflected in the implementation of E2E slicing, elastic resource allocation, operability of the service in emergency situations and also high service quality of experience (QoE).

5G ESSENCE's common orchestration of radio, network and cloud resources is expected to fully "meet" the requirements of the PS sector. The objectives to properly support a PS application are the following: (1) The priority access of first responders to the 5G ESSENCE enabled platform and, more generally, to a virtualised communication infrastructure; (2) the dimensioning and elastic resource allocation to first responders of radio, network and cloud resources in case of emergency; (3) the integration of first responders' deployable communications systems (macro base-stations, multi-RAT devices) to the 5G ESSENCE platform, and; (4) the hosting of MC applications and virtualised EPC (Enhanced Packet Core) to Edge DC for extremely low latency [60], as low latency is crucial to ensure applications are usable and interactive whether human-to-human, human-to-machine or machine-to-machine (M2M) communication.

In the 5G ESSENCE we focus on two mission critical services: first on the Mission Critical Push-To-Talk (MCPTT), and second on the mission critical messaging (chat) and localisation service. We can conceptually sum up the process of those two services as follows:

- The 5G ESSENCE platform owner provides the required network slices [61] to different tenants.
- Allocation of data rates is made by the SD-RAN controller in accordance with the cloud resources already allocated in the Edge DC by the VIM. In case of emergency, the Cloud Edge Small Cell will add new resources taking into consideration the request, close-to-zero delay and maintaining the connection even if the backhaul is damaged. Moreover, 5G ESSENCE SD-RAN controller will enforce the priority access of first-responders by extending the slices to the radio part, thus creating the end-to-end slices that isolate those responders from other parties' communications.
- In case that ICT infrastructure is damaged, we will maintain the operability of the services by deploying the control plane in the edge. Therefore, when the backhaul connection is damaged, we will display a new CESC to mitigate the damage in the macro base stations (BSs).

Figure 2 illustrates the different components involved in the service of MCPTT. MCPTT is a public safety mission-critical voice communication type [62], aimed at the coordination of emergency teams that are organised in groups [33]. It provides an arbitrated method by which two -or more- users may engage in communication. Users may request permission

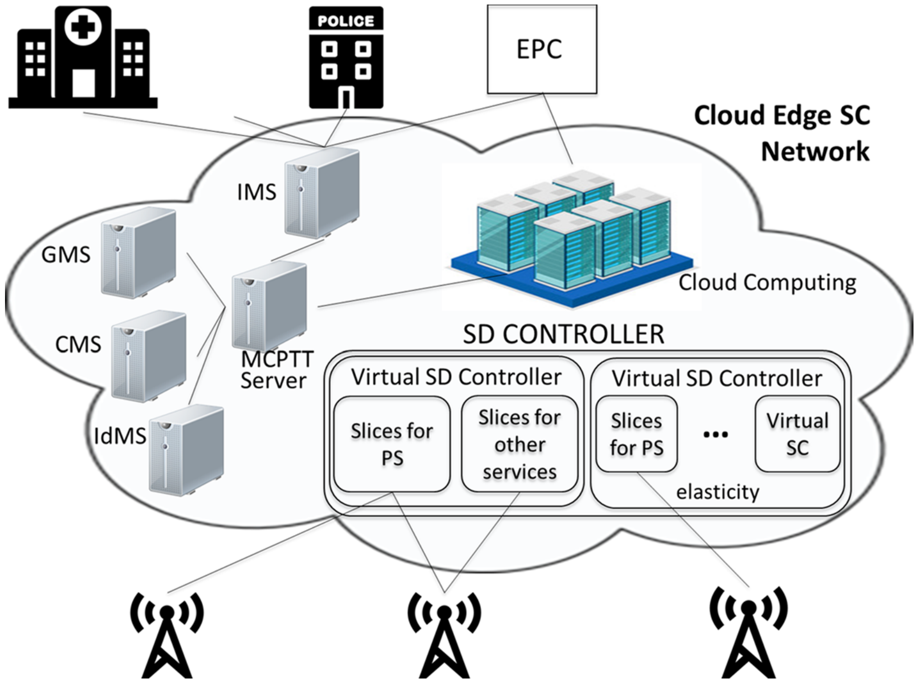

Fig. 2 Components involved in a MCPTT for PS deployment

to transmit (e.g., traditionally by means of a press of a button) and the MCPTT service provides a deterministic mechanism to arbitrate between requests that are in contention (i.e., floor control). When multiple requests occur, the determination of which user's request is accepted and which users' requests are rejected -or queued- is based upon a number of characteristics (including the respective priorities of the users in contention). Besides, the MCPTT service provides a means for a user with 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. As it appears, the management of this type of half-duplex communications is not trivial, since it requires an appropriate management of priorities and privileges to allow communication. The standardised MCPTT service imposes special requirements that include, *among others*, high availability and reliability, very low latency, support for one-to-one and group calls, talker identification and high audio quality for clear interchange of information. 5G ESSENCE's common orchestration of radio, network and cloud resources, significantly contributes to the fulfilment of the tight requirements of a MCPTT service, providing the tools to share both radio and edge computing capabilities between mission critical and commercial users [63]. The MCPTT network service is composed of different VNFs to optimize the usage of the resources. The main challenge consists on transparently and elastically allocating the available resources to the variety of actors requiring different services with different priorities in space and time. To that aim, the network slicing based on virtualisation techniques makes it possible to modify the network behaviour by changing functions or reconfiguring parameters.

The MCPTT service includes an MCPTT server at the network side, an IMS (IP Multimedia Subsystem), a DNS (Domain Name System) and an HSS (Home Subscriber Server).

Moreover, the MCPTT server can be brought near to the user to achieve a distributed and scalable approach. These functionalities can actively "run" as corresponding VNFs in the Main DC as they are common to all the CESCs in a service area. Subsequently, the MCPTT client can be hosted at each user equipment (UE). According to this approach, the creation of network slice 1 involves the instantiation of the abovementioned VNFs, done through the NFV MANO entities (i.e.: the NFVO (NFV Orchestrator), the VNFM (VNF Manager) and the VIM), and the instantiation of a RAN slice that provides a certain capacity to support the MCPTT transmissions at the radio interface, configured by the RAN slicing management function (a number of descriptors that specify the operation of the RRM algorithms). The services to support MCPTT are the following sort of calls, as described below:

- *Group calls* (with preemption for priority): to start a group call, the caller just selects the target group, presses the PTT (Push-to-Talk) button, speaks and the voice message is delivered instantly).
- *Private calls*, realised in a one-to-one manner.
- *Emergency calls*: These are pre-emptive calls due to an emergency condition. Following to a request for the realisation of an emergency call, on-going calls can be terminated so that to "free-up" resources for a higher priority call.

The MCPTT Network Service is composed of different VNFs that complete the mission critical push-to-talk service. This service is defined in multiple VNFs to optimize the usage of the resources, as described below:

- *VNF—IMS* is a virtualised IMS architecture required to provide the MCPTT service. MCPTT is an IP-based MC service that requires of a Session Initiation Protocol (SIP) core such as IP Multimedia Subsystem (IMS) to operate. Currently, this is implemented as a centralized subsystem attached to the Evolved Packet Core (EPC) of each operator. In the case that the MCPTT service was deployed over a network infrastructure already having IMS, this VNF would not be necessary and the MCPTT services would be attended by the network infrastructure provider.
- *VNF—CSC (Common Service Core):* An MCPTT service may rely on other auxiliary servers in order to manage status information about the service such as Group Management Server (GMS), Identity Management Server (IDMS), Key Management Server (KMS) and Configuration Management Server (CMS).
- *VNF—MCPTT AS (Application Server):* This entity provides centralised support for MCPTT services. The MCPTT server functional entity is supported by the SIP Application server (AS), HTTP client and HTTP server functional entities of the signalling control plane. The MCPTT server can support the controlling role and the participating role. The MCPTT server may perform the controlling role for private calls and group calls. The MCPTT server performing the controlling role for a private call or group call may also perform as participating role for the same private call or group call. For each private call and group call, there shall be only one MCPTT server assuming the controlling role, while one or more MCPTT servers in participating role may be involved. The MCPTT server performing the controlling role is responsible for: call control towards all the MCPTT users of the group call and private call; interfacing with the group management server for group policy and affiliation status information of this MCPTT server's served affiliated users; managing floor control entity in a group call and private call, and; managing media handling entity in call (i.e. conferencing,

transcoding). The MCPTT server performing the participating role is responsible for: call control to its MCPTT users for group call and private call; group affiliation support for MCPTT user, including enforcement of maximum number of simultaneous group affiliations by a user; relaying the call control and floor control messages between the MCPTT client and the MCPTT server performing the controlling role, and; media handling in call for its MCPTT users, that is transcoding, recording, lawful interception for both unicast and multicast media.

