Supporting Mission Critical Services through Radio Access Network Slicing

J. Pérez-Romero, I. Vilà, O. Sallent
Dept.of Signal Theory and Communications
Universitat Politècnica de Catalunya (UPC)
Barcelona, Spain
jorperez@tsc.upc.edu, irene.vila.munoz@upc.edu, sallent@tsc.upc.edu

B. Blanco, A. Sanchoyerto, R. Solozábal, F. Liberal
Dept. of Communications Engineering
University of the Basque Country (UPV/EHU)
Bilbao, Spain
[begona.blanco, aitor.sanchoyerto, ruben.solozabal, fidel.liberal]@ehu.eus

***Abstract*—While the support of Mission Critical (MC) communications on commercial cellular networks has already been incorporated in the latest releases of Long Term Evolution (LTE), it is expected that the network slicing feature of Fifth Generation (5G) systems will further boost the provision of these services thanks to the possibility of creating customized and isolated network slices adapted to the specific requirements of MC communications. At the Radio Access Network (RAN), the realization of a network slice requires to specify how the pool of available radio resources is split between the different slices in accordance with their service requirements. In this context, this paper addresses the use of RAN slicing for provisioning MC services taking as a reference the emergency scenario defined by the 5G ESSENCE project. It is characterized by different stages associated to the occurrence of an incident and its evolution, thus involving different communication needs. For each stage, an estimation of the capacity requirements to be granted to the MC RAN slice is provided. Then, the architecture of the project is discussed, focusing on the components that enable the RAN slicing management to properly support MC services.**

Keywords—Network slicing; 5G New Radio; RAN slice; Mission Critical services

I. INTRODUCTION

Fifth Generation (5G) systems will support a wide range of application scenarios and vertical industries (e.g. automotive, e-health, utilities, smart cities, high-tech manufacturing) with very different requirements in terms of data rate, latency, mobility, etc. [1]. Besides, 5G networks are expected to evolve current business models for the different stakeholders by providing more flexible network sharing models [2]. In this direction, neutral host infrastructure services enable that multiple tenants, e.g. mobile network operators (MNO), Over-the-top (OTT) service providers or private enterprises from vertical industries, provide services to their own users by sharing a common infrastructure deployed, operated and managed by a 3rd party , referred to as the Infrastructure Provider (InP). The InP could be e.g. the owner of the venue where the shared infrastructure is deployed or a MNO that provides network slicing services to business customers on top of its own infrastructure [3]. The *network slicing* feature introduced in the 5G system architecture [4] plays a central role for supporting this sharing model and realizing cost-efficient solutions that accommodate the foreseen heterogeneity of requirements by the diverse types of tenants. Network slicing allows sharing a common infrastructure among diverse end-to-end logical networks, referred to as *network slices*, which can be tailored to a given system behaviour with optimised characteristics for a specific application [5].

A relevant application of network slicing capability is the provision of Public Safety (PS) communication services making use of the same infrastructure used for the rest of commercial services, but operating in different slices. In contrast to the current situation, in which specific PS networks exist such as Terrestrial Trunked Radio (TETRA) or Tetrapol, the use of commercial networks will facilitate the support of new broadband services requested by first responders and PS operators including the exchange of data, images and video in addition to voice [6]. In this direction, 3GPP already started to include in Releases 12, 13 and 14 functionalities related to Mission Critical (MC) applications for public safety in the mobile networks standards [7]. In turn, the novel features of 5G including network slicing, Network Function Virtualization (NFV), Multi-access Edge Computing (MEC), Software-Defined Networking (SDN) or cloud computing will furthermore empower 5G to use the common infrastructure for the commercial users to support PS services within them [7][8][9][10].

Among the current activities towards the development of 5G systems, the 5G ESSENCE project [11] addresses the provision of Small Cells as a Service (SCaaS) to facilitate a third-party provisioning of radio access capacity to mobile network operators in dense localised areas. The project proposes a highly flexible and scalable platform relying on Cloud Enabled Small Cells (CESCs) in conjunction with NFV and MEC technologies, able to accommodate the requirements of different use cases associated to vertical industries. One of the considered use cases of the project deals with the support of PS services, relying on the creation of specific network slices for the PS and the commercial services.

A network slice is composed of one network slice subnet instance that includes the Radio Access Network (RAN) functions, denoted as RAN slice, and another one with the core network functions. The realization of RAN slices is particularly challenging because it has to address how the pool of radio resources available to one RAN node (e.g. a gNB in the case of 5G) can be configured and operated to simultaneously deliver multiple and diverse behaviours [12].

The lifecycle management (i.e. creation, modification, and termination processes) of RAN slices can be dynamically carried out through automatic network slicing management systems [13], so that the number and configuration of the activated RAN slices remains closely matched to the needs and dynamics of the scenario. Specifically, when a new RAN slice has to be created, the slicing management system needs to accurately estimate the amount of radio resources that will be needed by this slice to ensure its service requirements. In this way, the management system can allocate the appropriate capacity to the slice in each gNB and configure accordingly the Radio Resource Management (RRM) mechanisms to provide this capacity in the cells of this gNB. This process is particularly critical because the variability in the radio propagation and interference conditions experienced by the users in a cell, the cell location (e.g. indoor, urban, rural, etc.) and deployment (e.g. cell radius, frequency, transmitted power, etc.) impact on the cell capacity and thus on the amount of radio resources needed to support the requirements of a RAN slice.

