NOVA SCHOOL OF SCIENCE & TECHNOLOGY

DEPARTMENT OF
APPLIED SOCIAL SCIENCES

MISSION-CRITICAL COMMUNICATIONS FROM LMR TO 5G

A TECHNOLOGY ASSESSMENT APPROACH FOR SMART CITY SCENARIOS

DÉBORA VANESSA CAMPOS FREIRE

Master in Information Science

DOCTORATE IN TECHNOLOGY ASSESSMENT

NOVA University Lisbon
April 2023

NOVA SCHOOL OF SCIENCE & TECHNOLOGY

DEPARTMENT OF
APPLIED SOCIAL SCIENCES

MISSION-CRITICAL COMMUNICATIONS FROM LMR TO 5G

A TECHNOLOGY ASSESSMENT APPROACH FOR SMART CITY SCENARIOS

DÉBORA VANESSA CAMPOS FREIRE

Master in Information Science

Advisor: António Paulo Brandão Moniz de Jesus,
Associate Professor with Habilitation at NOVA School of Science and Technology, NOVA University Lisbon

Examination Committee:

Chair: Paulo da Costa Luís da Fonseca Pinto
Full Professor, NOVA School of Science and Technology, NOVA University Lisbon

Rapporteurs: Maísa Mendonça Silva
Associate Professor, Federal University of Pernambuco, Brazil
Pedro Filipe Xavier Mendonça
Cybersecurity Observatory Coordinator, Portugal

Advisor: António Paulo Brandão Moniz de Jesus,
Associate Professor with Habilitation at NOVA School of Science and Technology, NOVA University Lisbon

Members: Ana Clara Cândido,
Assistant Professor, Federal University of Santa Catarina, Brazil
Luís António Vicente Baptista
Full Professor, NOVA School of Social Sciences and Humanities, NOVA University Lisbon
Paulo da Costa Luís da Fonseca Pinto
Full Professor, NOVA School of Science and Technology, NOVA University Lisbon

DOCTORATE IN TECHNOLOGY ASSESSMENT

NOVA University Lisbon
April 2023

Mission-Critical Communications from LMR to 5G: a Technology Assessment approach for Smart City scenarios

This document was created with Microsoft Word text processor and the NOVA thesis Word template [1].

This work is dedicated to the ideal of a more democratic, egalitarian and collaborative society. I wish technological development could help us make this ideal a reality.

I also dedicate this work to the people of the Brazilian Northeast, who, despite so many difficulties, know better than anyone how to reap good fruits from arid land and how to turn small opportunities into a life change.

ACKNOWLEDGMENTS

I would like to express my gratitude to all of those who provided support and discussions, those who offered comments, and those who participated in the interviews, allowing me to quote their opinions.

I wish to express my appreciation for those who supported me from the beginning of my journey from the master's to the doctorate, without whom perhaps the writing of this work would not have been possible.

Marcelo de Azambuja Fortes and Fernando Antônio Maciel Ramos, thank you for helping make this journey possible. Ana Clara Cândido, Cátia Maroco, Nadja Verônica Campos Freire and Fernanda Fontenelle, thank you for all the support and for helping me to believe this journey, although difficult, would be possible.

I should also like to thank my supervisor, Professor António Brandão Moniz, for his support.

Finally, I'd like to express my thanks to the Federal Police of Brazil, for the opportunity to start this research.

"Only when we are fully aware of the limited scope of each point of view will we be on the way to the desired understanding of the whole" (Mannheim, 1972, p. 131).

ABSTRACT

Radiocommunication networks are one of the main support tools of agencies that carry out actions in Public Protection & Disaster Relief (PPDR), and it is necessary to update these communications technologies from narrowband to broadband and integrated to information technologies to have an effective action before society. Understanding that this problem includes, besides the technical aspects, issues related to the social context to which these systems are inserted, this study aims to construct scenarios, using several sources of information, that helps the managers of the PPDR agencies in the technological decision-making process of the Digital Transformation of Mission-Critical Communication considering Smart City scenarios, guided by the methods and approaches of Technological Assessment (TA).

Keywords: Mission-Critical Communication, Smart City; Public Protection & Disaster Relief (PPDR), 5G, Long Term Evolution (LTE), Technology Assessment

RESUMO

As redes de radiocomunicações são uma das principais ferramentas de apoio dos órgãos que realizam ações de Proteção Pública e Socorro em desastres, sendo necessário atualizar essas tecnologias de comunicação de banda estreita para banda larga, e integra- las às tecnologias de informação, para se ter uma atuação efetiva perante a sociedade . Entendendo que esse problema inclui, além dos aspectos técnicos, questões relacionadas ao contexto social ao qual esses sistemas estão inseridos, este estudo tem por objetivo a construção de cenários, utilizando diversas fontes de informação que auxiliem os gestores destas agências na tomada de decisão tecnológica que envolve a transformação digital da Comunicação de Missão Crítica considerando cenários de Cidades Inteligentes, guiado pelos métodos e abordagens de Avaliação Tecnológica (TA).

Palavas-chave: Comunicação de Missão Crítica, Cidades Inteligente, Proteção Pública e Assistência a Desastres, 5G, 4G, Avaliação de Tecnologia

CONTENTS

LIST OF FIGURES

Acronyms

2G	2nd generation
3D	Three dimensions
3G	3rd generation
3GPP	3rd Generation Partnership Project
4G	Fourth Generation
5G	Fifth Generation
5G-IoT	5G enabled IoT
AGA	Air-Ground-Air
AI	Artificial Intelligence
AIOps	Artificial Intelligence for IT Operations
ANPR	Automatic Number Plate Recognition
AR	Augmented Reality
ARFCN	Absolute Radio-Frequency Channel Number
ARP	Allocation and Retention Priority
ATG	Air-to-Ground
AeNB	Attached 4G eNodeB
BB	Broadband
BHCA	Busy Hour Call Attempts
BHRA	Busy Hour Register Attempts
BLER	Block Error Rate

BS	Base Station
CAM	Common Alerting Protocol
CAPEX	Capital Expenditures
CC	Critical Communication
CCC	Command and Control Center
CCTV	Closed-Circuit Television
CDNN	Convolutional Deep Neural Network
CERPS	Citizens Emergency Response Portal System
CESM	Composition-Environment-Structure-Mechanism
CIA	Central Intelligence Agency
CISA	Cybersecurity and Infrastructure Security Agency
CIoT	Cellular IoT
CO	Contractor Owned
COCO	Contractor Owned, Contractor Operated
CODet	City Object Detection
CPS	Cyber-Physical Systems
CQI	Channel Quality Indicator
CS	Coordinated Scheduling
CSI	Channel Status Information
CTA	Constructive Technological Assessment
CloudRAN	Cloud based Radio Access Network
CoMP	Coordinated MultiPoint
D2D	Device to Device
DHS	Department of Homeland Security
DITSEF project	Digital and Innovative Technologies for Security and Efficiency of First Responders operation
DL	Downlink
DMO	Direct Mode Operation

DPO	Data Protection Officer
DSCNs	Drone-based Small Cellular Networks
DSCs	Drone Small Cells
DSRC	Dedicated Short Range Communication
DSS	Decision Support Systems
E-UTRAN	Evolved UMTS Terrestrial Radio Access Network
E2EE	End-to End Encryption
EAS	Emergency Alert System
EC	European Commission
ECC	Electronic Communications Committee
EE	Everything Everywhere
EFR	Emergency First Responders
EMBMS	Evolved Multimedia Broadcast and Multicast Services
EMIS	Emergency Management Information System
EPC	Evolved Packet Core
EPS	Evolved Packet System
ESCAP	Economic and Social Commission for Asia and the Pacific
ESMCP	Emergency Services Mobile Communications Program
ETSI	European Telecommunications Standards Institute
EULER	European software defined radio for wireless in joint security operations
EWS	Early Warning System
FCC	Federal Communications Commission
FDD	Frequency Division Duplex
FEMA	Federal Emergency Management Agency
FIFA	Fédération Internationale de Football Association
FM	Frequency Modulation
FP7	Seventh Framework Programme

GCSE	Group Communication System Enabler
GDP	Gross Domestic Product
GFS	Google File System
GIS	Geographic Information System
GMG	Group Management
GO	Government Owned
GOCO	Government Owned, Contractor Operated
GOGO	Government Owned, Government Operated
GPS	Global Position System
GSM	Global System for Mobile Communications
GSMA	Groupe Speciale Mobile Association
GSP	Golden Shield Project
GTC	Grouping of Territorial Cooperation
GWCN	Gateway Core Network sharing
HAR	Human Activity Recognition
HCI	Human-Computer Interaction
HDFS	Hadoop Distributed File System
HELP Project	Enhanced Communications in Emergencies by Creating and Exploiting Synergies in Composite Radio Systems
HSS	Home Subscriber Server
HT	Handheld Terminal
ICIC	Intercell Interference Cancellation
ICS	Incident Command System
ICT	Information and Communication Technologies
ID	Identification
IDB	Inter-American Development Bank
IEEE	Institute of Electrical and Electronics Engineers
IMS	IP Multimedia Subsystem

IMT	International Mobile Telecommunications
IP	Internet Protocol
IPAWS	Integrated Public Alert and Warning System
ISI	Inter System Interface
ISITEP	Inter System Interoperability for TETRA and TETRAPOL NetworksISO
ISO	International Organization for Standardization
IT	Information Technology
ITS-S	Intelligent Transportation System – Station
ITU	International Telecommunication Union
IWF	Interworking Function
IoFRT	Internet of First Responder Things
IoPST	Internet of Public Safety Things
IoT	Internet of Things
IoUT	Internet of Underwater Things
KDD	Knowledge discovery in databases
KLU	Key Load Unit
KMC	Key Management Center
KPI	Key Performance Indicator
LMR	Land Mobile Radio
LSA	Licensed Shared Access
LTE	Long Term Evolution
LTE-R	LTE-based high-speed Railway
LoS	Line-of-Sight
M2M	Machine to Machine
MAC	Media Access Control
MC	Mission-Critical
MCC	Mission-Critical Communication
MCIOPS	Mission-Critical over Isolated E-UTRAN operations for Public Safety