- *VNF—DNS:* This separates the DNS server from the MCPTT service VNF. This means that, from this point, any MCPTT service will need an external virtualised DNS server. This DNS server could be hierarchically arranged with other DNS servers in the network.

With the large impact of the latest advances in the IT and Internet communication tools, the Mission Critical domain has started to shift from an exclusively voice based communication model to a more rich and diversified interaction model. In fact, the success of chatting has motivated the interest of Public Safety operators in these modern services. Therefore, ensuring consistent chat services can be evaluated as an indispensable communication tool during intended rescue operations. As the rapid and indisputable growth of various communication *Apps* (such as *WhatsApp*, *Slack*, *Telegram*, *Viber*, *Facebook* communicator, hangout and many others) is perceived at the global level, first responders look for innovative communication modes allowing for efficient distribution of data (including text and images) to variable "actors" being present on the emergency scene. Definitely, the group communication feature in these applications do compose a useful means for distributing content to first responders groups and also between them. Nevertheless, these broadly used applications depend upon a centralized architecture that cannot deal with the high degree of resilience required in a situation of emergency.

What is more, the one to many communication patterns allowed by these applications, the facility in creating and modifying groups as well as the diversity of content these tools allow (text, and multimedia) constitute new features of high interest for mission critical operations, intensively relying on software and web based highly distributed frameworks; these new applications can be easily deployed on top of the 5G ESSENCE architecture. Furthermore, these frameworks can take advantage of the virtualisation of resources and infrastructures since they are based on software components that can be easily deployed in containers or eventually as VNFs. As of the localisation and messaging service, the proposed solution, called as *FeedSync (FS)*, is based upon an innovative publish subscribe modular solution that operates on top of the 5G ESSENCE leveraging the flexibility of 5G architecture. FeedSync is a web server application for content distribution; it is deployed on a classical server and interacts with a database system management for storing data. The whole system is delimited by the corresponding server and the database, where the former delivers a suitable interface for interacting with client applications (web and mobile device applications) in diverse settings. FeedSync can be simultaneously deployed on various servers and the content can be distributed. The corresponding synchronisation function is realised through the data base system, while an offline mode is also offered by the client-side database. When a connection link is lost, each connected device can have a client database management and can continue storing new content within, until the server is back online, and the synchronisation is activated again. In addition to classical chat services, FeedSync ensures a set of features including, among others: Blue Force Tracking (BFT) information; geo-located multi-part content; direct communications between terminals; capability to share content; management service, and; geo-content management.

From a standardisation perspective, this solution ensures compatibility with current and future standards, by operating as an application on top of the 5G ESSENCE architecture. Moreover, being completely relying on software allows easy virtualisation and deployment of this framework leveraging the SDN and VNF paradigms. Messaging and Localisation is implemented as an application on the top of the 4G/5G stack. The FeedSync can be assessed as a sort of a classical IP-based application in the 5G ESSENCE architecture. The Chat and Localisation Application is used with the aim of demonstrating ways about how the first responders can use services on the field, deployed as close as possible, and simultaneously enabling high throughput and low latency. More interestingly, our virtualised approach enables "on-the-fly" deployment of new resources close to the users as envisaged by the 5G ESSENCE approach. What is more, instantiated resources can be "tailored" to the capacity of the hosting hardware in the sense that light versions of our application are favored when it comes to instantiating services in small cells and light DC, as highlighted in Fig. 3.

4.2 Stakeholders and Overall Scenario Deployment

The involved stakeholders for the realisation of the above services are listed as described below; although the selection has been done in a way to be conformant to the specific scope of the context structured within the original 5G ESSENCE context, it remains more generic and able to serve many similar scenarios of use. We distinguish the following involved "actors":

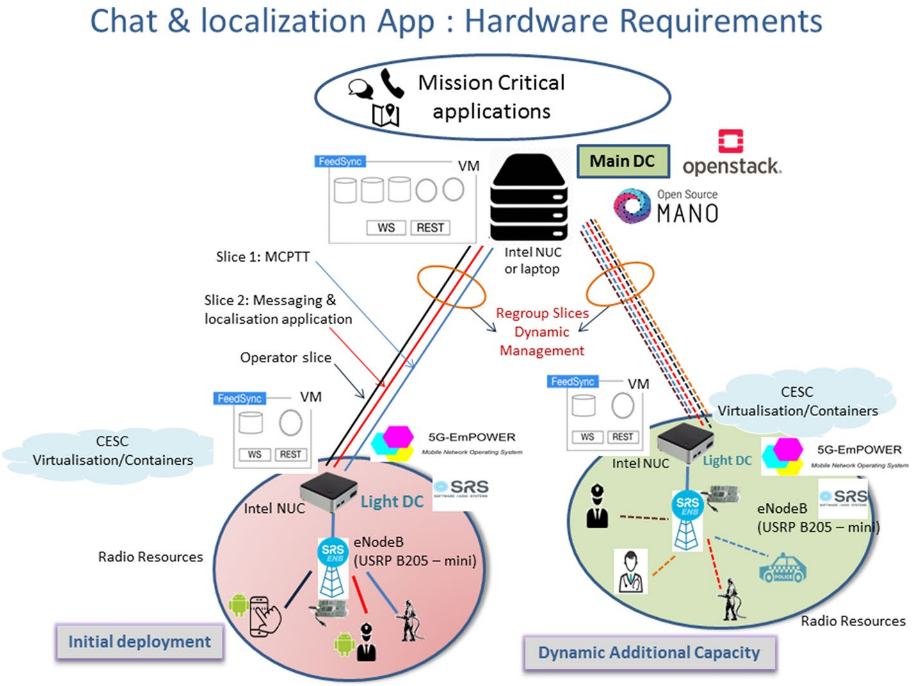
Chat & localization App : Hardware Requirements
Mission Critical applications
FeedSync
VM
WS
REST
Main DC
openstack.
Open Source MANO
Intel NUC or laptop
Slice 1: MCPTT
Slice 2: Messaging & localisation application
Operator slice
Regroup Slices Dynamic Management
CESC Virtualisation/Containers
5G-EmPOWER
Mobile Network Operating System
SRS
Intel NUC
Light DC
eNodeB (USRP B205 – mini)
Radio Resources
Initial deployment
Dynamic Additional Capacity

Fig. 3 Mapping of the 5G ESSENCE architecture to a PS deployment FOR messaging and localization

- *A legacy mobile operator (platform owner)* offering its infrastructure to classical end-users as well as to PS virtual operators. Note here that virtual operators can rely on multiple legacy operators for additional guarantees.
- *A PS operator* that offers connectivity services with strict QoS guarantees to First Responders. (Note that in our situation we can have multiple virtual operators each offering a "separate" slice for a different First Responder Agency).
- *First Responder 1* (i.e.: firefighters) are end-users exploiting the connectivity offered by a PS operator through a dedicated slice. For the sake of demonstration, firefighters use MCPTT application for their communications.
- *First Responder 2* (i.e.: paramedics) are another set of end-users relying on the same PS operator or another slice coming from a different operator, in order to exchange chat messages as well as preregistered pictures for situation assessment.
- *Legacy end-users* constitute classical user that have subscribed to the legacy operator communication and Internet data offers. They are not part of any first responder entity but exploit only the network of the legacy mobile operator without any intermediary.