Based on the above, this paper focuses on the use of RAN slicing for supporting MC services in a shared cellular infrastructure, as considered by the 5G ESSENCE project. Specifically, the paper will describe the MC scenario considered in the project, which consists in three different stages representing, respectively, the default operation situation, the occurrence of an emergency incident requiring additional capacity for MC services and a further capacity extension associated to the evolution of the incident. For each of the stages, an estimation of the capacity requirements to be granted to the MC slice and the impact on the services of the commercial slice will be given. Then, the paper will discuss the architecture of the 5G ESSENCE project focusing on the components that enable the management of RAN slices to properly support MC services.

The rest of the paper is organized as follows. Section II presents the MC scenario considered in the 5G ESSENCE project. Section III presents estimation of the radio resources required by the MC slice and includes some results in the considered scenario. Then, Section IV discusses the architectural solution considered in the 5G ESSENCE project to deal with the management of the MC slices. Finally, conclusions are summarized in Section V.

II. SCENARIO DESCRIPTION

To show the capability of the 5G ESSENCE platform to provide different types of users with the required level of service in a shared network model, the project has defined a scenario that involves one PS communications provider with a Mission Critical Push To Talk (MCPTT) service and one commercial communications provider (e.g. offering a video streaming service). The two service providers share the resources available at a deployed cellular infrastructure. The challenge consists on providing the required RAN slice in order to allocate the radio resources to the critical actors (e.g., the first responders), who by nature require prioritized and high quality services.

MCPTT is a MC communication standard that allows half duplex group and one-to-one voice services. MCPTT is designed to coordinate emergency teams. It provides an arbitrated method to engage two or more users in communication. Users request permission to transmit pressing a button. 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. 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.

For the scenario configuration, 5G ESSENCE considers an incident in the central train station of a medium sized city. The public safety resources of the city involve three fire stations, three emergency services offices, three hospitals, the transport police that operates in the train station and the emergency coordination centre (112 headquarter). The communication between the participants in the incident is performed through the MCPTT service. In this context, the deployment of the cellular network includes 4 zones that divide the city into 4 coverage areas:

- Zone 1: includes the Fire Station 1, the Emergency Services Office 1 and the Hospital 1.
- Zone 2: includes the Fire Station 2, the Emergency Services Office 2 and the Hospital 2.
- Zone 3: includes the Fire Station 3, the Emergency Services Office 3, the Hospital 3, the Transport Police Headquarters and the Emergency Coordination.
- Zone 4: includes the Train station.

With this layout, the scenario is organised in three stages. Initially, only the basic personnel are deployed for surveillance operations. The occurrence of an incident triggers the transition to the second stage, attracting first responders to the scene and, therefore, increasing communication requirements. Finally, the events lead to the declaration of emergency state in the third stage, which involves another reconfiguration of the network to guarantee the communication between the PS forces. Next, we will describe with more detail the development of the incident and how the different PS bodies are activated.

A. Stage 1: Initial situation

It is an ordinary working day at the train station. The Transport Police (TP) is in charge of surveillance, control and security. At this moment, there are two agents (TP_01 and TP_02) patrolling the station (zone 4). There are two additional agents (TP_03 and TP_04) in zone 3, two more (TP_05 and TP_06) in zone 2 and another two (TP_07, TP_08) in zone 1. The central police station belongs to zone 3 where the Transport Police Officer TPO_01 coordinates the 8 agents through 2 MCPTT group calls. At the same time, the officer TPO_01 is in direct contact with the Transport Police Captain (TPC_01) via a private call. TPC_01 is located at the TP headquarters located in zone 3.

Additionally, each fire station is managed by a Fire Captain (FIREC) and a Fire agent (FIRE). At this time, they are located in their respective stations and are coordinated through a MCPTT private call.

In the hospitals, the emergency department is coordinated by an Urgent Care Manager (UCM) and an Urgent Care Medical Officer (UCMO). Coordination is done through a private MCPTT call.

Urgent health care at the scene of the incident, stabilization, cataloguing and transport of the injured to the hospital is carried out through the "Emergency Care Assistance" service. This service works in the city from its three bases located in zones 1, 2 and 3. The coordination of each of the bases is carried out by an Emergency Care Assistance Captain (ECAC) and an Emergency Care Assistance Officer (ECAO). In each of the bases, a private MCPTT call is established between them.

Table I provides a list of all the active calls and Table II shows their distribution along the 4 zones.

TABLE I. LIST OF MCPTT CALLS IN STAGE 1

Call Type	ID	Participants
MCPTT Private Call	PC_01	TPC_01, TPO_01
	PC_02	FIREC_01, FIREO_01
	PC_03	FIREC_02, FIREO_05
	PC_04	FIREC_03, FIREO_09
	PC_05	UCM_01, UCMO_01
	PC_06	UCM_02, UCMO_05
	PC_07	ECAC_01, ECAO_01
	PC_08	ECAC_02, ECAO_05
	PC_09	ECAC_03, ECAO_09
MCPTT Group Call	GC_01	TPO_01, TP_01...TP_04
	GC_02	TPO_01, TP_05...TP_08

TABLE II. DISTRIBUTION OF CONNECTIONS PER ZONE IN STAGE 1

	Zone 1	Zone 2	Zone 3	Zone 4
MCPTT Private Calls	PC_02 (2) PC_05 (2) PC_07 (2)	PC_03 (2) PC_06 (2) PC_08 (2)	PC_01 (2) PC_04 (2) PC_09 (2)	
MCPTT Group Calls	GC_02 (2)	GC_02 (2)	GC_01 (4)	GC_01 (2)
Total user connections	8	8	10	2

B. Stage 2: The incident occurs

An explosion is heard within the station precincts and transport police officers at the station are sent to investigate. They discover the remains of a container that has exploded, causing physical injuries to 5 people in the vicinity. Of greater concern is the fact that these 5 and 4 others all appear to be having respiratory difficulties and there is evidence of some form of powder residue on surfaces close to the seat of the explosion. The agent TP_01 at the scene informs the immediate superior (TPO_01) through the group call (GC_01) already established. The officer TPO_01 establishes a private call (PC_01) with the captain TPC_01 to inform about the incident.