MCPTT	Mission-Critical Push-to-Talk
MCS	Mobile Crowd-Sensing
MDM	Mobile Device Management
MEC	Multi-access Edge Computing
MIMO	Multiple Input Multiple Output
ML	Machine Learning
MME	Mobility Management Entity
MNO	Mobile Network Operators
MOCN	Multi Operator Core Network
MORAN	Multi-Operator Radio Access Network
MSS	Mobile Satellite Services
MTC	Machine Type Communication
MU	Multi-User
MU-MIMO	Multi-User MIMO
MVNE	Mobile Virtual Network Enabler
NB	Narrowband
NEXRAD	Next-Generation Radar
NFV	Network Function Virtualization
NGO	Non-Governmental Organization
NIMS	National Incident Management System
NIST	National Institute of Standards and Technology
NOAA	National Oceanic and Atmospheric Administration
NPSTC	National Public Safety Telecommunications Council
NSA	Non-StandAlone
NTN	Non-Terrestrial Network
NetApps	Open source repository for PPDR 5G Network Applications
NetBenefits	Net socioeconomic value
Nprb	Number of Physical Resource Block

Nrb	Number of resource blocks
O-RAN	Open Radio Access Network
OFDM	Orthogonal Frequency-Division Multiplexing
OFDMA	Orthogonal Frequency-Division Multiplexing Access
OPEX	Operational Expenditures
P-25 / APCO-25	Project 25 / Association of Public Safety Communications Officials - Project 25
P-GW	Packet Network Data Gateway
PAS	Publicly Available Specifications
PBCH	Physical Broadcast Channel
PCC	Policy and Charging Control
PCP	Pre-Commercial Procurement
PDSCH	Physical Downlink Shared Channel
PLMN IDs	Public Land Mobile Network Identifiers
PMI	Precoding Matrix Indicator
POC	Proof of concept
PPDR	Public Protection & Disaster Relief
PRACH	Physical Random Access Channel
PS	Public Safety
PS-LTE	LTE-based Public Safety
PS-LTE	Public Safety-LTE
PSAP	Public Security Answering Point
PSMA	Public Safety Mobile Application
PSN	Public Services Network
PSP	Public Safety Platform
PSS	Primary Synchronization Signal
PTT	Push To Talk
PUSCH	Physical Uplink Shared Channel

PWS	Public Warning Systems
ProSe	Proximity Services
QAM	Quadrature Amplitude Modulation
QCI	Quality of Service Class Indicator
QPSK	Quadrature Phase Shift Keying
QoE	Quality of Experience
QoR	Quality of Resilience
QoS	Quality of Service
RA	Random Access
RAN	Radio Access Network
RAT	Radio Access Technologies
RB	Resources Blocks
RFID	Radio-Frequency IDentification
RI	Rank Indicator
RNP	Radio Network Planning
RRC	Radio Resource Control
RS	Reference Signal
RSRP	Reference Signal Received Power
RSRQ	Reference Signal Received Quality
RSSI	Received Signal Strength Indicator
RSU	Road Side Unit
S-GW	Serving Gateway
S-MVNO	Secure Mobile Virtual Network Operator
SA	Stand Alone
SAE-GW	System Architecture Evolution Gateway
SC-FDMA	Single Carrier Frequency Division Multiplex Access
SDG	Sustainable Development Goal
SDN	Software Defined Networking

SDR	Software Defined Radio
SIB	System Information Block
SIDS	Small Island Developing States
SIM	Subscriber Identity Module
SINR	Signal to Interference plus Noise Ratio
SISO	Single-Input Single-Output
SLA	Service Level Agreement
SLR	Systematic Literature Review
SMS	Short Message Service
SOC	Security Operations Center
SON	Self Organizing Network
SRS	Sounding Reference Signal
SS	Synchronization Signals
SSS	Secondary Synchronization Signal
SU	Single User
SUS	System Usability Scale
SpiceNet	Standardized PPDR Interoperable Communication for Europe
TA	Technology Assessment
TBS	Transport Block Size
TCCA	TETRA and Critical Communications Association
TDD	Time Division Duplex
TETRA	Terrestrial Trunked Radio
TETRAPOL	Terrestrial Trunked Radio Police
TIA	Telecommunications Industries Association
TMK	Terminal Master Key
TMO	Trunking Mode Operation
TPS	Terminal Programming Station
TR	Technical Reports

TS	Technical Specification
TVC	Technical Validation Committee
TX	Transmitter
UA-gNBs	UAVs as mobile gNBs
UAV	Unmanned Aerial Vehicle
UE	User Equipment
UHF	Ultra High Frequency
UICDS	Unified Incident Command and Decision Support
UK	United Kingdom
UMTS	Universal Mobile Telecommunications System
USIM	Universal Subscriber Module Identity
V2X	Vehicle to Everything
VHF	Very High Frequency
VPN	Virtual Private Network
VR	Virtual Reality
VoLTE	Voice over LTE
WEA	Wireless Emergency Alerts
e-ICIC	Enhanced Inter-cell interference coordination
eMBB	Enhanced Mobile Broadband
eNodeB / eNB	Evolved Node B
gNodeB / gNB	Next Generation Node B
mMTC	Massive Machine-Type Communication
mcMTC	Mission-Critical Machine-Type Communications
uRLLC	Ultra-reliable Low Latency Communication

1

INTRODUCTION

All cities face problems related to Public Protection & Disaster Relief (PPDR)[1] agencies, such as Public Safety (PS), natural disasters, pandemic situations, among others. Therefore, the search for solutions capable of improving these agencies' performance by enabling better service to the population and providing sustainable social development with better quality of life concern various actors, such as the civil society, PPDR agencies, governments and the scientific community.

Also, the large concentration of people, added to the growing importance of urban centers, present challenges to the cities, urging humanity to rethink the ways of managing cities according to their particularities. In these terms, Information and Communication Technologies (ICT) can be important tools to support the management and decision-making processes of the actors involved.

Technological solutions through ICTs could assist PPDR agencies in solving problems. However, most of PPDR agencies still use communication technologies that are not integrated with information systems and intelligent resources. Even though there are several technological solutions in this area, the agencies currently face the problem of trying to migrate to new communication technologies without knowing the best time or the proper way to start (Ferrús et al., 2013; Freire, 2019; Kumbhar & Güvenç, 2015; TCCA, 2019; TCCA & ACCF, 2020). According to BroadMap (2017, p. 11), the key findings of the current situation and strategies "clearly indicate the need for broadband services over the current narrowband capabilities.

[1] Public protection (PP) institutions are "agencies and organizations dealing with maintenance of law and order, protection of life and property, and emergency situations". Disaster Relief (DR) institutions are "agencies and organizations dealing with a serious disruption of the functioning of society, posing a significant, widespread threat to human life, health, property or the environment, whether caused by accident, nature or human activity, and whether developing suddenly or as a result of complex, long-term processes" (ITU-R, 2003, p. 7).

However, to date, only a few countries have formalized a strategy towards mission-critical broadband services".

According to BroadMap (2017, p. 11), "the solution must be cost-effective, needs to be very adaptive to different national implementations whilst still maintaining the key objectives of cross-agency interoperability and cross-border interoperability, security, availability, system management and open standard compliance".

This research presents a Technology Assessment approach considering potential Smart City scenarios that can enable a Smart City Public Safety Emergency Management process. Through a general framework based on use cases, literature review, Systematic Literature Review (SLR), and data treatment from interviews, this study aims to enable applied case scenarios of Mission-Critical Communication (MCC) systems integrated with the Cyber-Physical System, avoiding "one size fits all" solutions for Smart City strategies. Such scenarios can help the PPDR agencies' decision-making process through the digital transformation of MCC into an integrated emergency system.

According to Grunwald (2009), the Technology Assessment (TA) approach is characterized by the combination of knowledge generation, as conditions for technology implementation; evaluation of this knowledge centered on society; and formulation of recommendations for decision-makers (government) and society. This involves challenges such as incorporating existing knowledge about the side effects early in decision-making processes, facilitating the valuation and impact assessment of technologies. This way, the construction of scenarios is part of TA, which intends to maximize the positive effects of the implementation of a given process or technology while neutralizing the negative ones, strengthening democracy and institutions by increasing transparency and scientificity in the decision-making process of technological decisions that affects the society.

The agents that act in emergency situations, such as police, firefighters, rescue squads and emergency medical personnel, are called Emergency First Responders (EFR). The EFRs are the first actors in crisis situations, working in the area called Public Protection & Disaster Relief (PPDR). During their work, agents use communications equipment such as mobile phones or handheld radios, assisted by dispatch centers that collect information and coordinate the response to incidents.

Radiocommunication networks are one of the main support tools used by PPDR agencies, which is why they are regarded as Mission-Critical Communication. There are specific international protocols for these technologies. According to the GSM Association[2] (GSMA, 2018, p. 6), Critical Communications (CC) are used in situations "where human life and other values for society are at risk and where timely and reliable communications between First

[2] Industry organization that represents the interests of mobile network operators worldwide, with more than 750 mobile operators and 400 companies as GSMA members (GSMA, 2018).