The demonstration of the MCPTT use case cannot be based on a static scenario, since one of its objectives to be proven is the elastic allocation of resources attending to different levels of emergency conditions detected by the monitoring system. In our approach a deployment topology of three main stages has been considered, as shown in Fig. 4.

At the beginning, in a situation under normal circumstances, the system instantiates the network slices that correspond to a default service agreement. Here, the first responder only needs a reduced amount of access capacity and communication features for its normal operations. Then, triggered by an emergency incident, the first responder requires increased capacity in terms of both data rate and edge computing resources, in order to serve a higher number of communications and/or public safety users. This situation may involve a deterioration of the service for legacy users, since their network slice(s) must be reduced in order to appropriately allocate the higher priority MCPTT service. Finally, the aim is to demonstrate how the service responds to an extreme situation of damaged infrastructure where a coverage extension is needed. In this situation, backhaul connectivity is lost, all the resources must be dedicated to the MCPTT network slice and the public safety organisation may dynamically add new access points to

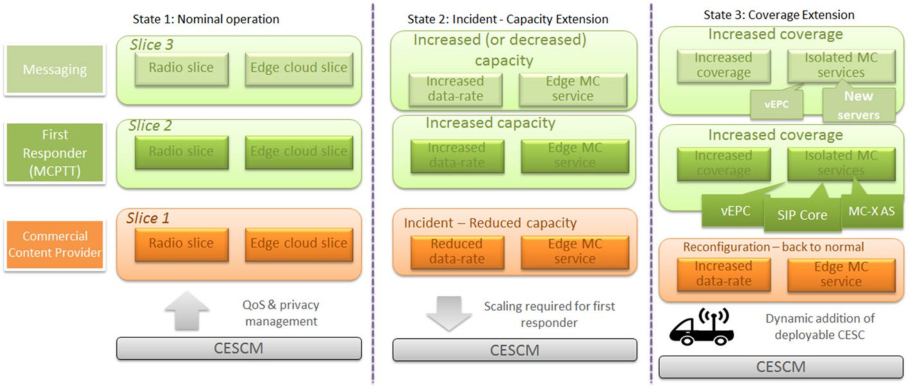

Fig. 4 Mission critical applications for public safety

the network in order to improve connectivity. This use case aims at demonstrating that the 5G ESSENCE context provides a solution for an efficient and elastic end-to-end network slicing and the efficient orchestration of the radio, network and cloud resources, in the defined three main stages discussed as follows:

Stage 1: Under normal circumstances, the 5G ESSENCE platform owner is providing three differentiated network slices. Two slices correspond to a Public Safety organisation running, respectively, a MCPTT and a messaging application, and the third slice corresponds to legacy end-users that have subscribed to the classical communications and Internet data offers. Each network slice is composed of an allocated data rate over a coverage area (which is mapped by the cSD-RAN Controller to a portion of CESC radio resources) and an allocated of cloud resources (which is mapped to processing power/storage capabilities in the Edge DC). For the service of PS organisations, normal operations require a certain amount of access capacity and communications features (e.g., group communications capabilities) supported in the area of the CESC cluster. This requirement can be mapped to a number of radio KPIs in the CESCs and the deployment of Group Communication service instances at the edge for multimedia and MC Application Servers (ASs) for voice with enhanced responsiveness. In addition to the QoS guarantees for each tenant, the deployment owner has to assure the required levels of isolation in the provisioning of the network slices.
Stage 2: In case where there is an emergency in the area, the CESCM will be able to react to the new service requirements. For instance, the MCPTT communications provider may require additional service in order to cope with an increased number of first responders and/or teams. Based on pre-arranged and/or on-demand service scaling policies, the CESCM implements new elastic resource allocation schemes, thus giving priority access to first responders and taking into account both radio (for the access connections) and cloud resources (for deploying more resource-consuming edge services). The deployment of edge service instances serves a two-fold objective, that is: first, it enables minimal delay in the MC services; second, it allows maintaining the operability even when the backhaul connection is damaged.
Stage 3: In case where the ICT infrastructure is damaged during a natural disaster or a terrorist attack, the first action should address the need for radio coverage supplementation. In this stage, we use a deployable system to mitigate the damage in the macro base stations. In the proposed use case, the deployable system can offer 5G connectivity to the first responders in the field, consolidating the interoperability requirements. In order to better orchestrate the radio transmissions, the deployable system is considered as a new CESC that can be dynamically integrated to the small cell cluster. In this way, the enhanced 5G ESSENCE SON and RRM features can be applied to the coverage extension unit. The interconnection of the deployable unit with the CESC cluster is made through a wireless backhauling technology.

4.3 Related KPIs, Technical Enablers and Functionalities

The Key Performance Indicators (KPIs) used in the 5G ESSENCE scope vary, depending on the service evaluated in order to better understand and illustrate the behaviour of each specific part. The reference KPIs for MCPTT are detailed below [33]:

- *MCPTT Access time* is defined as the time between when an MCPTT User request to speak (normally by pressing the MCPTT control on the MCPTT UE) and when this user gets a signal to start speaking. This time does not include confirmations from receiving users.
- *The End-to-end MCPTT Access time* is defined as the time between when an MCPTT User requests to speak (normally by pressing the MCPTT control on the MCPTT UE) and when this user gets a signal to start speaking, including MCPTT call establishment (if applicable) and possibly acknowledgement from first receiving user before voice can be transmitted.
- *The Mouth-to-ear latency* is the time between an utterance by the transmitting user, and the playback of the utterance at the receiving user's speaker.
- *The Late call entry time* is the time to enter an ongoing MCPTT Group call measured from the time that a user decides to monitor such an MCPTT Group Call, to the time when the MCPTT UE's speaker starts to play the audio.
- *System response time* is defined as the time required to distribute a chat message to all members of group.
- The *number of delivery failure* denotes the number of messages that were not delivered after the delivery deadline. Indeed, after the expiry of this deadline messages become obsolete and are simply discarded.

Figure 5 illustrates the particularisation of the general 5G ESSENCE architecture, including the relevant components to support the Public Safety use case. This use case supports two different PS services/applications, as discussed in the previous section, each one associated to a different network slice. This way, from infrastructural perspective, the control and data traffic isolation between both applications is fostered to an achievable level. The reduction of latency is one of the key pillars of 5G and the use of network slicing, along with VNFs, are critical in this approach.

The first network slice is the MCPTT service corresponding to slice 1 in the figure. The second one is the chat messaging and localisation service corresponding to slice 2. Other slices including, *for example*, commercial services are also naturally considered but are not depicted in Fig. 5, for simplicity purposes. Both PS services rely upon different