In this moment, TPO_01 establishes an Emergency Private Call (EPC_01) with the 112 Headquarter, who declares an Emergency Incident and increases the Antiterrorist Alert Level (AAL) to 5 (High). But it still does not declare a potential terrorist incident.

The 112 headquarter sends a 112 Mobile Command Vehicle Post and a 112 Emergency Technician (112_ET) to the train station. This settles the advanced command post that will manage all the emergency services from the train station.

The Emergency Technician (112_ET) establishes an Emergency Group Call (EGC) with the captains of each service and each captain establishes a MCPTT private call with one staff policeman to inform about the action that the 112_ET decides during the incident.

During the Stage 2, the 112 Emergency Technician (112_ET) activates all the Transport Police resources, Fire Headquarter 1, Hospital 1, Emergency Care Assistance Headquarter 1 and 2.

The officers and the staff of all of the activated resources go to the station (zone 4). The resources of the hospital 1 will not move to the train station. The Fire Headquarter 2 and Fire Headquarter 3 have all the resources activated but they remain in the headquarter until they are activated by 112_ET.

As in the previous subsection, Table III provides a list of all the active calls and Table IV shows their distribution along the 4 zones.

TABLE III. LIST OF MCPTT CALLS IN STAGE 2

Call Type	Name	Participants
MCPTT Emergency Group Call	EGC_01	TPC_01, FIREC_01, FIREC_02, FIREC_03, UCM_01, UCM_02, ECAC_01, ECAC_02, ECAC_03
MCPTT Private Call	PC_10	TPC_01, TPO_01
	PC_11	FIREC_01, FIREO_01
	PC_12	FIREC_02, FIREO_05
	PC_13	FIREC_03, FIREO_09
	PC_14	UCM_01, UCMO_01
	PC_15	UCM_02, UCMO_05
	PC_16	ECAC_01, ECAO_01
	PC_17	ECAC_02, ECAO_05
	PC_18	ECAC_03, ECAO_09
MCPTT Group Call	GC_03	TPO_01, TP_01...TP_04
	GC_04	TPO_01, TP_05...TP_08
	GC_05	FIREO_01, FIRE_01…FIRE_04
	GC_06	UCMO_01, DOC_01…DOC_04
	GC_07	ECAO_01, ECAD_01...ECAD_04
	GC_08	ECAO_02, ECAD_05...ECAD_08

TABLE IV. DISTRIBUTION OF CONNECTIONS PER ZONE IN STAGE 2

	Zone 1	Zone 2	Zone 3	Zone 4
MCPTT Emergency Group Call	EGC_01(3)	EGC_01 (3)	EGC_01 (2)	EGC_01(1)
MCPTT Private Call	PC_11(1) PC_14(2) PC_16(1)	PC_12(2) PC_15(2) PC_17(1)	PC_10(1) PC_13(2) PC_18(2)	PC_10(1) PC_11(1) PC_16(1) PC_17(1)
MCPTT Group Call	GC_06 (5)			GC_03 (5) GC_04 (5) GC_05 (5) GC_07 (5) GC_08 (5)
Total user connections	12	8	7	30

C. Stage 3: State of emergency

The Emergency Technician (112_ET) declares a potential terrorist incident. The first consequence of this decision is the activation of Hospital, Emergency Care Assistance Headquarter 3 and Fire Headquarters 2 and 3. As a result of the activation of these new resources, new group calls are created.

The Transport Office moves 12 Transport Police agents to zone 4 organized in three groups: GC_19, GC_20 and GC_21. The police officer TPO_01 coordinates these resources. TPO_01 establishes 3 MCPTT call groups, one per group and is included in all of the Transport Police group calls of this incident.

Again, Table V provides a list of all the active calls and Table VI shows their distribution along the 4 zones.

TABLE V. LIST OF MCPTT CALLS IN STAGE 3

Call Type	Name	Participants
MCPTT Emergency Group Call	EGC_01	TPC_01, FIREC_01, FIREC_02, FIREC_03, UCM_01, UCM_02, ECAC_01, ECAC_02, ECAC_03
MCPTT Private Call	PC_19	TPC_01, TPO_01
	PC_20	FIREC_01, FIREO_01
	PC_21	FIREC_02, FIREO_05
	PC_22	FIREC_03, FIREO_09
	PC_23	UCM_01, UCMO_01
	PC_24	UCM_02, UCMO_05
	PC_25	ECAC_01, ECAO_01
	PC_26	ECAC_02, ECAO_05
	PC_27	ECAC_03, ECAO_09
MCPTT Group Call	GC_09	TPO_01, TP_01...TP_04
	GC_10	TPO_01, TP_05...TP_08
	GC_11	FIREO_01, FIRE_01…FIRE_04
	GC_12	UCMO_01, DOC_01…DOC_04
	GC_13	ECAO_01, ECAD_01...ECAD_04
	GC_14	ECAO_02, ECAD_05...ECAD_08
	GC_15	UCMO_02, DOC_05…DOC_08
	GC_16	UCMO_03, DOC_09…DOC_12
	GC_17	FIREO_02, FIRE_05…FIRE_08
	GC_18	FIREO_02, FIRE_09…FIRE_12
	GC_19	TPO_01, TP_09...TP_12
	GC_20	TPO_01, TP_13...TP_16
	GC_21	TPO_01, TP_17...TP_20