Responders is essential to avoid or at least mitigate damage". Even though CC is applicable to many other sectors of society and industries, the term Mission-Critical Communication (MCC) is used to refer to the communication between EFRs working at PPDR agencies, who also use terms such as Mission-Critical Voice and Mission-Critical Services (Lair & Mayer, 2017; Yy et al., 2018). MCC systems are used to coordinate teams and provide quick emergency response; therefore, they need to be resilient, ultra-reliable and secure. The systems used in disasters (e.g., a tsunami warning system), called Public Warning Systems (PWS), also share these characteristics (Zhou et al., 2021).

MCC systems are technologies globally used by public agencies in the PPDR field. Most PPDR networks still use Land Mobile Radio (LMR), a digital system based on trunked radio technology[3], conceived for priority use of voice with very limited capabilities for data applications, providing an average bandwidth of 12.5 kHz, which allows the transmission of text messages only. Currently, three sets of LMR MCC standards have become predominant, namely APCO-25[4], TETRA[5] and TETRAPOL[6] (Baldini et al., 2014; Freire, 2019). The LMR systems used nowadays do not have enough bandwidth to enable the use of intelligent resources. These devices are not standardized enough to allow technology integration without adding new devices to function as a gateway between networks; even with these gateways, services cannot be fully shared, which means that PPDR agencies using different LMR standards are not able to communicate with each other. However, given the technological evolution of today's society, it is necessary to modernize these systems, thus enabling a more efficient performance of PPDR agencies based on data analysis and systems integration.

With the intention of developing MCC for broadband, allowing system integration and high data traffic, the TETRA and Critical Communications Association (TCCA), an association representing all MCC standards in LMR, indicated LTE (4G) as the preferred broadband technology for MCC (Doumi et al., 2013; Freire, 2019). Long Term Evolution (LTE) uses standardization defined by 3GPP, a collaborative project between seven telecommunications standard development organizations that provides Technical Specifications (TS) and Technical Reports (TR) for mobile networks (3GPP, 2018).

Through broadband communication, the technological capabilities are expected to be transformed — e.g., PPDR agencies accessing data in real time and modifying the way the police acts and investigates; firefighters receiving real-time information from fire sites through drones providing images over a 5G network; medical emergency services receiving help from hospital doctors by using augmented reality; remotely controlled machines for the most

[3] Technology that involves two-way radio, allowing the sharing of a few radio frequency bands between a large number of users.
[4] APCO-25 has standards defined by the Telecommunications Industry Association (TIA, 2002).
[5] TETRA has standards defined by the European Telecommunications Standards Institute (ETSI, 2020).
[6] TETRAPOL has standards defined by the TETRAPOL Forum (2022).

diverse purposes. Security, control, network availability, costs, management, and regulatory affairs are the main concerns (Freire, 2019; Freire & Cândido, 2020).

Also, the evolution of 4G, the 5G network, is ready to improve PS networks. As highlighted by Chen Cui et al. (2022, p. 427), "legacy public safety networks require modernization to improve the safety, situational awareness and operational effectiveness for first responders and the application of 5G technology can solve this problem well".

Nevertheless, the 3GGP sets the technological standard, but does not set a standard for the digital transition. Since PPDR agencies already have their own LMR communication system in narrowband, vendors and experts understand that some models are viable for this transition, but it is up to the PPDR agencies to determine the best solution for each situation. Due to the lack of information on how each agency should make the digital transition of the MCC, and given each city's particularities, a Technology Assessment (TA) is necessary, focused on the applied cases to avoid a "one size fits all" solution.

According to Coates (2016, p. 107), TA is defined as "a policy study designed to better understand the consequences across society of the extension of the existing technology or the introduction of a new technology, with emphasis on the effects that would normally be unplanned and unanticipated". With components as "Examine problem statements", "specify system alternatives", "identify parties at interest", and "draw conclusions and recommendations" are some of the components of TA. In that sense, TA is about decision-making for technologies that should impact the society, intending to anticipate risks, better allocate resources, and avoid negative consequences in society. On the other hand, Constructive Technology Assessment (CTA) approach intends to align expectations of a broad range of stakeholders, involving them in the design process of the use of the technology to better suit the society needs (Versteeg et al., 2017). With the aim of creating the broadest possible positive impact on society this research will also make use of CTA.

The literature review showed that several cities already use broadband communication solutions integrated with information technology, e.g., using information technology through mobile and web applications, collecting data from citizens in crowd-sensing / social sensing, and combining Internet of Things (IoT) devices with database information, to help the cities to reduce crime rates and act more effectively in emergency situations.

Combining those sources of information with the traditional government monitoring system will provide basis for designing an early warning and information system — an information platform that allows the transmission of warning messages to authorities, and even dealing with incidents before they occur to prevent emergencies from occurring, driven by different goals to assure the overall safety of the city and citizens (Cui, 2015; Wu & Yu, 2020; Atat et al., 2018).

The "Smart City Public Safety Emergency Management"[7] (Wang & Li, 2021, p. 169) should make full use of Internet, IoT, Cloud Computing, and system integration in a Smart City scenario, allowing the emergency management system to play a positive role in urban safety governance. The integration of various technological resources could prevent the lack of emergency forward-looking information and weak decision-making support, in order to improve the accuracy of urban smart emergency systems and the level of emergency management from the government (Wei & Sheng, 2019).

However, the technological integration leads to debate regarding data protection and privacy. The use of broadband networks with system integration by PPDR agencies in Smart City scenarios allows accessing various information from different agencies, such as electricity, gas, police, traffic agencies, and from different sources, such as crowdsourcing and IoT devices, also combined with artificial intelligence (AI). Without proper regulation, such use can bring negative consequences to society in terms of privacy and government control over citizens.

In addition, one of the main concerns about using crowd-sourced information combined with artificial intelligence is the algorithmic bias in predictive policing models. Predictive policing is defined as "the application of analytical techniques – particularly quantitative techniques – to identify likely targets for police intervention and prevent crime or solve past crimes by making statistical predictions" (Perry et al., 2013, p. 16). Police departments are increasingly utilizing software to identify future offenders and forecast criminal activity and future crime. This leads to concerns regarding police-recorded data sets being rife with systematic bias targeting specific groups, as discussed by Lum and Isaac (2016).

As the ICT sector experiences significant growth in development and solutions, it is expected to come up with several technological solutions intending to improve the PPDR services. Nevertheless, there should be further analysis on how the agencies perform the digital transition in each applied case, and its consequences to society.

Also, published studies and specialists state that LTE for MCC is intended to complement the services currently offered by narrowband networks, not to replace legacy systems, as LMR will continue to be the MCC standard during the following years. Some projections estimate it may take only a few years, while others estimate the full replacement may take 10 to 15 years to occur (Baldini et al., 2014; Freire, 2019; Ferrús et al., 2013; TCCA, 2019; TCCA & ACCF, 2020; Kumbhar & Güvenç, 2015; BroadMap, 2017).

As many countries still don't have Smart City Emergency management or any particular solution implemented for broadband MCC, the construction of scenarios can help PPDR

[7] It can be inferred, from the literature review, that Smart City Public Safety Emergency management refers to systems used in Smart City for both applications, emergencies such as disasters, and for Public Security, also referred by Smart City.

agencies in the technological decision-making process of the digital transformation of MCC considering Smart City options, without increasing the risks of massive disruptions in society.

1.1 Objectives

This research aims to achieve a general objective and specific objectives.

1.1.1 General objective

To construct scenarios to help PPDR agencies in the decision-making process of the digital transformation of MCC considering Smart City scenarios.

1.1.2 Specific objectives

1. To gather knowledge about the concept of Smart City Public Safety Emergency Management.
2. To design an Innovation Ecosystem for Smart City Public Safety Emergency Management, focusing on understanding the role of MCC and considering a Constructive Technology Assessment approach.
3. To construct a general MCC scenario considering Smart City Public Safety Emergency Management, based on the interviews, literature review and SLR.
4. To point out existing and/or potential technological paths for applied case scenarios to help in the decision-making process.
5. To list a set of recommendations for the application of scenarios, considering the principles of Constructive Technology Assessment.

1.2 Research questions

- Why should MCC consider Smart City environments and how could that be described?
- What are the scenarios for the digital transformation of Mission-Critical Communication considering Smart City options?
- What is a Smart City Public Safety Emergency Management?

2

LITERATURE REVIEW

This chapter presents some concepts covered by this thesis in the fields of Mobile Communication and Information Technology used by PPDR agencies. It also presents concepts related to the societies in which PPDR agencies are included, which are affected by the use of technology.

2.1 Mobile communication

There are two distinct technology families that provide wireless communications over a wide coverage area: dedicated communication systems for PS and disaster relief, which are provided by Public Protection & Disaster Relief (PPDR) agencies and have Emergency First Responders (EFRs) as users; and commercial cellular networks, which are provided by Mobile Network Operators (MNO)s and have private and commercial consumers as users (Sharp, 2018).

While PPDR agencies have used communication systems since the invention of the Wireless Telegraph, the development of wireless communications through cellular mobile telephony began to emerge in 1978, specifically for commercial use, without meeting the requirements for critical communications, as will be presented in later topics. Cellular systems such as GSM (2G) and UMTS (3G) have not been designed for PS purposes and requirements, "as they lack the level of reliability, availability, responsiveness and security requested by Public Safety organizations" (Baldini et al., 2014, p. 629). Furthermore, the first generation of networks had low spectral efficiency and low data rate.

It was only with the rise of LTE (4G), which began to be implemented in 2005 and was popularized due to lower implementation costs in the 2010s, that high data rates though broadband networks became possible, enabling the integration of resources and the use of massive data applications. After 4G it would make sense to consider using these technologies for MCC, due to their technological capabilities and to the fact that 4G networks started to meet MCC criteria after Release 12, as will be discussed further.