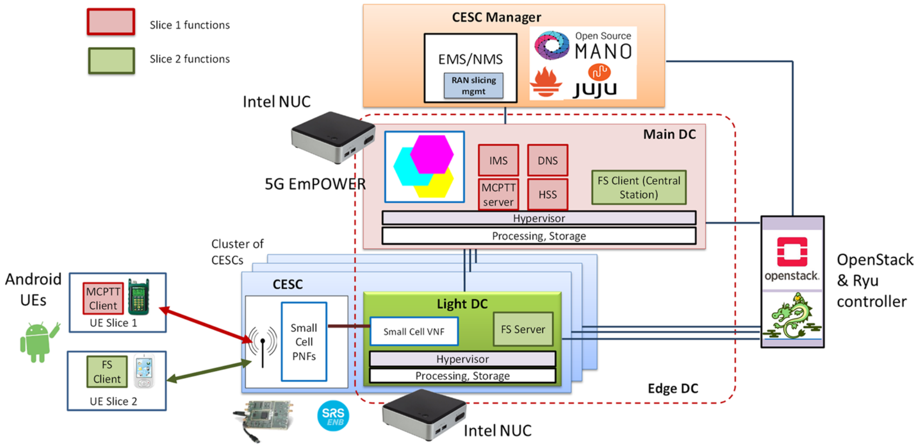

Fig. 5 Particularisation of the 5G ESSENCE for the PS use case

VNFs running at the Edge DC and on the radio transmission capabilities provided by the SC at the CESCs. The MCPTT service includes an MCPTT server at the network edge, an IMS, a DNS and an HSS. These functionalities can run as VNFs in the Main DC as they are common to all the CESCs in a service area. In turn, the MCPTT client will be hosted at each UE. Based on this, the creation of network slice 1 involves the instantiation of the abovementioned VNFs, done through the NFV MANO [57] entities (the OSM NFV Orchestrator, Juju VNF manager and OpenStack Virtualised Infrastructure Manager), and the instantiation of a RAN slice that provides a certain capacity for supporting the MCPTT transmissions at the radio interface, configured through the RAN slicing management function (e.g. through a number of descriptors that specify the operation of the RRM algorithms such as radio admission control or the packet scheduling behaviour). OSM is delivering an open source Management and Orchestration (MANO) stack aligned with ETSI NFV Information Models. As an operator-led community, OSM is offering a production-quality open source MANO stack that meets the requirements of commercial NFV networks. Juju has adopted a domain neutral model and does not encode policy. It can therefore be described as a generic VNF Manager (VNFM) and not a VNF Orchestrator. Juju is useful across many domains and is being adopted in big data, cloud infrastructure, Platform as-a-Service (PaaS) and other scale-out scenarios. OpenStack is the only virtual infrastructure manager in OPNFV. The role of the virtual infrastructure manager is to configure the compute, hypervisor and infrastructure network domains. When there is no SDN controller, it can also configure the underlying physical networks. However, in the OPNFV scenarios, OpenStack only deals with configuring virtual switches, i.e. infrastructure networking.

As for the network slice 2 associated to the messaging service, it involves three types of functions, namely the FS Client of the central station, the FS client at the UEs and the FS server. There, a FS server is assumed to be associated to each CESC deployed during the emergency to provide the communication with the UEs connected to that CESC and with the central station. In that respect, it can be assumed to run as a VNF at the Light DC. In turn, the FS client of the central station can run at the Main DC or even at the PS operator premises outside the CESC infrastructure. The chat and localisation service shows the importance of slicing when the availability of the service is needed. The 5G-EmPOWER can manage and ensure the minimum needed resource blocks when one specific slice is prioritised.

In the 5G ESSENCE two-tier architecture this kind of structure is perfectly matched with the use of CESCs on the edge of the network, having enough processing power and network capacity to run services distributed between multiple locations (small cells deployed on fire engines or police trucks in this case) in a way that it is possible to deploy and use both Messaging and localisation and Mission-Critical Push-to-talk (MCPTT) applications much closer to the end-user and, *as a result*, to achieve lower latencies [64]. This is possible since the petitions and responses sent using the specified tenant slice to the server are not necessarily managed by the Main DC that is further from the end user and, at the same time, reducing Main DC traffic or eliminating it completely, as an added value. The minimum capabilities of the use case should enable:

- Deploying slice-oriented management and operation features of the 5G ESSENCE with selected open-source LTE SDR [e.g.: Open-Air Interface (OAI), Software Radio Systems (SRS)] and Orchestrators;

- configuring per slice QoS guarantees (e.g. through defining amount of PRBs per slice) but also inter-slice priorities in accordance with the objectives of the original use case focusing on MC for PS deployment;
- demonstration of selected radio resource management techniques for radio resource allocation which is configurable per slice (e.g. radio scheduler, admission control);
- provisioning an E2E slice and service which spans across EPC, RAN and eventually also the end-terminals (UE);
- defining an interaction between the slice operation and the D2D "infrastructure-less" modes, and;
- extending *on-the-fly* a slice with new resources (e.g. LightDC with small cell) as well extending a slice with new heterogeneous resources (e.g. LightDC with small cell + LightDC with WiFi).

However, the real set of functionalities supporting slicing, largely depend on the selected SD-RAN controller platform. The actual use case is implemented by using 5G-EmPOWER and open-source SDRs (i.e.: OAI, srsLTE) available for the integration of research results. The use case utilises the 5G-EmPOWER Controller [65, 66] which is responsible for the management of the heterogeneous RANs. The 5G-EmPOWER Controller supports multiple virtual networks -or tenants- on top of the same physical infrastructure (here a tenant is conceived as a virtual network with its own set of end-points). Network applications (Network Apps) run on top of the Runtime in their own slice of resources and exploit its programming primitives through either a REST API or a native Python API. The 5G-EmPOWER Controller ensures that a Network App is only presented a view of the network corresponding to its slice.

The evaluation of the 5G ESSENCE slicing solution aims at proving the following verifiable features:

- Technical means to extend current service slice with new resources "on-the-fly" (e.g., as new fire engines are arriving in the theatre)—this would also target resource adaptation of the current slice (e.g., adding new points of presence, support of load balancing between Light DCs deployed on the trucks);
- configurable level of resource isolation between slices and services (i.e. traffic pattern variations in one slice should have no or minimal effect on the parallel slice operations);
- capability of maintaining local communications after infrastructure failure than ensure content coherence after reconnection (e.g. thanks to the alternative D2D communications during failure);
- the possibility of showcasing performance improvement (at workload or at radio resources level) by utilizing results from the "Analytics" module backed by the monitoring system data of the 5G ESSENCE and enhancing orchestration, resource allocation or both processes [67];
- capabilities of configuring two different slices separately (e.g. slice supporting eMBB can include WiFi AP, while it does not make sense to include WiFi AP into a ULLRC slice);
- end-user application specific composition of slice (e.g. orchestrator decides VNFs and its configuration based on the target application to be supported by a slice)—an enhanced feature could be for orchestrator to also decide on the placement of a VNF between the Main and Light DCs;
- infrastructure wide orchestration functions and slice-based orchestration functions;

- configurable assignment of PRBs between slices but also within a slice;
- application driven, request-based slice reconfiguration, *and*;
- SD-RAN controller and Orchestrator running in CESC.

The MCPTT-*enabled* architecture (and correspondingly also the FS solution) involves the following elements: MCPTT clients (devices of first responders and personnel at the central station) and server (providing connection to clients and control-plane operations), media distribution unit (for media transmission on the data-plane), media mixer and the MCPTT user database (for profiling, authentication and authorization (AA) and security).

In detail, there are more options for the virtualisation of the MCPTT service architecture. The basic option is with all the functional blocks of the service packed in a single VNF. This configuration simplifies the connection between blocks, but provides little flexibility for scaling possibilities. While, the ultimate step of separation corresponds to the separation of also the data and control planes of the MCPTT service, bringing the data plane and needed control plane elements to the edge to reduce the transmission latencies.

As for the Network Slice 2 associated to the messaging service, it involves three types of functions, namely the FeedSync (FS) Client of the central station, the FS client at the UEs and the FS server. A FS server is assumed to be associated to each CESC deployed during the emergency situation to provide the communication with the UEs connected to that CESC and with the central station. Hence, it can be assumed to run as a VNF at the Light DC. In turn, the FS client of the central station can run at the Main DC or even at the PS operator premises outside the CESC infrastructure.

In conclusion, each of the services is associated to a different RAN slice. The MCPTT (corresponds to the slice 1) shows the interest of employing monitoring mechanisms and, *on the other hand*, mission-critical messaging and localisation application (corresponds to the slice 2) highlights the importance of implementation of slicing and availability of the service in case of emergency. Each of these applications validates some technical components of the 5G ESSENCE project to establish an E2E service for the next generation (NG) of edge computing communication scenarios.