TABLE VI. DISTRIBUTION OF CONNECTIONS PER ZONE IN STAGE 3

	Zone 1	Zone 2	Zone 3	Zone 4
MCPTT Emergency Group Call	EGC_01(3)	EGC_01 (3)	EGC_01 (2)	EGC_01(1)
MCPTT Private Call	PC_20(1) PC_23(2) PC_25(1)	PC_21(2) PC_24(2) PC_26(1)	PC_19(1) PC_22(2) PC_27(2)	PC_19(1) PC_20(1) PC_25(1) PC_26(1)
MCPTT Group Call	GC_11 (5)	GC_14 (5)		GC_09 (5) GC_10 (5) GC_12 (5) GC_13 (5) GC_15 (5) GC_16 (5) GC_17 (5) GC_18 (5) GC_19 (5) GC_20 (5) GC_21 (5)
Total user connections	12	13	7	60

III. CAPACITY REQUIREMENTS

Based on the considered scenario, this section determines the capacity needed by the RAN slice that provides PS communications in the considered zones. Assuming a radio technology based on 5G New Radio (NR), the capacity is measured in terms of the amount of Physical Resource Blocks (PRBs) needed by this RAN slice in each of the cells that cover the identified zones, where a PRB is defined as a block of 12 consecutive Orthogonal Frequency-Division Multiple Access (OFDMA) subcarriers. This section describes the methodology for estimating the number of required PRBs and then it presents some results in the considered scenario.

A. Estimation of PRB requirements of the MCPTT RAN slice

Let us assume that the PS communications provider of the MCPTT service makes use of a RAN Slice Instance (RSI) deployed on the shared cellular infrastructure that provides coverage in the different zones of the scenario.

MCPTT service requirements are given in terms of the Guaranteed Bit Rate (GBR) value to be ensured to each MCPTT call and the maximum degradation probability $P_{d,max}$, which represents the maximum allowed percentage of the call duration time that the MCPTT service experiences transfer bit rates lower than its requirement *GBR*. Note that this last parameter represents an important requirement for MCPTT services, due to its mission critical nature.

Given that, in general, the MCPTT RSI may operate in diverse cell sites with a variety of deployment characteristics (radius, transmitted power, location, frequency operation, etc.) and, consequently, users experience different propagation conditions, different bit rates per PRB are achieved in each of the cells. For this reason, the proposed methodology to compute the number of PRBs required by the RSI is performed on a per cell-basis using the statistical characterisation of the spectral efficiency in each cell provided by data analytics functions, following the approach described in [14]. In this sense, the spectral efficiency S_{eff} is treated as a random variable and its probability density function (pdf), denoted as $f_{Seff}(s)$, is obtained by gathering samples of the experienced wideband Channel Quality Indicator (CQI) of the different users in each cell.

Based on $f_{Seff}(s)$, the following metrics are obtained for carrying out the PRB estimation process: (a) average spectral efficiency $\overline{S_{eff}}$ of the cell; (b) pdf of the random variable $Y=1/(S_{eff} \cdot B)$, denoted as $f_Y(y)$, where B is the PRB bandwidth, and is obtained as:

$$f_Y(y) = f_{S_{eff}}\left(\frac{1}{y \cdot B}\right)\frac{1}{y^2 B} \quad (1)$$

In order to achieve *GBR*, the number of PRBs required by a call of a user with spectral efficiency S_{eff} is:

$$N_{req} = \frac{GBR}{S_{eff} \cdot B} \quad (2)$$

Consequently, N_{req} is another random variable with pdf given by:

$$f_{N_{req}}(k) = f_Y\left(\frac{k}{GBR}\right)\frac{1}{GBR} \quad (3)$$

Then, assuming a total of u MCPTT users with an active call in the cell and that each user experiences independent propagation conditions, the pdf of the aggregate number of required PRBs r by all the MCPTT users is given by:

$$f_r(k) = \left(\frac{1}{GBR}\right)^u \cdot \underbrace{f_Y\left(\frac{k}{GBR}\right) * \ldots * f_Y\left(\frac{k}{GBR}\right)}_{u} \quad (4)$$

where * represents the convolution operator.

The service degradation will occur whenever the aggregate number of required PRBs r is higher than the number of PRBs available in the cell for the MCPTT RSI, denoted as N_{th}. Therefore, in order to ensure the maximum degradation probability requirement $P_{d,max}$, the required number of PRBs N_{th} is given by the minimum integer value that satisfies the following condition:

$$P_{d,\max} \geq \int_{N_{th}}^{\infty} f_r(k)dk \quad (5)$$

B. Results

Let us assume that each one of the four zones of the scenario is covered by a different cell. The configuration parameters of the cells are shown in Table VII. The MCPTT service requirements are given by GBR=50 kb/s and different values of $P_{d,max}$ will be considered in the results.