The technological evolution of commercial networks currently makes it possible to combine those two previously distinct technological families, with the possibility of using various scenarios, including integration with information systems, and considering different aspects, as shown in Figure 1. The multiplicity of scenarios and use cases justifies carrying out a Technology Assessment to consider the different aspects involved in the application of technology.

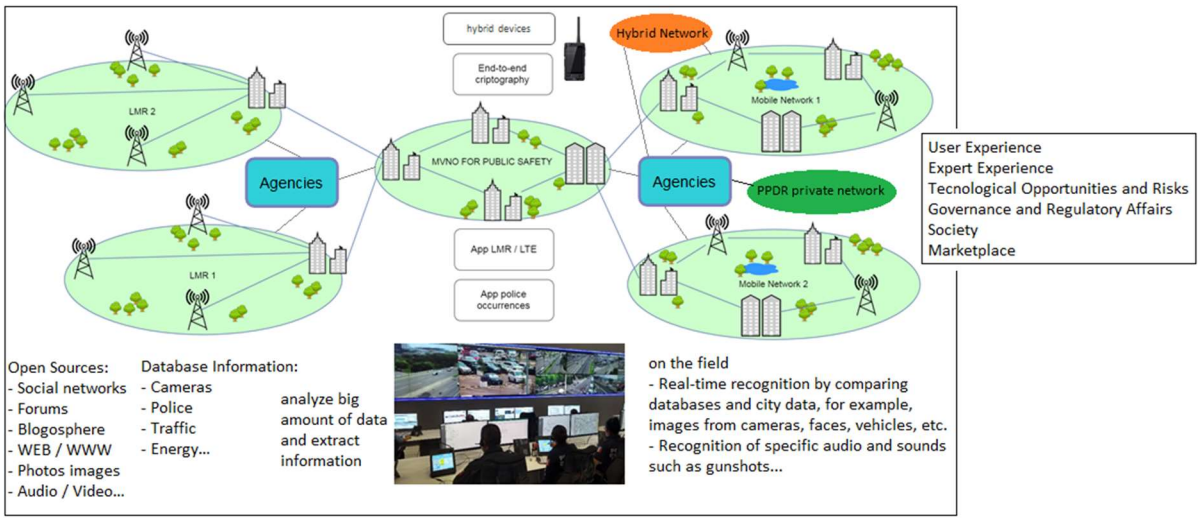


Figure 1 - Possible scenarios (Author).

2.2 Mobile communication technologies for MCC

The technologies used for MCC went through several stages. When the first technologies emerged, the armed forces created specific battalions to test and manage communication systems, such as the United States (US) Army Signal Corps, created in 1860 within the US Army (Raines, 2005); the Arme de Transmissions, created in 1942 in the French land army (Ministère des Armée, 2022); the Portuguese Army Transmission Weapon, created in 1970; and the Royal Corps of Signals, created in the United Kingdom (UK) in 1920 (Royal Corps of Signals, 2020). Most of these forces were born from telegraphic corps, e.g., the Portuguese case, where the Transmission Weapon was originated in the Military Telegraphic Corps, created in 1810 (Regimento de Transmissões do Exército Português, 2021).

Radiocommunications emerged at the end of the 19th century when telephone and telegraphic networks had already reached several parts of the globe. However, it was during World War I that its importance was consolidated, with states investing in wireless communications "oriented towards imperatives of order strategic and defensive, with a view to strengthening military networks and creating alternatives in the event of sabotage of submarine cable networks" (Queiroz, 2015, p. 12).

The discovery of the thermionic triode and its applications led to a great evolution and diversification of equipment from the 1920s on. When World War II took place, from 1939 to 1945, the world already had several shortwave systems installed for civil and military purposes, as well as radio broadcasts such as the British Broadcasting Corporation (BBC), founded in 1922. Radiocommunication equipment installed on ships and airplanes and portable radios used by soldiers were technological war weapons.

The Very High Frequency (VHF) communications were extensively developed during World War II. In the post-war period, the research addressed a potential market for commercial applications and for PPDR agencies, motivated by factors such as simplicity of operation, reduced equipment size, operation in extreme temperatures, reliability, and channel separation ensuring privacy in the communication.

The Detroit Police Department, in the US, was the first to use radiocommunication systems operating in vehicles in 1917. They also activated the first Base Station (BS), named KOP, in 1921. The KOP was licensed by the Federal Radio Commission, predecessor of the Federal Communications Commission, as an entertainment station, with no dedicated frequency. Therefore, police communications could be heard among the songs of other stations. It was only in 1928 that the police started to use a dedicated frequency (IEEE, 2018).

When the first radiocommunication systems were installed in US police, in the 1920s and 1930s, the US were experiencing a crime wave brought on by the Prohibition (a law that banned the manufacture, sale and transport of alcoholic beverages) and the Great Depression. During the unprecedented financial crisis of the Great Depression, not only did the gangsters commit crimes, but also the countless unemployed; several people began to manufacture and sell alcohol illegally, and bank robberies multiplied at the time.

Many of these criminals managed to escape because the police did not have communication systems to notify the officers; even when police officers were informed about the robbery, they could not reach the vehicles nearby the occurrence place. This started to change in 1928, when the first one-way radio was installed in a Detroit police vehicle. In 1933, the first two-way radio was installed in a Bayonne police vehicle — a disruptive innovation that changed the way the police worked with the technological response against crime. In 1940, when the system was improved with bidirectional Frequency Modulation (FM), installed in the Connecticut police, there was a significant improvement in the quality of service, i.e., the voice became more intelligible, and the system received less interference.

The communications used by PPDR agencies were continually developing, using Very High Frequency (VHF) and Ultra High Frequency (UHF) bands, first through analog systems and later moving on to digital systems. Nowadays, radiocommunication networks are one of the main tools for PPDR agencies, with international protocols for these technologies. The system currently used is the Land Mobile Radio (LMR), which was conceived for priority use of voice, with very limited capabilities for data applications, and provides an average bandwidth of 12.5

kHz, which allows sending text messages only. Currently there are three LMR MCC standards, namely: APCO-25, TETRA, and TETRAPOL.

The digital radiocommunication brought advantages such as quality of service; lower susceptibility to interference and noise, which provides intelligibility in communication; low latency, with communication occurring quickly, which is an essential attribute for MCC since a few seconds delay in receiving information can be fatal to the agent; reliability, through the use of secure systems with robust cryptographic keys; availability, since the system belongs to the police and the organization can choose the location to implement the base stations according to their operational needs; and systems with different modes of operation, which allow tactical and operational adaptation. Also, the LMR digital systems aim to reach certain objectives and requirements, such as "interoperability, reliability, functionality, security in operation and fast call set-up[8] in each area of operation" (ITU-R, 2003, p. 1), to provide effective communications to the PPDR agencies.

The different LMR operating modes, shown in Figure 2, are:

1. Fixed mode or Trunking Mode Operation (TMO) — through Base Stations (BS)s installed and distributed according to coverage objectives, connected to regional centers called control nodes;
2. Tactical Network — through portable transmitters, the tactical stations have the same power as a BS and can be connected to the regional centers via internet;
3. Direct mode — without the need of coverage from a BS or tactical station, the Direct Mode Operation (DMO) allows users to communicate direct from a handheld terminal (HT) to another HT.

[8] Fast call set-up indicates reducing the response time to access the network (ITU-R, 2003, p. 1).

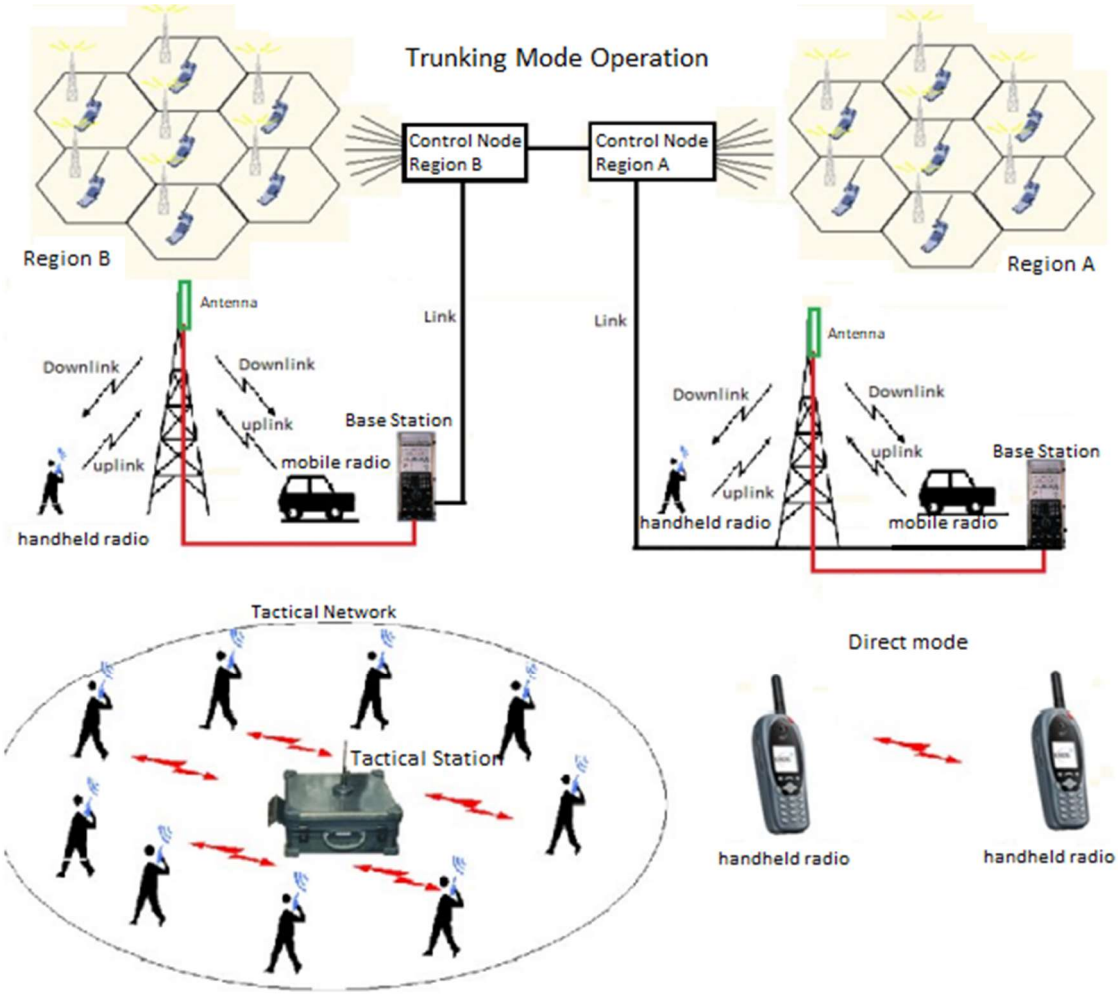


Figure 2 - LMR network operating modes, adapted from Freire (2019).