The final demonstration of the above PS use case took place at the B-APCO annual event in Newcastle, UK, in early November 2019. The Mission Critical Push-To-Talk (MCPTT) application and Chat-and-Localization application have been addressed and instantiated through the realization of a real testbed. The demonstration storyline followed the activities of first responders in a crowded city to ensure the safety of everyone. Based on the selection of the previous mission critical services, the demonstration was able to show three different situations -or scenarios-, that is: the normal circumstances when there is no emergency; an emergency in the specific area, and; an emergency in that area with a damage in the ICT infrastructure.

The demonstration evaluated the above scenarios that have all been considered for the validation of the MC services of the 5G ESSENCE architecture. Three situations have been identified, briefly discussed as follows: In the first situation, the 5G ESSENCE platform provided the required network slices (in terms of radio frequencies, data rate, cloud resources and QoS) in the area of the CESC cluster. This situation has been considered as a baseline to deploy the second situation, where an emergency in the area occurs. In this case, the CESCM was able to react to the new service requirements and satisfying the needed requirements of first responders in terms of capacity and computation resources, because the PS communications provider may require additional service in order to cope with an increased number of first responders or additional types of services such as mission-critical video transmissions. In the third case, when the ICT infrastructure may be damaged during a natural disaster or a terrorist attack, the first action should address the need for radio coverage extension. In this stage, a deployable system to mitigate the damage in the infrastructure can used, offering 5G connectivity to the first responders in the field.

Obtained results from the demos have been about the Network Service (NS) deployment, the slicing capabilities and the Service Network adaptation based on the monitored information. These can briefly be summarised as follows: (1) For the NS deployments, the tests demonstrated the feasibility of deployed the VNFs and NSD (Network Service Descriptor) in both environments (Main DC and Edge DC of the infrastructure) providing mission critical services to the users; (2) for the slicing capabilities, the tests showed the adaptation of the created slice for the virtual service and adapted based on the security stage identified in the application; (iii) for the monitored information, tests came from registering metrics from the network services to the alerting of an unexpected behaviour in order to scale it or to do another mitigation action. Every component has been integrated and tested in different cases with successful results.

5 Conclusion

The increase of heterogeneity in technology, services offered and the coverage area of radio access in the context of the forthcoming 5G wireless communications, implicates for new challenges and opportunities in optimising users' access to the underlying infrastructures [68]. At present, most critical communications user organizations employ LTE and 5G NR as complementary technologies to augment existing voice-centric LMR networks with broadband capabilities. However, with the standardization and commercial availability of MCX (i.e.: Mission-Critical PTT, Video and Data) [9, 26, 27], IOPS (Isolated Operation for Public Safety) [69], HPUE (High-Power User Equipment) [70] and other 3GPP-defined critical communications features, LTE and 5G NR networks are increasingly gaining recognition as an all-inclusive critical communications platform for the delivery of mobile broadband and industrial IoT capabilities, as well as MCPTT (Mission-Critical PTT) voice functionality comparable to that offered by traditional LMR systems.

The present paper has focused on mission-critical communications that, by nature, have strict QoS requirements and are not easily able to be fulfilled by traditional infrastructure sharing models. Upon the specific context of the 5G ESSENCE project that promotes a cloud-enabled small cell infrastructure with a fully distributed orchestration architecture leveraging multi-access technologies in 5G, we have proposed a public safety use case, with the pure aim of demonstrating the sharing of the common 5G infrastructure in an emergency scenario between first responders and civilians. Based on the context of the original 5G ESSENCE architectural approach, we have defined two distinct services (i.e.: the MCPPT service and the MC chat and localisation application) that can both be provided by using separate and dedicated, for this purpose, network slices. This offers flexibility for dedicated mission critical public safety applications also at the edge of the network.

One of the essential features emphasized in this use case is the ability of a more generalized 5G-based architecture (such as the one proposed by the 5G ESSENCE solution), to deal with dynamic reconfiguration challenges, depending on the requirements of the delivered services. The network slicing perception as one among the core features of the 5G, has been assessed together with highly virtualised and software-based platforms so that to allow for the adaption, on-the-fly, of the selected slices to the modifying environment together with the possibility to consider creation of new slices to serve new traffic requests, when necessary. This feature is essential in mission critical environments where disconnections as well as dynamic allocation of new resources and their configuration are frequently required.

For the case of both offered services, the results highlight the value of the shared network model, demonstrating the capacity of the 5G ESSENCE architecture to autonomously allocate network resources to first responders whenever they are required, but giving them up to the commercial services when the requirements are low. The elastic allocation of resources is performed automatically, but can also take place manually, when required. The PS use case has reassured the contribution of the original 5G ESSENCE scope to some fundamental 5G architectural concepts, such as the realisation of the network slicing at the network edge, enabling multiple tenants and vertical industries sharing the same CESC infrastructure. Future work can cover a broader realization of the proposed solution at management and orchestration levels, as well as at the level of single functional components (e.g. control and monitoring).

Funding This work has been realised in the scope of the *5G-ESSENCE* European Research Project and has been supported by the Commission of the European Communities under the H2020/5G-PPP Grant Agreement No.761592.

Declarations

Conflict of interest The authors declare no conflict of interest.

References

1. Kumbhar, A., Koohifar, F., Guveniç, I., & Mueller, B. (2017). A survey on legacy and emerging technologies for public safety communications. *IEEE Communications Surveys and Tutorials, 19*(1), 97–124
2. Baldini, G. (2014). Survey of wireless communication technologies for public safety. *IEEE Communications Surveys and Tutorials, 16*(2), 619–641
3. Gomez Chavez, K. M., Goratti, L., Rasheed, T., et al. (2015). The evolutionary role of communication technologies in public safety networks. *Elsevier Wireless Public Safety Networks, 1*, 21–48
4. Favraud, R., Apostolaras, A., Nikaein, N., & Korakis, T. (2016). Toward moving public safety networks. *IEEE Communications Magazine, 54*(3), 14–20
5. Ferrús, R., Sallent, O., Baldini, G., & Goratti, L. (2013). LTE: The technology driver for future public safety communications. *IEEE Commununications Magazine, 51*(10), 154–161
6. Xinjun, M. (2015). *An evolution in public safety networks*. Huawei Technologies Co., https://e.huawei.com/us/publications/global/ict_insights/201608271037/focus/201608271435
7. Fantacci, R., Gei, F., Marabissi, D., & Micciullo, L. (2016). Public safety networks evolution toward broadband: Sharing infrastructures and spectrum with commercial systems. *IEEE Communications Magazine, 54*(4), 24–30