TABLE VII. CELL CONFIGURATION PARAMETERS

Parameter	Value
Cell radius	288 m
gNB height	25 m
UE height	1.5 m
Minimum gNB-UE distance	35 m
Path Loss and Shadowing model	Urban Macrocell model of Sec. 7.4 of [15]
Shadowing standard deviation in LOS	4 dB
Shadowing standard deviation in NLOS	6 dB
Frequency	3.6 GHz
gNB transmitted power (dBm/PRB)	18 dBm
gNB antenna Gain	Omnidirectional antenna with 5 dBi gain
UE noise figure	9 dB
Average Spectral efficiency ($\overline{S_{eff}}$)	4.45 b/s/Hz
Link-level model to map SINR and bit rate	Model in Sec. 5.2.7 of [16] with maximum SINR= 30 dB and minimum SINR= -10 dB with alpha parameter=0.6
PRB Bandwidth (B)	180 kHz, corresponding to subcarrier spacing 15 kHz [17]
Number of PRBs per cell	106, corresponding to cell bandwidth 20 MHz [18]

Fig. 1 plots the number of PRBs N_{th} required by the MCPTT RSI in each cell to support the traffic conditions existing in each stage of the scenario. The cell number corresponds to the zone number. Results are obtained for a maximum degradation probability $P_{d,max}$=0.1%. The figure shows that the impact of the traffic increase associated to the emergency incident is particularly relevant in the case of the cell 4 that provides service to the train station where the incident has occurred. Specifically, under normal conditions (stage 1) one single PRB is sufficient to serve the MCPTT communication needs. This PRB will be dynamically assigned by the scheduler to the different users on a short (i.e. 1 ms) so that each user gets on average the required GBR. In turn, with the traffic increase associated to the incident occurrence (stage 2) and the declaration of the emergency state (stage 3), this PRB becomes insufficient to serve all the users, thus requiring the extension of the MCPTT RSI capacity in the cell 4 with additional PRBs. Comparing the number of PRBs for this cell in Fig. 1 with the number of user connections indicated in Tables II, IV and VI for the different stages, it can be noticed that the number of required PRBs does not scale linearly with the number of users.

As for the rest of cells, even though the different stages of the incident involve some traffic increase, this can still be properly served in cells 1 and 3 with the same number of PRBs as during the normal operational conditions (stage 1), so no RSI reconfiguration is needed in these cells. For cell 2, an additional PRB is required in stage 3.

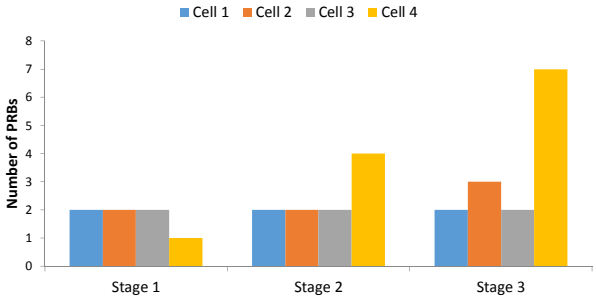

Fig. 1 Number of required PRBs for the MCPTT RSI in the different cells and stages for $P_{d,max}$=0.1%.

To analyse the impact of the service requirements, Fig. 2 plots the number of PRBs required by the MCPTT RSI in cell 4 for different values of the maximum degradation probability $P_{d,max}$. It is observed that the number of PRBs increases when reducing the value of $P_{d,max}$, which corresponds to more stringent requirements. In any case, the observed increase is quite moderate, as observed from the fact that in stages 2 and 3 a reduction of the degradation probability in two orders of magnitude from 1% down to 0.01% can be just achieved with two additional PRBs.

The impact of the increase of PRB requirements in the MCPTT RSI for the different stages of the incident over the performance obtained by the RSI of the commercial service provider is shown in Fig. 3. The figure plots the aggregate average throughput available in cell 4 for the different stages. The throughput is progressively reduced as more PRBs are allocated to the MCPTT RSI, since, for every reconfiguration of this slice, the commercial RSI will have less PRBs available from the total in the cell. However, the reduction is relatively small, e.g. for the case $P_{d,max}$=0.01% the throughput in stage 3 is only 5.8% lower than the throughput in stage 1. This is due to the low GBR demanded by MCPTT calls, which allows supporting a large number of users with a relatively low number of PRBs.

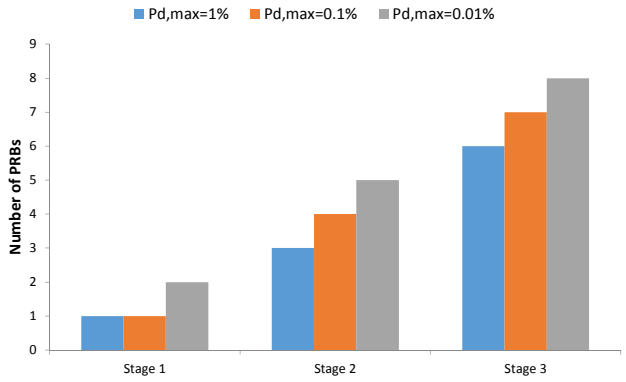

Fig. 2 Number of required PRBs for the MCPTT RSI in cell 4 for the different stages of the incident and with different values of $P_{d,max}$.