The use of LMR systems, in addition to technological innovation, was also a process innovation, using communication groups managed from a dispatch center. The LMR network is managed by agents specialized in information and communications technology, creating communication groups, inserting users into communication groups, managing servers for local and national networks, configuring the radios' cryptographic keys locally, installing tactical stations at operation sites, among other network management activities.

The PPDR agencies have control of the LMR network infrastructures and management. This solved problems that were quite evident since World War I, when infrastructure and technology management were under control of private companies whose services were contracted by the government. For example, in the UK, during the World War I, the Marconi Company was hired by the Post Office for a fifth of pence per word processed, which resulted in a dispute in court for the government to settle the debt (Baker, 1971).

LMR systems are open technologies, which means the specifications are made available by the associations responsible for the standards, allowing manufacturers to develop products and solutions based on the Publicly Available Specifications (PAS). The associations are

TETRAPOL Forum (2022) for TETRAPOL; European Telecommunications Standards Institute (ETSI, 2020) for TETRA; and Telecommunications Industry Association (TIA, 2002) for APCO-25 (known also as P25). The TETRA and Critical Communications Association (TCCA) emerged later, as an organization of members representing all MCC standards, seeking to standardize and develop joint solutions. TCCA is currently the main organization in the MCC area, and it works in collaboration with other institutions, including 3GPP. LMR systems are globally used for PPDR networks, being present in more than 130 countries (Jarwan et al., 2019).

LMR technologies are open for development; however, the interfaces are not open enough to enable different manufacturers in the various interfaces. In that sense, PPDR agencies were implementing the systems using a single manufacturer. While APCO-25 was preferred in the US, TETRA was the preference in Europe. As an exception, France adopted TETRAPOL, largely due to MATRA Communications Company, the first manufacturer to develop equipment in this system. MATRA was headquartered in France, and became part of the Airbus Group, also headquartered in France. In most countries, the prevalence of TETRA is observed, resulting in a greater diversity of manufacturers for this technology.

According to Mehmet Ulema (2019), TETRA became widely used in the world; TCCA estimates there are more than 250 networks deployed in more than 120 countries. According to BroadMap (2017), in Europe there are 27 legacy PPDR networks, 22 of which are TETRA, four are TETRAPOL and one is P25. Also, some countries have more than one PPDR network, e.g., Latvia, Spain and France.

According to Gianmarco Baldini et al. (2014, p. 638), "the fragmentation of public safety wireless communication systems can create problems of interoperability, which can negatively impact the resolution of natural disasters or emergency crisis". Nowadays, if a PPDR agency uses TETRAPOL, for example, it cannot communicate with another agency that uses APCO-25, unless they use some equipment to integrate voice communication; however, interoperability of resources is not possible. That results in the fragmentation of MCC networks in many countries, such as Brazil, where more than US$600 million were invested in more than 30 LMR networks for MCC, which are used by different agencies, in many cases with overlapping network coverage, and most of them without system integration (Freire, 2019).

Due to the lack of technological resources such as capacity and interoperability, EFRs have faced several problems in emergency situations where the agencies were operating with LMR technologies. During the attack to the World Trade Center, on September 11, 2001, the United States of America (USA) faced several communication and information problems, such as lack of coverage of MCC systems, agencies using different MCC systems without interoperability, and lack of sharing information between agencies. However, most of the problems that occurred in that day were due to the lack of procedures and preparedness. Without these factors, the technologies' results are limited, as reported by the commission

created to investigate the events (The National Commission on Terrorist Attacks Upon the United States [9-11 Commission], 2004).

In disaster situations, the communication efficiency and provision of quality information from the emergency site to the EFRs help to ensure the success of the operation. Also, communication failures can worsen the crisis. In the case of the fire that occurred in Pedrógão Grande, Portugal, on June 17, 2017, the report of the Center for Studies on Forest Fires of the University of Coimbra stated that "the failure of the communication system had contributed to the lack of coordination on fire combat and rescue services, to the difficulty in requesting help by the population, and to the worsening of the fire consequences" (CTI, 2017, p. 225).

The 9/11 Commission Report recommended several actions to mitigate the problems and improve countermeasures. Figure 3 highlights two recommendations related to the matters discussed (9-11 Commission, 2004, p. 397):

Recommendation: Emergency response agencies nationwide should adopt the Incident Command System (ICS). When multiple agencies or multiple jurisdictions are involved, they should adopt a unified command. Both are proven frameworks for emergency response. We strongly support the decision that federal homeland security funding will be contingent, as of October 1, 2004, upon the adoption and regular use of ICS and unified command procedures. In the future, the Department of Homeland Security should consider making funding contingent on aggressive and realistic training in accordance with ICS and unified command procedures.
Recommendation: Congress should support pending legislation which provides for the expedited and increased assignment of radio spectrum for public safety purposes. Furthermore, high-risk urban areas such as New York City and Washington, D.C., should establish signal corps units to ensure communications connectivity between and among civilian authorities, local first responders, and the National Guard. Federal funding of such units should be given high priority by Congress.

Figure 3 - Recommendations made by the 9/11 Commission Report.

After 9/11, several actions were taken by the United States (US) Government to meet the recommendations suggested by The National Commission on Terrorist Attacks Upon the United States (9-11 Commission, 2004), intending to avoid the problems that occurred on that day. Due to the experience of 9/11, the US Congress demanded that the interoperability requirements were the first to be developed towards the LTE network for MCC. This way, a working group composed by industry members, service providers, and security and defense organizations, all appointed by the Federal Communications Commission (FCC), studied critical aspects of interoperability, such as network interfaces, security, applications, devices, handovers, roaming, service design, and prioritization (Doumi et al., 2013).

In 2012, the TCCA and the National Public Safety Telecommunications Council (NPSTC) signed a memorandum of agreement expressing the need to develop LTE for MCC (Doumi et al., 2013). In February 2012, the US Congress approved legislation that led to the creation of the First Responder Network Authority (FirstNet), for the deployment and operation of a nationwide LTE-based MCC network (Baldini et al., 2014). In 2013, the USA allocated a bandwidth of 20 MHz in the 700 MHz band, for the development of the national broadband MCC network — an action that would not have been possible without the joint action of regulatory agencies, legislators, manufacturers, and PPDR and defense organizations. The development intended to allow MCC networks to have capacity similar to commercial networks and achieve interoperability of communications between agencies (Doumi et al., 2013).

This effort resulted in the construction of the FirstNet, a national LTE-based MCC network integrated with existing LMR networks. The FirstNet was the first MCC initiative in the USA involving commercial cellular systems, providing "a scalable, robust, reliable broadband communication system for first responders, and has gradually been formed into a standard for the USA and the rest of North America" (Zahid et al., 2019, p. 619). FirstNet actually assist in the communication and interoperability between various EFR organizations. The initiative to modernize MCC networks has been followed by other countries with other implementation models, according to the available financial resources and local needs.

Figure 4 and Figure 5, from FirstNet (2018), exemplify the idea of what is technologically expected for an EFR using broadband networks, and what is expected regarding data integration in a smart community, receiving data from connected devices, from the Internet of Things (IoT) to new concepts such as Internet of First Responder Things (IoFRT) and Internet of Public Safety Things (IoPST). IoFRT refers to wearables for EFRs, while IoPST are IoT devices used for PS purposes, such as sensors.

Figure 4 - First Responders of the future (FirstNet, 2018).

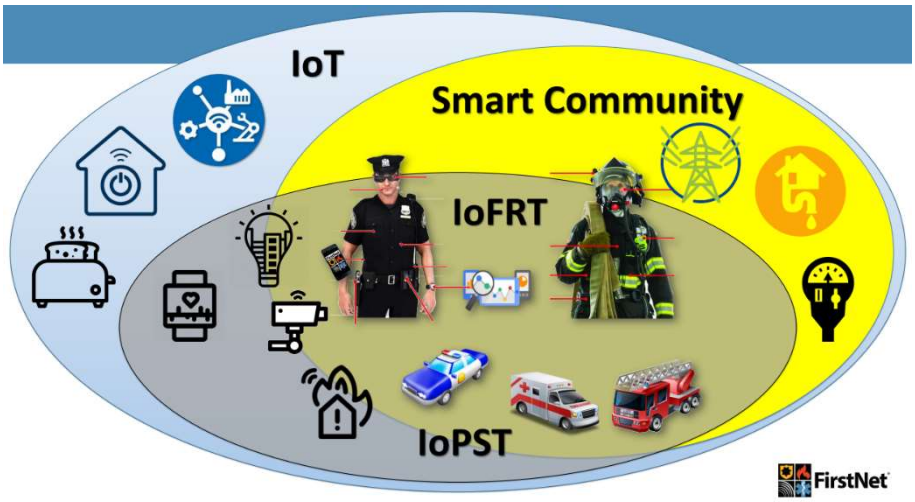


Figure 5 - First Responders Ecosystem of the Future (FirstNet, 2018).