8. The 3rd Generation Partnership Project (3GPP). https://www.3gpp.org/specifications/67-releases
9. The 3rd Generation Partnership Project (3GPP): 3GPP TS 22.280 V17.2.0 (2019–12): "Mission critical services common requirements (MCCoRe); Stage 1; Release 17" (2019).
10. Höyhtyä, M., Lähetkangas, K., Suomalainen, J., et al. (2018). Critical communications over mobile operators' networks: 5G use cases enabled by licensed spectrum sharing, network slicing and QoS control. *IEEE Access, 6*, 73572–73582
11. Jimeno, E., Pérez-Romero, J., Muñoz, I. V., Blanco, B., Sanchoyerto A., & Hidalgo, J. F. (2018). 5G framework for automated network adaption in mission critical services. In *Proceedings of the 2018 IEEE conference on network function virtualization and software defined networks (NFV-SDN)* (pp. 1–5). IEEE.
12. Andrews, J. G., Buzzi, S., Choi, W., Hanly, S. V., Lozano, A., Soong, A. C. K., & Zhang, J. C. (2014). What will 5G Be? IEEE JSAC. *Special Issue on 5G Wireless Communications Systems*, *32*(6), 1065–1082.
13. Kostopoulos, A., Chochliouros, I. P., Kuo, F.-C., Riggio, R., Goratti, L., Nikaein, N., Giannoulakis, I., Pérez-Romero, J., Chen, T., Steinert, R., & Panaitopol, D. (2017). Design aspects for 5G architectures. The SESAME and COHERENT approach. In *Proceedings of the 4th IEEE international conference on communications workshops (ICC workshops)—4th international workshop on 5G architecture* (pp. 986–992). IEEE.
14. Blanco, B., Fajardo, O. J., Giannoulakis, I., Kafetzakis, E., Peng, S., Pérez-Romero, J., Trajkovska, I., Khodashenas, P. S., Goratti, L., Paolino, M., & Sfakianakis, E. (2017). Technology pillars in the architecture of future 5G mobile networks: NFV, MEC and SDN. *Computer Standards and Interfaces, 54*, 216–228
15. Nam, H., Calin, D., & Schulzrinne, H. (2015). Intelligent content delivery over wireless via SDN. In *Proceedings of the IEEE wireless communications and networking conference (WCNC)* (pp. 2185–2190). IEEE.
16. Solozabal, R., Sanchoyerto, A., Atxutegi, E., Blanco, B., Fajardo, J. O., & Liberal, F. (2018). Exploitation of mobile edge computing in 5G distributed mission-critical push-to-talk service deployment. *IEEE Access, 6*, 37665–37675
17. Jiang, M., Xenakis, D., Constanzo, S., Passas, N., & Mahmoodi, T. (2017). Radio resource sharing as a service in 5G: A software-defined networking approach. *Computer Communications*, *107*(15), 13–29.
18. Sexton, C., Kaminski, N. J., Marquez-Barja, J. M., Marchetti, N., & DaSilva, L. A. (2017). 5G: Adaptable networks enabled by versatile radio access technologies. *IEEE Communications Surveys and Tutorials, 19*(2), 688–720
19. The 3rd Generation Partnership Project (3GPP): 3GPP TR 21.915 V15.0.0 (2019–09): "Release 15 Description; Summary of Rel-15 Work-Items (Release 15)".
20. Ergul, P., Shah, G. A., Canberk, B., & Akan, O. B. (2016). Adaptive and cognitive communication architecture for next-generation PPDR systems. *IEEE Communications Magazine, 54*(4), 92–100
21. Kapucu, N., Haupt, B., Yuksel, M., Guvenc, I., & Saad, W. (2016). On the evolution of wireless communication technologies and spectrum sharing for public safety: Policies and practice: Evolution of policies and practice. *Wiley Online Library, Risk, Hazards and Crisis in Public Policy, 7*(3), 129–145
22. Liebhart, R. (2015). *LTE for public safety*. Wiley.
23. Ali, K., Nguyen, H. X., Shah, P., Vien, Q.-T., & Bhuvanasundaram, N. (2016). Architecture for public safety network using D2D communication. In *Proceedings of the IEEE wireless communications and networking conference (WCNC-2016)* (pp. 1–6). IEEE
24. Lynch, T. (2016). *LTE in public safety*. IHS Technology, May 2106. https://omdia.tech.informa.com/580532/whitepaper-lte-in-public-safety
25. The 3rd Generation Partnership Project (3GPP): 3GPP TS 36.877 V12.0.0 (2015–03): "LTE Device to Device (D2D) Proximity Services (ProSe); User Equipment (UE) radio transmission and reception; Release 12".
26. The 3rd Generation Partnership Project (3GPP): 3GPP TS 22.281 V16.0.0 (2018–09): "Mission critical video services (Release 16)".
27. The 3rd Generation Partnership Project (3GPP): 3GPP TS 22.282 V16.4.0 (2018–12): "Mission critical data services (Release 16)".
28. García-Pérez, C. A., Díaz-Zayas, A., Ríos, A., Merino, P., Katsalis, K., & Morris, D. (2017). Supporting new application and services over LTE public safety networks. *Elsevier Wireless Public Safety Networks, 3*, 113–132

29. Carlà, L., Fantacci, R., Gei, F., Marabissi, D., & Micciullo, L. (2016). LTE enhancements for public safety and security communications to support group multimedia communications. *IEEE Network, 30*(1), 80–85
30. Zhang, K. (2014). Exploiting multimedia services in mobile social networks from security and privacy perspectives. *IEEE Communications Magazine, 52*(3), 58–65
31. The 3rd Generation Partnership Project (3GPP), Public safety on 3GPP*:* https://www.3gpp.org/news-events/3gpp-news/1455-Public-Safety
32. The 3rd Generation Partnership Project (3GPP). https://www.3gpp.org/news-events/1875-mc_services
33. The 3rd Generation Partnership Project (3GPP): 3GPPP TS 22.179 V15.0.0 (2017–06): "Technical specification group services and system aspects: Mission critical push to talk (MCPTT) over LTE; Stage 1 (Release 15)".
34. The 3rd Generation Partnership Project (3GPP): 3GPPP TR 21.915 V15.0.0 (2019–09): "Technical specification group services and system aspects: Release 15 description; Summary of Rel-15 Work Items (Release 15)".
35. Next Generation Mobile Networks (NGMN) Alliance. (2015). *5G white paper*. https://www.ngmn.org/uploads/media/NGMN_5G_White_Paper_V1_0.pdf
36. 5G ESSENCE (Embedded Network Services for 5G Experiences) project (GA No.761592) Website: http://www.5g-essence-h2020.eu/Home.aspx
37. 5G Public Private Partnership (5G-PPP) (2019): 5G-PPP Architecture Working Group View on 5G Architecture. https://5g-ppp.eu/wp-content/uploads/2019/07/5G-PPP-5G-Architecture-White-Paper_v3.0_PublicConsultation.pdf
38. Fajardo, J. O., Liberal, F., Giannoulakis, I., Kafetzakis, E., Pii, V., Trajkovska, I., Bohnert, T. M., Goratti, L., Riggio, R., Garcia-Lloreda, J., Paolino, M., Bliznakov, P., Pérez-Romero, J., Meani, C., Chochliouros, I. P., & Belesioti, M. (2015). Introducing mobile edge computing capabilities through distributed 5G cloud enabled small cells. *ACM/Springer Mobile Networks and Applications (MONET), Special Issue on Mobile Networks and Management, 21*(4), 564–574.
39. Kourtis, M.-A., Blanco, B., Pérez-Romero, J., Makris, D., McGrath, M. J., Xilouris, G., Munaretto, D., Solozabal, R., Sanchoyerto, A., Giannoulakis, I., Kafetzakis, E., Riccobene, V., Jimeno, E., Kourtis, A., Ferrús, R., Liberal, F., Koumaras, H., Kostopoulos, A., & Chochliouros, I. P. (2019). A cloud-enabled small cell architecture in 5G networks for broadcast/multicast services. *IEEE Transactions on Broadcasting, 65*(2), 414–424
40. European Telecommunications Standards Institute (ETSI). (2017). *Multi-access edge computing*. http://www.etsi.org/technologiesclusters/technologies/multi-access-edge-computing. Accessed: 2017–0710.
41. Zhou, X., Li, R., Chen, T., & Zhang, H. (2016). Network slicing as a service: Enabling enterprises' own software-defined cellular networks. *IEEE Communications Magazine, 54*(7), 146–153
42. Chochliouros, I. P., Spiliopoulou, A. S., Lazaridis, P., Dardamanis A., Zaharis, Z., & Kostopoulos, A. (2020). Dynamic network slicing: Challenges and opportunities. In *Proceedings of AIAI-2020 international conference, IFIP AICT 585* (pp. 704–715). Springer.
43. The 3rd Generation Partnership Project (3GPP): 3GPP TR 32.851 (2015–01). "Telecommunication management: Study on Operations, Administration and Maintenance (OAM) aspects of Network Sharing (Release 12)".
44. European Telecommunications Standards Institute. (2016). Network functions virtualization—Introductory white paper. http://portal.etsi.org/NFV/NFV_White_Paper.pdf
45. Chochliouros, I. P., Spiliopoulou, A. S., Kourtis, A., Giannoulakis, I., et al. (2018). Enhancing network management via NFV, MEC, cloud computing and cognitive features: The "5G ESSENCE" modern architectural approach. In *Proceedings of AIAI-2018, IFIP AICT 520* (pp. 1–12). Springer.
46. Chochliouros, I. P., Spiliopoulou, A. S., Agapiou, G. et al. (2019). Inclusion of telemetry and data analytics in the context of the 5G ESSENCE architectural approach. In *Proceedings of AIAI-2019, IFIP AICT 560* (pp. 46–59). Springer.
47. Chochliouros, I. P., Sallent, O., Pérez-Romero, J., Spiliopoulou, A. S., & Dardamanis, A. (2017). Implications for multi-tenancy upon RRM/Self-x functions supporting mobility control. In *Proceedings of EANN-2017, CCIS 744* (pp. 657–668). Springer.
48. Chochliouros, I. P., Spiliopoulou, A. S., Kostopoulos, A. et al. (2017). Putting intelligence in the network edge through NFV and cloud computing: The SESAME approach. In *Proceedings of EANN-2017, CCIS 744* (pp. 704–715). Springer.
49. Chochliouros, I. P., Kostopoulos, A., Spiliopoulou, A. S., Kourtis, A., Giannoulakis, I., Kourtis, M. A., et al. (2018). Small cells, NFV and cloud computing as enablers for offering innovative 5G services: From the SESAME to the 5G ESSENCE architectural framework. In *Proceedings of EuCNC 2018* (pp. 570–574). IEEE.