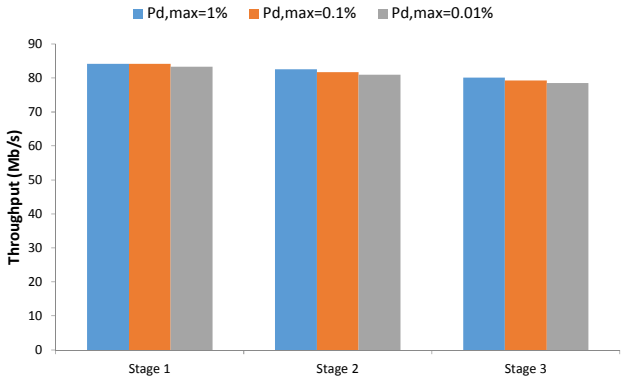

Fig. 3 Aggregate throughput available for the commercial RAN slice in cell 4 for different stages of the incident and different values of $P_{d,max}$

IV. 5G ESSENCE MANAGEMENT SOLUTION FRAMEWORK

The results of Section III have shown that the occurrence of an emergency situation can lead to substantial increases in the amount of required radio resources by an MCPTT RAN slice. This poses the challenge of how to appropriately deploy and manage the shared cellular network to deal with these increases. In this respect, an efficient design can be achieved by dimensioning the network to deal with the normal operating conditions and incorporate the dynamic mechanisms to modify the network when an incident occurs. In this direction, this section describes the mechanisms considered by the 5G ESSENCE project to provide the required dynamicity to deal with the needs of the different stages of an emergency.

A. 5G ESSENCE architecture

Fig. 4 depicts a simplified version of the general architecture considered by the 5G ESSENCE project [19]. It allows the different tenants (i.e. PS provider, commercial service provider, etc.) to provide service to their users through a number of CESCs deployed, owned and managed by a third party. A CESC is a multi-operator enabled small cell that integrates a virtualized execution platform for executing applications and services inside the access network infrastructure. A CESC consists of a small cell Physical Network Function (PNF) unit, where a subset of the small cell functionality is implemented via tightly coupled software and hardware, and a micro server that supports the execution of Virtualized Network Functions (VNFs), which provide the rest of the small cell functionality together with other added-value services.

The Network Function Virtualization Infrastructure (NFVI) in the architecture spans across two tiers, namely the Main Data Centre (DC) and the Light DC, the latter resulting from the aggregation of the micro servers in a cluster of CESCs. Among different service VNFs, the Main DC hosts the centralized Software Defined - Radio Access Network (cSD-RAN) controller, which enables the coordinated operation of the small cells by incorporating centralized RRM algorithms.

Also running in the Main DC, the MCPTT VNF is composed of four Virtualization Deployment Units (VDU), which are the simple building blocks that form a VNF. As shown in Fig. 5, these VDUs are the vMCPTT_AS (Application Server), the vCSC (Common Services Core), the vIMS (IP Multimedia Subsystem) and the vDNS (Domain Name System). The vMCPTT_AS is the main component that provides the push-to-talk functionality. The vCSC provides auxiliary services such as identity, group, key and configuration management, required to support the MCPTT voice service. Finally, the vIMS is a Session Initiation Protocol (SIP) core, also required to support the MCPTT voice communications, and the vDNS is used for service discovery. All these components, and the ones that are described next are internally connected through a series of Virtual Links (V) between the Connection Points (C) that provide the internal interface to each module. A VNF including the described VDUs is able to provide a standard MCPTT service. However, in order to take the maximum advantage of 5G ESSENCE architecture and its enhanced management and orchestration features, the network service must offer some monitoring capabilities. The VNF includes a mcptt_exporter that exposes user and service metrics through

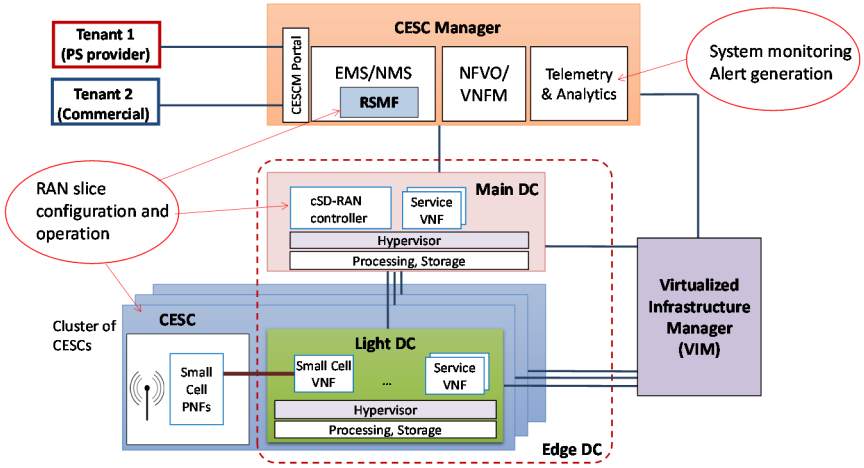

Fig. 4 General architecture of 5G ESSENCE

a REST API for external monitoring. The exporter uses a collection task inside the vIMS to collect metrics about the users of the service (registered users, active users,…) and pulls service metrics from the vMCPTT_AS (number and types of calls).

The CESC Manager (CESCM) in Fig. 4 is the central service management component in the architecture that integrates the traditional network management elements, i.e. Element Management System (EMS) and Network Management System (NMS), and the novel functional blocks of the Network Function Virtualization Management and Orchestration (NFV-MANO) framework, namely the Network Function Virtualization Orchestrator (NFVO) and the VNF Manager (VNFM). The CESCM includes telemetry and analytics functions which, based on different metrics collected from the different components of the architecture, provide Management Data Analytics Services (MDAS) to other management functions.

The RAN Slicing Management Function (RSMF) is included in the CESCM as part of the EMS or the NMS and it is in charge of the lifecycle management (i.e. creation, modification and termination) of RSIs. For this purpose, the RSMF interacts with the cSD-RAN controller and the CESCs to properly configure the radio access capabilities at the layers 1, 2 and 3 of the radio interface protocol stack to support the RAN slices.