For the development of MCC in 4G, it was essential the participation of the 3rd Generation Partnership Project (3GPP), since the 3GPP develops the telecommunications standards adopted globally for mobile communication networks. In 2013, the cooperation between 3GPP and TCCA began, with TCCA providing technical requirements and inputs while the industry and 3GPP provided LTE enhancements to meet MCC requirements.

3GPP improved the LTE standard for MCC through 3GPP Release 11, RP-120362, which allows high-power MCC User Equipment (UE) for band 14 region 2 (EUA); and 3GPP Release 12, SP-120883 for Proximity Services (ProSe), which allows Device to Device (D2D) communication between UE, and SP-120876 for Group Communication System Enabler (GCSE), enabling the creation of communication groups managed by a dispatch center (Sharp, 2018).

The PS interest in ProSe is allowing communication in areas with no network coverage. In this situation, it is also interesting that UE can emit higher power then a usual handset, allowing for greater reach of direct communication. The group call enablers' objectives provided efficient group communication in dynamic groups with mobile users and dispatchers, support for floor control, e.g., Push-to-Talk (PTT) mode, communication groups with a large number of users, and low latency to add users and obtain channels.

The 3GPP Release 13 also brought the standardization of Mission-Critical Push-to-Talk (MCPTT), allowing the use of the UE through the PTT button, as used in handheld radios with trunking system, in which, as long as the channel is available, just pressing a button establishes the communication. That could be done by physical buttons on the side of mobile phones, or through an application that simulated this button on the screen. Release 13 also brought the Mission-Critical over Isolated E-UTRAN Operations for Public Safety (MCIOPS) functionality, which translates into the tactical network used by the LMR.

The subsequent releases made improvements to the services, offering modes in LTE that were already available in LMR and including new services that were not available in LMR networks, such as Mission-Critical (MC) Data and Mission-Critical Video. In addition, the

standardization of 5G for MCC will bring the possibility of offering new services, such as Non-Terrestrial Network (NTN), allowing satellites to be used as BSs (named eNodeB in 4G and gNodeB in 5G). Nowadays, in isolated areas such as the Amazon rainforest, PPDR agencies face communications problems using LMR networks, while satellite phones have a high cost. This type of solution can improve communication in places where it is difficult to install and operate Mission-Critical radiocommunication systems.

Figure 6 shows the regulatory frameworks for standardization, based on Chitturi (2021), Jaffar and Chuberre (2021), Lair and Mayer (2017), Nokia (2022) and 3GPP.

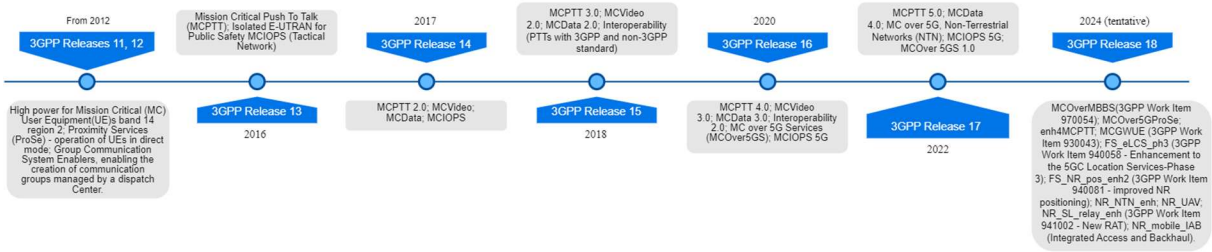


Figure 6 - 3GPP roadmap for MCC (Author).

In Europe, the MCC evolution is also leading for 3GPP networks. According to BroadMap (2017, p. 26), "analysis of requirements and specifications has shown that the technology for a European PPDR communication solution is best based on 3GPP Release 15, which includes Mission-Critical standards and which has been labelled 5G by 3GPP. This encompasses 4G LTE technology and opens for use of new 5G radio solutions".

In addition to the advantages of using broadband networks, networks standardized by 3GPP have solutions developed together with various actors, such as industries, companies, and research centers, enabling open interfaces. That opening can bring benefits due to the diversity of equipment manufactures and solution providers. Also, with MCC operating in 4G and 5G networks, it is possible to bring to the MCC ecosystem actors that had previously developed solutions for commercial mobile networks only.

According to Baldini et al. (2014), PS organizations have a high cost per subscriber in the dedicated network, due to the small number of subscribers in comparison to the cost of the network. With the evolution of commercial networks, the implementation and operational costs can be reduced while providing high data rates. With those benefits, the use of MNOs became an option to reduce the cost per subscriber, due to the diversity of actors and offers.

The Open Radio Access Network (O-RAN) initiative is one of the initiatives in 5G aimed at open interfaces. Based on the concept of interoperability and standardization of the Radio Access Network (RAN) elements, the O-RAN includes a unified interconnection standard for hardware, and open source software elements from different vendors. The disaggregation of interfaces is essential for 5G deployment and evolution, allowing the MNOs to open the RAN and to leverage multivendor solutions (O-RAN Alliance, 2022).

Although the 3GGP sets the technological standard, it does not set a standard for the digital transition. Through literature review, some models were considered viable, namely:

1. Dedicated solution: broadband networks for PPDR agencies; specific spectrum is needed.
2. Hybrid solution: most network resources are under control of agencies, sharing RAN resources with MNOs; PPDR agencies also build some RAN if necessary. Possibility of implementing infrastructure sharing as Multi Operator Core Network (MOCN) or Multi Operator RAN (MORAN). MORAN is a solution with base station sharing, MOCN is a solution with spectrum sharing, as shown in Figure 7. Possibility of implementing PPDR core or shared core, Gateway Core Network sharing (GWCN).
3. Secure Mobile Virtual Network Operator (S-MVNO): control and security of the user base and applications, RAN of MNOs, possibility of coverage of multiple MNOs; possibility of implementing MOCN or MORAN.
4. Through MNOs: agencies use operator networks; coverage may not be tied to one MNO if legislation allows national roaming for PPDR; priority and preemption for First Responders over regular users depends on country regulatory issues. Technically, LTE user prioritization can occur through priority levels, preemption capability and preemption vulnerability, Allocation and Retention Priority (ARP). Although, some countries' regulations don't allow differentiation between users (everyone must have the same priority to access mobile network services).

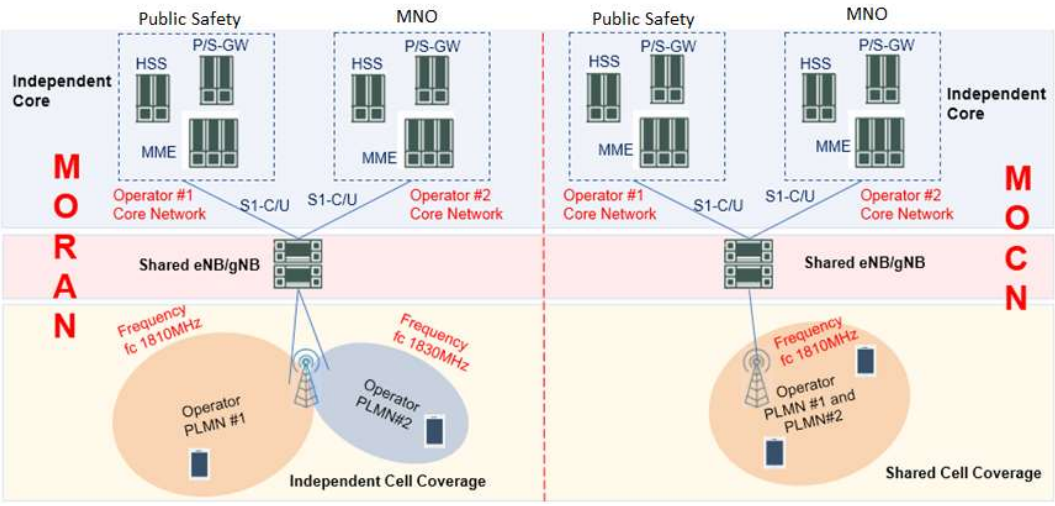


Figure 7 - MORAN vs MOCN, adapted from Techplayon (2019).

Due to the limited frequency spectrum available and to the costs of dedicated networks, since there are MNOs that could provide coverage with the PPDR agencies having a dedicated core, some countries have adopted a mixed model, with their own eNodeBs, partnerships with

MNOs, and connected to LMR networks. When PPDR agencies have dedicated network, security is not a big issue. However, when MNOs are used, a point of vulnerability is created.

Access to the LTE network is controlled through the registration management, security keys and user service profiles, administered through the Universal Subscriber Module Identity (USIM) on the terminal side, and by Home Subscriber Server (HSS) from the network side. Mixed solutions could have PPDR users implementing their own HSS, controlling their own SIM cards, and having network identifiers. Public Land Mobile Network Identifiers (PLMN IDs) through a Public Services Network (PSN) also use shared LTE commercial networks, or Mobile Virtual Network Operators (MVNO)s with their own PLMN ID. In case of MVNOs or shared use of MNOs, the network capacity depends on the MNOs and roaming agreements are necessary (Freire, 2019; Ferrús et al., 2013).

Regarding integration between LMR and 3GPP technologies, this could be done through IP gateways, which can be performed by unencrypted audio interface transformed into Voice over internet Protocol (VoiP). In that case, LMR encryption is lost, and the communication security will be performed by the 3GPP network. This represents an operational change for PS agencies, since nowadays the organizations can use and manage their own encryption keys.