50. Rost, P., Mannweiler, C., Michalopoulos, D. S., Sartori, C., et al. (2017). Network slicing to enable scalability and flexibility in 5G mobile networks. *IEEE Communications Magazine, 55*(5), 72–79
51. The 3rd Generation Partnership Project (3GPP), 3GPP PS scope: https://www.3gpp.org/news-events/3gpp-news/1455-Public-Safety
52. The 3rd Generation Partnership Project (3GPP) (2016). 3GPP TR 22.862 v14.1.0: "Feasibility study on new services and markets technology enablers—Critical communications; Stage 1 (Release 14)".
53. Ferrús, R., & Sallent, O. (2015). Mobile broadband communications for public safety: The road ahead through LTE technology. Wiley.
54. Blue Light Mobile (Online). http://bluelightmobile.be/en
55. Gallagher, J. C. (2018). The first responder network (firstnet) and next-generation communications for public safety: Issues for congress. Congressional Research Service.
56. Kostopoulos, A., Chochliouros, I. P., Sfakianakis, E., Munaretto, D., Keuker, C., Kourtis, M. A., & Giannoulakis, I. (2019). Network functions for supporting 5G services. In *Proceedings of the EuCNC 2019* (pp. 1–4). IEEE.
57. European Telecommunications Standards Institute (ETSI). (2014). NFV management and orchestration—An overview, GS NFV-MAN 001 v1.1.1. ETSI.
58. Openstack: https://www.openstack.org/
59. Opendaylight: https://www.opendaylight.org/
60. Cau, E., Corici, M., Bellavista, P., Foschini, L., Carella, G., Edmonds, A., &and Bohnert, T. M. (2016). Efficient exploitation of mobile edge computing for virtualized 5G in EPC architectures. In *Proceedings of the MobileCloud 2016* (pp. 100–109). IEEE.
61. The 3rd Generation Partnership Project (3GPP). (2018). TR 28.801 V15.1.0 (2018–01). Study on management and orchestration of network slicing for next generation network (Release 15).
62. Sanchoyerto, A., Solozabal, R., Blanco, B., & Liberal, F. (2019). Analysis of the impact of the evolution towards 5G architectures on mission critical push-to-talk services. *IEEE Access, 7*, 115052–115061
63. The 3rd Generation Partnership Project (3GPP). (2017). TS 23.501 V1.3.0 (2017–09): System architecture for the 5G system: Stage 2 (Release 15).
64. Spada, M.-R., Perez-Romero, J., Sanchoyerto, A., Solozabal, R., Kourtis, M.-.A., & Riccobene, V. (2019). Management of mission critical public safety applications: The 5G ESSENCE project. In *Proceedings of the EuCNC-2019* (pp. 155–160). IEEE.
65. 5G-EmPOWER controller. https://5g-empower.io/
66. Coronado, E., Kahn, S. N., & Riggio, R. (2019). 5G-EmPOWER: A software-defined networking platform for 5G radio access networks. *IEEE Transactions on Service and Network Management, 16*(2), 715–728
67. Richart, M., Baliosian, J., Serrat, J., & Gorricho, J. L. (2016). Resource slicing in virtual wireless networks: A survey. *IEEE Transactions on Network and Service Management, 13*(3), 462–476
68. SNS Telecom & IT (2020). The public safety LTE & 5G Market: 2020–2030—Opportunities, challenges, strategies & forecasts. Research and Markets.
69. The 3rd Generation Partnership Project (3GPP): 3GPPP TS 22.346 V16.0.0 (2020–07). "Isolated evolved universal terrestrial radio access network (E-UTRAN) operation for public safety: Stage 1 (Release 16).
70. The 3rd Generation Partnership Project (3GPP): 3GPPP TR 36.886 V14.1.0 (2019–03). Evolved universal terrestrial radio access (E-UTRA): Band 41 high power UE (HPUE) (release 14).

Dr. Ioannis P. Chochliouros graduated from the Dept. of Electrical Engineering of the Polytechnic School of Aristotle University of Thessaloniki, Greece, holding also a M.Sc. (D.E.A.) and a Ph.D. (Doctorat) from the University Pierre et Marie Curie (Paris VI), France. His practical experience as an engineer has been mainly in Telecommunications, as well as in various constructive projects in Greece and the wider Balkan area. Since 1997 he has worked at the Competition Department and as an engineer-consultant of the Chief Technical Officer of the Hellenic Telecommunications Organisation S.A. (OTE). He has been very strongly involved in major OTE's national and international business activities, as a specialist-consultant for technical and regulatory affairs, especially for the evaluation and the adoption of innovative e-Infrastructures and e-Services in Greece and abroad. He has also served as the Head of Technical Regulations Dept. of OTE's Division for Standardisation and Technical Regulations, representing OTE in international standardisation for a and he has been involved in an enormous variety of issues regarding European and international standardisation, with emphasis on modern technologies. In addition, he has also worked as an independent consultant in the scope of several European and/or international research and business studies. Since 2005, he is the Head of OTE's Fixed Network R&D Programs Section and has been involved in different national, European and international R&D projects and market-oriented activities, many of which have received international awards. During his professional career, he has participated either as coordinator or as a scientist-researcher in more than 62 European and national research programs, some of which have received distinctive awards. He is author/co-author of three international books and he has published more than 250 distinct scientific or business papers/reports in the international literature (book chapters and articles in magazines, journals and conferences proceedings), especially for technical, business and regulatory options arising from innovative e-Infrastructures and e-Services. He is an expert in project management activities with an extensive experience in EU-funded projects where he has very successfully exercised coordinator's duties (e.g., 5G-PPP 5G ESSENCE, 5G-PPP SESAME, Privacy-Flag, LiveCity, D-SPACE). He is also an active participant of various international and national associations, both of scientific and business nature. Dr. Chochliouros has also performed an extended educational activity in Greece and in France, in cooperation with Universities and other high-level Institutes, covering a broad variety of issues in the scope of modern e-communications. Recently he has received the distinctive award of being a member of the IPv6 Hall of Fame.

Mrs. Anastasia S. Spiliopoulou is a Lawyer, Member of the Athens Bar Association. She also holds a Post-Graduate Diploma from the Law School of National and Kapodistrian University of Athens, Greece. She has a long professional experience in telecommunications and IT-related issues and she has been involved in many affairs about regulatory issues and other matters affecting the deployment and the provision of both modern electronic communications networks and services. She is an OTE's (Hellenic Telecommunications Organization S.A.) expert for a great variety of regulatory issues affecting both European and national policies. She is author/coauthor of more than 100 papers in the international literature and has participated to numerous conferences, in several of which as invited speaker.