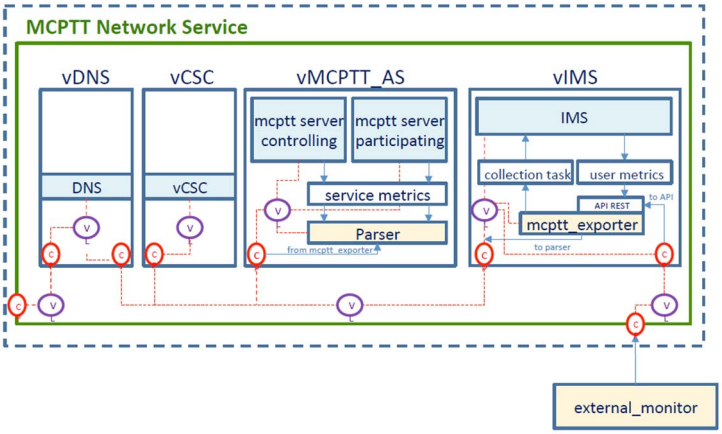

Fig. 5 Functional architecture of the MCPTT VNF.

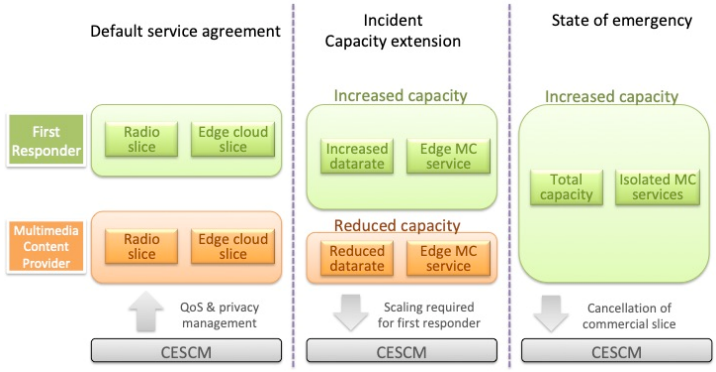

Fig. 6 Slicing and resource allocation to services.

B. Dynamic mechanisms to deal with emergency scenarios

The 5G ESSENCE platform must be able to react to the events associated to an emergency situation in order to allocate the necessary resources for first responders at each time, as depicted in Fig. 6. Under normal circumstances, the 5G ESSENCE platform owner is providing the required RAN slice to each service. For the MCPTT service, normal operations require a basic access for the working personnel. Then, when an incident happens, the PS communications provider will demand additional resources in order to cope with an increased number of incoming first responders, and therefore the CESCM must react to the new MCPTT requirements. Based on pre-arranged or on-demand service scaling policies, the CESCM will implement new elastic resource allocation schemes, giving priority access to first responders. In this respect, the RSMF will modify accordingly the MCPTT RSI to increase its amount of radio resources. Further capacity extensions may be needed depending on how the situation evolves and the number of actors working on the scenario. Eventually, in case of declaring the state of emergency, the CESCM may cancel the commercial slice and assign all the RAN capacity to the MCPTT service.

To provide the capability of detecting the need to modify the MCPTT RSI, the MCPTT service is integrated into the 5G ESSENCE architecture through the monitoring system that is part of the Telemetry and Analytics module. The monitoring system collects data about the status of the infrastructure and the running services at different levels using a variety of parameter exporters installed in the modules involved (Fig. 4). All this information is stored and later processed by the monitoring system. This system applies the policies designed according to the Service Level Agreement (SLA) between the PS provider and the infrastructure owner to generate the alerts that will be used to dynamically reconfigure the system.

In particular and as shown in Fig. 7, for the case of the MCPTT service, the monitoring system collects information about the number of users in the system, both registered and active, and also information about the on-going and cancelled voice calls. This set of data can be combined with additional data from the cloud infrastructure and from the cSD-RAN controller about the distribution of users along the CESCs. More precisely, knowing that each user requires 50 kb/s per active conversation, and monitoring the number of users per cell, it is possible to estimate and adjust the RAN slice per cell. Modifications of the RAN slice will be done by means of the RSMF, which will configure the radio protocol stack at the cSD-RAN controller and the CESC to provide the capacity required by the slice. On the other hand, the combination of the service operation parameters with the information about the status of the cloud infrastructure (memory, storage and computing resources) can lead to take scaling decisions on the NFVI resources used by the VNFs

of the MCPTT service. These will be executed through the NFVO and the Virtualized Infrastructure Manager (VIM).

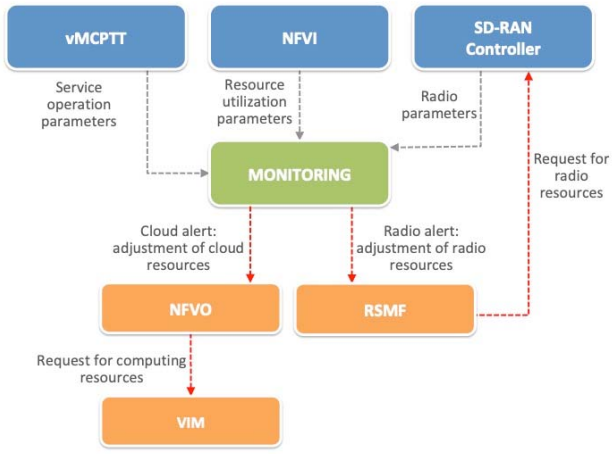

Fig. 7 System monitoring process.