The main MCC equipment vendors are selling proprietary applications for LTE User Equipment and hybrid UE (LTE and LMR), allowing the connection of communication groups between LMR and LTE, in addition to functionality between LTE UE. The application allows the use of commercial LTE networks integrated with LMR networks, without the need of a proprietary LTE network or dedicated MVNO for MCC to be implemented, but also enabling its subsequent implementation. Control of the communication group is performed by PS agencies from a dispatch center (Freire, 2019). Regarding UE, the hybrid UE allows MCC users to continue communicating through the LMR network even in case of LTE networks problems, such as congestion due to high traffic during a big event or a disaster.

Regarding the roadmap for MCC broadband services transition, some countries already started this transition, as EUA and UK (for more details see section 4.3.10). Other countries, like Portugal, intend to continue using LMR systems and waiting for the maturity of other technologies, according to SIRESP, S.A. (2023). Figure 8 shows the transition of services in Europe, according to the BroadMap project, which also highlights that "after the transition period, the 3GPP Mission-Critical PPDR broadband system will be the one and only solution" (BroadMap, 2017, p. 55).

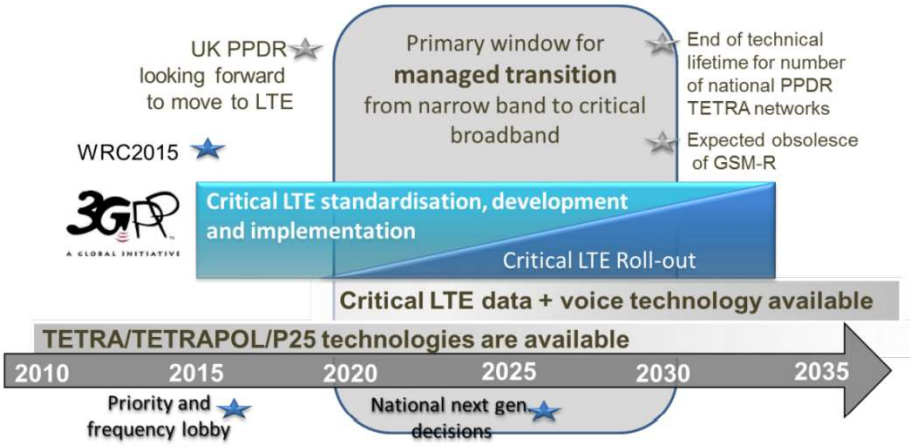


Figure 8 - Roadmap for PPDR MC broadband services transition (BroadMap, 2017, p. 55).

2.2.1 Some technical aspects of LTE and 5G

For years the voice calls dominated traffic on telecommunications networks, but in recent years the scenario has changed radically. While the demand for voice calls has remained stable, data traffic has grown exponentially (Ferreira, 2015). In that sense, new technologies were developed to allow better data rates.

2.2.1.1 4G Networks

LTE was designed to provide high data rates from IP connectivity, with low latency and high spectral efficiency rates. It can be used by applications with IP communication, allowing the operation of multiple services, such as database consultation, video streaming, and voice communication in real time. The LTE network consists of two main parts: the radio access network, known as the Evolved UMTS Terrestrial Radio Access Network (E-UTRAN), and the Evolved Packet Core (EPC). E-UTRAN is primarily responsible for radio transmission functions, while mobility management functions are performed by the EPC. The E-UTRAN consists of base stations called evolved NodeBs (eNBs), responsible for radio protocols.

The EPC comprises the Mobility Management Entity (MME), responsible for control functions such as location management; the Serving Gateway (S-GW), which anchors user traffic to/from the E-UTRAN; and the PDN Gateway (P-GW), which provides IP connectivity to external IP networks. The operation of the EPC is assisted by the Home Subscriber Server (HSS), which is a database that contains, among other things, information related to users. The Policy and Charging Control (PCC) provides operators with advanced tools for Quality of Service (QoS) and control. IP-based service control platforms such as IP Multimedia Subsystem (IMS) can additionally be used for LTE connectivity service with QoS support for multimedia. LTE IP connectivity is accomplished through the establishment of the Evolved Packet System (EPS) between the UE and the P-GW, through the QoS control, as shown in Figure 9.

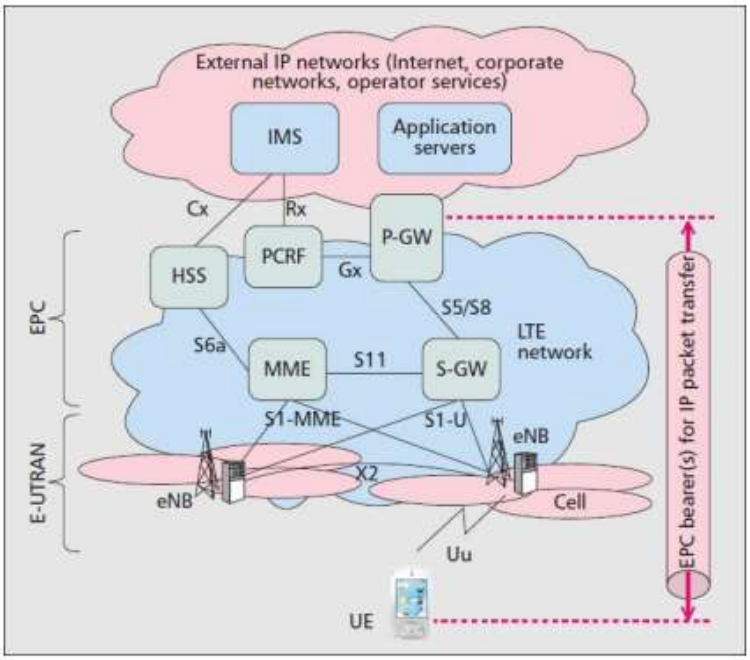


Figure 9 - Basic architecture of LTE, extract from Ferrús et al. (2013).

The carrier[9] frequency is specified by the E-UTRA Absolute Radio-Frequency Channel Number (EARFCN). The EARFCN can be a pair of codes designated for the transmission and reception of the carrier, that is, one EARFCN for the uplink and one for the downlink. The EARFCN also reflects the center frequency of the carrier and is within the range of 0 to 65535 (ETSI 3GPP, 2011).

On a physical level, LTE can operate both in Frequency Division Duplex (FDD) and Time Division Duplex (TDD). In FDD, the downlink and uplink occupy two distinct frequency bands; therefore, it is possible to transmit simultaneously on both links. In TDD, both links are transmitted on the same band, separated by the allocation of different time slots. Concerning frequency band, LTE can operate in different frequencies (800, 1800 and 2600 MHz) and bandwidths (5, 10, 15, 20 Mhz). The frequency and bandwidth will depend on the country's regulation, on what the mobile operator or agency is authorized to explore, and on what they decide as strategy.

To achieve high spectral efficiency rates, the LTE uses Orthogonal Frequency-Division Multiplexing Access (OFDMA) for the downlink, and Single Carrier Frequency-Division Multiplexing Access (SC-FDMA) for the uplink. SC-FDMA resembles OFDMA but has a lower peak power, which ensures longer battery life for the mobile device. LTE has frequency reuse equal to 1, i.e., all cells use all available bandwidth for transmission. Intracellular interference, which is the interference caused between sectors of the same station, is avoided due to the use of OFDMA (Top Optimized Technologies, 2018).

[9] The modulated waveform conveying the E-UTRAN physical channels (ETSI 3rd Generation Partnership Project (3GPP), 2011).

Intercellular interference is produced between neighboring cells with coverage areas meeting at some point. It is avoided with inter-cell interference coordination strategies. Interference is also a function of the user load, and the interference margin varies directly with the station load — more load, more interference (Basit, 2009).

In LTE, the channel is divided into frames and subframes. Frames are 10 milliseconds (ms) long, made up of 1 ms sub-frames. Within these sub-frames there are 0.5 ms slots, each slot being composed of 7 OFDM symbols. Uplink and downlink transmission is scheduled by Resource Blocks (RB), with each RB in time slots of 0.5 ms or 180 kHz and composed of 12 subcarriers of 15 KHz, orthogonal to each other, allowing transmission to a different user on each subcarrier. Figure 10 shows the RB structure. In the channel bandwidth, +- 10% is used for signaling, and the remaining 90% are effectively used for data. The transport blocks will be transported with data, and the size of these blocks is a function of the bandwidth and the number of RBs, according to Table 7.1.7.2.1-1 of the 3GPP documentation on LTE Release 14 (ETSI 3GPP, 2017).

As an example, considering an available bandwidth of 10 MHz, 90% of this bandwidth (9 MHz) is effectively used for data. Each RB contains 12 subcarriers of 15 KHz each, totaling a width of 180 KHz for each resource block. 9,000,000 / 180,000 = 50, meaning 50 resource blocks can be used for a bandwidth of 10 MHz. The Transport Block Size (TBS) is what determines the data rate for an LTE user.