Prof. Pavlos I. Lazaridis is a Professor in Electronic and Electrical Engineering at the University of Huddersfield, UK. He received the Electrical Engineering degree from the Aristotle University of Thessaloniki, Greece, in 1990, the M.Sc. degree in Electronics from Université Pierre et Marie Curie, Paris 6, France, in 1992, and the Ph.D. degree in Electronics and telecommunications from Ecole Nationale Supérieure des Télécommunications (ENST) and Paris 6, Paris, in 1996. From 1991 to 1996, he was involved with research on semiconductor lasers, wave propagation, and nonlinear phenomena in optical fibers for the Centre National d'Etudes des Télécommunications (CNET) and teaching at the ENST. In 1997, he became the Head of the Antennas and Propagation Laboratory, TDF-C2R Metz (Télédiffusion de France/France Télécom Research Center), where he was involved with research on antennas and radio coverage for cellular mobile systems (GSM), Digital Audio Broadcasting (DAB), and Digital Video Broadcasting-Terrestrial (DVB-T). From 1998 to 2002, he was with the European Patent Office, Rijswijk, The Netherlands, as a Senior Examiner in the field of Electronics and Telecommunications. From 2002 to 2014, he was involved with teaching and research at the Alexander Technological Educational Institute of Thessaloniki, Greece, and Brunel University, West London. He is leading the EU Horizon 2020 projects ITNMOTOR5G and RISE-RECOMBINE for the University of Huddersfield. He is a member of the IET and a senior member of IEEE.

Dr. Zaharias D. Zaharis received the B.Sc. degree in physics, the M.Sc. degree in electronics, the Ph.D. degree, and the Diploma degree in electrical and computer engineering from the Aristotle University of Thessaloniki, Thessaloniki, Greece, in 1987, 1994, 2000, and 2011, respectively. From 2002 to 2013, he was with the administration of the telecommunications network, Aristotle University of Thessaloniki, and since 2013 he has been with the Department of Electrical and Computer Engineering of the same university. His current research interests include design and optimization of antennas and microwave circuits, signal processing on smart antennas, development of evolutionary optimization algorithms, and neural networks. Dr. Zaharis is a member of the Technical Chamber of Greece and a senior member of IEEE.

Dr. Maria-Rita Spada graduated in Physics in 1983 and Strategic Communication Sciences in 2011. She is involved in the Technology Architecture and Remedies Management Department in Wind Tre; she has more than 30 years of experience in the fields of Information Technology and Telecommunications. She worked in Olivetti R&D in Image Processing, AI and 4th generation tools for banking applications. She joined Infostrada/Wind in 1996, working on network planning and customer services tools. She has been involved in several European projects and in different research programs (BASS, MOICANE, PHOENIX, OPERA, ANIKETOS, CHOREOS, ESS, All4Green, DOLFIN, ASAP, MUSES, ACTIVAGE, 5GCity, 5G ESSENCE, NRG5, ICT4CART) and in the activities of 5G-PPP.

Prof. Jordi Pérez-Romero is a Professor at the Dept. of Signal Theory and Communications of the Universitat Politècnica de Catalunya (UPC) in Barcelona, Spain. He received the Telecommunications Engineering degree and the Ph.D. from the same university in 1997 and 2001, respectively. His research interests are in the field of mobile communication systems with a main focus of 5G, covering radio resource and QoS management, self-organizing networks, network slicing, multi-tenancy and application of data analytics and artificial intelligence tools in the management of 5G networks. He has been involved in different European Projects as well as in projects for private companies. He has published more than 250 papers in international journals and conferences and has co-authored two books on mobile communications. He accumulates more than 4400 citations in Google Scholar and has an h-index of 31. He is associate editor of IEEE Vehicular Technology Magazine and Eurasip Journal on Wireless Communications Networks.

Dr. Bego Blanco received her B.S. and M.Sc. in Telecommunications Engineering from the University of the Basque Country, Spain, in 2000, and her Ph.D. in Telecommunications Engineering in 2014 from the same university. She currently works as a lecturer and researcher in the Faculty of Engineering in Bilbao. Her research interests include PQoS/QoE/QoS assessment as well as multicriteria optimization in 5G networks.

Dr. Hicham Khalife received his M.Sc. degree from the University Pierre et Marie Curie in 2005, then his Ph.D. from the same university in 2008. From 2009 to 2011 he served as an associate professor in the computer engineering department of IPB ENSEIRB-MATMECA in Bordeaux France and as a member of the LaBRI research laboratory enrolled in the COMET Networking team. He joined Thales Communications and Security in December 2011. His main research contributions are mainly in the area of wireless networks and multi-hop collaborative radio networks. He has been involved in several collaborative projects at National (ANR LiCoRNe project coordinator) and European levels (FP7 DUPLO, MOTO and RESCUE as project coordinator). He has served as committee member of many international conferences and published and reviewed for international journals and conferences.

Dr. Ehsan Ebrahimi Khaleghi received his Ph.D. degree in 2016 from communications and electronics (ComElec) department of Telecom-ParisTech (ENST). From May 2016 to June 2017 he has been working as a Post-Doctoral researcher at Inria-Paris and Nokia Bell-Labs on D2D evolution towards 5G; specially working on the impacts of the Near-Far Effect on Coded Slotted ALOHA. From July 2017 to October 2017 he has been a research engineer in Orange-Gardens, Châtillon working on MIMO systems, beamforming and simulation of fast fading channels for 5G. Since November 2017 he has been working as a research engineer at Thales SIX GTS, in Gennevilliers, France. His current research interests are in Software-defined networking, deep learning, neural networks, network coding, next-generation mobile networks, random access protocols, resource allocation, interference alignment, relaying protocols, 5G and precoding techniques. He has been involved in several collaborative European projects such as 5G ESSENCE. Furthermore, He holds a M.Sc. in digital communication systems (2012) and a B.Sc. in Electronics (2010) both from the University of Paris 6—UPMC (France-Paris).

Dr. Michail-Alexandros Kourtis received his Ph.D. from UPV/EHU in 2018 and his Diploma and Master's Degree in Computer Science from the Athens University of Economics and Business, in 2011 and 2013 respectively. Since 2015, he has worked on applications of Network Function Virtualisation for cybersecurity, as well as on the definition of privacy and security risk metrics on virtualized infrastructures. His research interests include QoE, QoS, Video Processing, Video Quality Assessment, Image Processing, LTE, 5G, Network Function Virtualization, and Software Defined Networks. He is a contributor at the OPNFV open source project Yardstick, and an active member, participant and contributor at the IETF NFVRG, also a TPC member and reviewer at various conferences and journals.

Authors and Affiliations

Ioannis P. Chochliouros[1] · Anastasia S. Spiliopoulou[1] · Pavlos I. Lazaridis[2] · Zaharias D. Zaharis[2] · Maria-Rita Spada[3] · Jordi Pérez-Romero[4] · Bego Blanco[5] · Hicham Khalife[6] · Ehsan Ebrahimi Khaleghi[6] · Michail-Alexandros Kourtis[7]

[1] Hellenic Telecommunications Organization S.A. Member of the Deutsche Telekom Group of Companies, 99 Kifissias Avenue, 15124 Maroussi, Athens, Greece

[2] University of Huddersfield, Queensgate, Huddersfield HD1 3DH, UK

[3] Wind Tre, S.p.A., Rho, Milan, Italy

[4] Universitat Politecnica de Catalunya, Barcelona, Spain

[5] University of the Basque Country, Bilbao, Spain

[6] Thales Six GTS France SAS, Gennevilliers, France

[7] National Centre for Scientific Research "Demokritos", Agia Paraskevi, Athens, Greece