V. CONCLUSIONS

This paper has focused on the use of RAN slicing for supporting mission critical services in an emergency scenario characterized by different stages that involve increasing communication needs associated to the occurrence of an incident and the eventual declaration of the emergency state. Starting from a detailed scenario that represents these situations as considered by the 5G ESSENCE project, the paper has analysed the dimensioning of the RAN slice instance that supports the MCPTT services in terms of the number of required PRBs. The results have shown that the traffic increase associated to the emergency occurrence involves reconfigurations in the MCPTT RAN slice to increase the number of allocated PRBs. Based on this, the paper has presented the 5G ESSENCE architecture and its monitoring, analytics and RAN slicing management mechanisms that allow dynamically handling the RAN slice reconfigurations.

ACKNOWLEDGEMENT

This work has been supported by the EU funded H2020 5G-PPP project 5G ESSENCE under grant agreement 761592, by the Spanish Research Council and FEDER funds under SONAR 5G grant (ref. TEC2017-82651-R) and 5RANVIR (ref. TEC2016-80090-C2-2-R) and by the Secretariat for Universities and Research of the Ministry of Business and Knowledge of the Government of Catalonia under grant 2019FI_B1 00102.

REFERENCES

[1] NGMN Alliance, “5G White Paper,” February 2015.

[2] X. Zhou, R. Li, T. Chen and H. Zhang, "Network slicing as a service: enabling enterprises' own software-defined cellular networks," in *IEEE Communications Magazine*, vol. 54, no. 7, pp. 146-153, July 2016.

[3] K. Samdanis, X. Costa-Perez and V. Sciancalepore, "From network sharing to multi-tenancy: The 5G network slice broker," in *IEEE Communications Magazine*, vol. 54, no. 7, pp. 32-39, July 2016.

[4] 3GPP TS 23.501 v15.2.0 “System Architecture for the 5G System; Stage 2 (Release 15)”, June, 2018.

[5] P. Rost et al. “Network Slicing to Enable Scalability and Flexibility in 5G Mobile Networks”, *IEEE Communications Magazine*, vol. 55, no. 5, pp. 72-79, May, 2017.

[6] R. Fantacci, F. Gei, D. Marabissi and L.Micciullo, “Public Safety Networks Evolution toward Broadband: Sharing Infrastructures and Spectrum with Commercial Systems”, *IEEE Commun. Magazine*, pp.24-30, April 2016.

[7] M. Höyhtyä, K. Lähetkangas, J. Suomalainen and others, “Critical communications over mobile operators’ networks: 5G use cases enabled by licensed spectrum sharing, network slicing and QoS control.” *IEEE Access*, Vol. 6, 10.1109/ACCESS.2018.2883787, December 2018.

[8] B. Blanco *et al.*, ‘‘Technology pillars in the architecture of future 5G mobile networks: NFV, MEC and SDN,’’ *Comput. Standards Interfaces*, vol. 54, pp. 216–228, Nov. 2017. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0920548916302446

[9] R. Solozabal, A. Sanchoyerto, E. Atxutegi, B. Blanco, J. O. Fajardo and F. Liberal, "Exploitation of Mobile Edge Computing in 5G Distributed Mission-Critical Push-to-Talk Service Deployment," in *IEEE Access*, vol. 6, pp. 37665-37675, 2018. doi: 10.1109/ACCESS.2018.2849200.

[10] M. R. Spada, J. Perez-Romero, A. Sanchoyerto, R. Solozabal, M. A. Kourtis, V. Riccobene, “Management of Mission Critical Public Safety Applications: the 5G ESSENCE Project”, European Conference on Network and Communications (EuCNC 2019), Valencia, Spain, June, 2019.

[11] 5G ESSENCE project website: http://www.5g-essence-h2020.eu/Home.aspx

[12] R. Ferrús, O. Sallent, J. Pérez-Romero, R. Agustí, “On 5G Radio Access Network Slicing: Radio Interface Protocol Features and Configuration”, *IEEE Communications Magazine*, May, 2018, pp.184-192.

[13] R. Ferrús, O. Sallent, J. Pérez-Romero and R. Agusti, "On the Automation of RAN Slicing Provisioning and Cell Planning in NG-RAN," 2018 *European Conference on Networks and Communications (EuCNC)*, Ljubljana, Slovenia, 2018, pp. 37-42.

[14] I. Vilà, J. Pérez-Romero, O. Sallent, A. Umbert, R. Ferrús, “Performance Measurements-based Estimation of Radio Resource Requirements for Slice Admission Control”, IEEE 90th Vehicular Technology Conference (VTC2019-Fall), Honolulu, USA, 22-25 September, 2019.

[15] 3GPP TR 38.901 v15.5.0, “Study on channel model for frequencies from 0.5 to 100GHz (Release 15),” March 2019.

[16] 3GPP TR 38.803 v14.2.0, “Study on new radio access technology: Radio Frequency (RF) and co-existence aspects (Release 14),” September 2017.

[17] 3GPP TS 38.214 v15.5.0, “NR; Physical layer procedures for data (Release 15),” March 2019.

[18] 3GPP TS 38.104 v15.5.0, “NR; Base Station (BS) radio transmission and reception (Release 15),” April 2019.

[19] I. Giannoulakis (editor), “Overall System Architecture and Specifications”, Deliverable D2.2 of the 5G ESSENCE project, February, 2018.