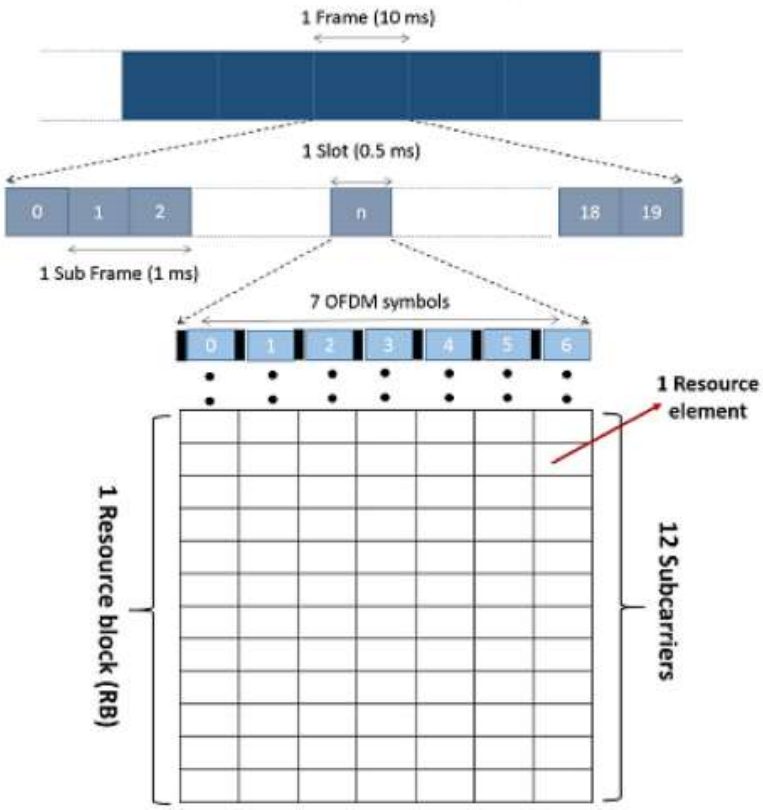


Figure 10 - LTE Structure (Kumbhar & Güvenç, 2015).

According to Table 7.1.7.2.1-1 in ETSI 3GPP (3GPP, 2017), the maximum TBS, considering a maximum TBS index (Itbs) lower than 27, for 50 resource blocks (Nprb), is 36,696 bits. Each block of 36,696 bits is transmitted in 1 ms; therefore, the maximum speed achieved per user in 1 second is about 36.7 Mbps. this example considers only one transmission layer, without using multiple antennas. A variety of multi-antenna techniques can help increase the throughput.

Figure 11 shows part of the transport block size table — Table 7.1.7.2.1 from ETSI 3GPP (2017). In our example, Nprb=50. In case of 20 MHz of bandwidth, Nprb=100 and, according to Table 7.1.7.2.1, the maximum block size is 75,376 bits. With a transmission time of 1 ms, it is equivalent to a maximum user speed of 75.37 Mbps. That means, without Multiple Input Multiple Output (MIMO) techniques, the maximum data rates for 10 and 20 MHz bandwidths are 36 and 75 Mbps respectively (Top Optimized Technologies, 2018).

The network load also impacts LTE throughput. Since radio resources are divided among subscribers, if more subscribers are active, less resources are allocated to a given subscriber. Radio conditions impact user bit rates; the UE measures radio channel quality and sends Channel Quality Indicator (CQI) to the eNodeB, which selects the modulation and coding scheme based on current radio conditions. In better radio conditions, a higher throughput is available because a higher modulation and coding scheme can be used, meaning more bits can be transmitted per time unit. There are 15 possible CQI values, each associated with a specific modulation and transmission format.

I_{TBS}	N_{PRB}									
	41	42	43	44	45	46	47	48	49	50
0	1128	1160	1192	1224	1256	1256	1288	1320	1352	1384
1	1480	1544	1544	1608	1608	1672	1736	1736	1800	1800
2	1800	1864	1928	1992	2024	2088	2088	2152	2216	2216
3	2408	2472	2536	2536	2600	2664	2728	2792	2856	2856
4	2984	2984	3112	3112	3240	3240	3368	3496	3496	3624
5	3624	3752	3752	3880	4008	4008	4136	4264	4392	4392
6	4264	4392	4584	4584	4776	4776	4968	4968	5160	5160
7	4968	5160	5352	5352	5544	5736	5736	5992	5992	6200
8	5736	5992	5992	6200	6200	6456	6456	6712	6968	6968
9	6456	6712	6712	6968	6968	7224	7480	7480	7736	7992
10	7224	7480	7480	7736	7992	7992	8248	8504	8504	8760
11	8248	8504	8760	8760	9144	9144	9528	9528	9912	9912
12	9528	9528	9912	9912	10296	10680	10680	11064	11064	11448
13	10680	10680	11064	11448	11448	11832	12216	12216	12576	12960
14	11832	12216	12216	12576	12960	12960	13536	13536	14112	14112
15	12576	12960	12960	13536	13536	14112	14688	14688	15264	15264
16	13536	13536	14112	14112	14688	14688	15264	15840	15840	16416
17	14688	15264	15264	15840	16416	16416	16992	17568	17568	18336
18	16416	16416	16992	17568	17568	18336	18336	19080	19080	19848
19	17568	18336	18336	19080	19080	19848	20616	20616	21384	21384
20	19080	19848	19848	20616	20616	21384	22152	22152	22920	22920
21	20616	21384	21384	22152	22920	22920	23688	24496	24496	25456
22	22152	22920	22920	23688	24496	24496	25456	25456	26416	27376
23	23688	24496	24496	25456	25456	26416	27376	27376	28336	28336
24	25456	25456	26416	26416	27376	28336	28336	29296	29296	30576
25	26416	26416	27376	28336	28336	29296	29296	30576	31704	31704
26	30576	30576	31704	32856	32856	34008	35160	35160	36696	36696

Figure 11 - Part of the transport block size table (Table 7.1.7.2.1-1) (3GPP).

For each CQI reported in the uplink subframe, the UE must use the highest CQI index possible, between 1 and 15, from Tables 7.2.3-1, 7.2.3-2 and 7.2.3-3 of the ETSI 3GPP (3GPP, 2017). CQI indexes and their interpretations are given in these tables for reporting CQI based on the modulation: Quadrature Amplitude Modulation (QPSK), 16QAM, 64QAM, and 256QAM. A single Physical Downlink Shared Channel (PDSCH) transport block, with a combination of modulation scheme and transport block size corresponding to the CQI index, occupying a group of downlink physical resource blocks termed the CSI reference resource, could be received with a transport Block Error Rate (BLER) not exceeding 0.1. The CSI reference resource is defined by the downlink physical resource blocks corresponding to the band to which the derived CQI value relates (ETSI 3GPP, 2017).

The usual indicator for expressing coverage in 4G is the Reference Signal Received Power (RSRP), which measures the average power per LTE carrier calculated on all reference signals. This power is defined per carrier; therefore, it is related to the average reception power through Equation 2.1, which considers the number of resource blocks (Nrb) in the available bandwidth, and the number of carriers per block (12 for LTE), called subcarriers; each subcarrier transmits different users (Top Optimized Technologies, 2018).

$$RSRP(dBm) = Power\ Rx(dBm) - 10 \times log\ (12Nrb) \tag{2.1}$$

Other important indicators are Reference Signal Received Quality (RSRQ), which is the average value of the received signal related to the measured band; Received Signal Strength Indicator (RSSI), which is a measurement of the received power of the band, considering interference and noise; and Signal-to-Interference-plus-Noise Ratio (SINR), measured at the mobile receiver, which determines the quality of the signal and the data rate achieved. The SINR value determines the maximum modulation and coding scheme usable in the transmission that allows the BLER not to be exceeded.

Regarding spectral efficiency, 3GPP adopted a methodology based on the calculation of spectral efficiency, obtained from adjustments in the Shannon formula, which determines the theoretical maximum capacity of a Single Input, Single Output (SISO) channel, measured in spectral efficiency as a function of SINR, which cannot be achievable in practice due to several considerations in the implementation that lead to efficiency loss. According to 3GGP considerations, described in 3GPP (2009), the achieved spectral efficiency considers an attenuation factor, which includes the implementation losses, spectral efficiency and SINR.

As an example, applying the methodology used by 3GPP, for the 800 MHz band, with a bandwidth of 10 MHz, MIMO 2X 2, 3 bps/Hz of spectral efficiency would be necessary to obtain 30 Mbps, with the SINR value of 12 dB. It should be noted that a 3 bps/Hz efficiency requires a 16QAM modulation format and high modulation and coding scheme, because the higher the modulation and code used, the higher the SINR required and vice versa. Therefore, using a

QPSK ½ modulation will have a lower SINR required than 16-QAM ½, and the UE will have to support this modulation, according to its category (Top Optimized Technologies, 2018).

In the radio channel architecture, there are three different types of channels: the logical channels, composed by control and traffic channels; transport channels; and physical channels. All of these have uplink and downlink direction, with more channels in downlink. The logical downlink control channels carried common channel information used to broadcast, paging, control information to a particular UE, and multicast information. The downlink traffic channels carried traffic to a particular UE and multicast data.

The transport channels carried data and signaling between the Medium Access Control (MAC) and the physical layer in LTE. The physical channels are responsible for the radio related issues as modulation/demodulation, coding/decoding, and MIMO techniques; they can be classified into physical control channels and physical data channels. As the Physical Broadcast Channel (PBCH), which carries system information for UE; the Physical Downlink Shared Channel (PDSCH), which carries System Information Block (SIB), paging information and user plan data, both transmitted in downlink; the Physical Uplink Shared Channel (PUSCH), used for data transmission by the UE; and the Physical Random Access Channel (PRACH), used for random access procedure, both transmitted in uplink. PDSCH and PUSCH are the channels used for data transmission in downlink and uplink, respectively. PRACH is the channel used when the UE wants to connect for outgoing transmissions, as a call or transfer data, to respond incoming services, to request information, synchronization, handover, etc.

2.2.1.2 Quality of service, priority and preemption

Preemption for traffic bearers intends to provide access to MCC users in commercial networks even in situations with high traffic usage; that is useful when EFRs share resources with MNOs. The radio admission and traffic bearer assignments for MCC users are based on LTE admission control mechanisms, allocation and retention priority. When the UE carries out the RACH procedure, the following step is the radio resource assignment procedure, where high priority access parameters can be used by MCC users for Radio Resource Control (RRC). To ensure the priority Allocation and Retention Priority (ARP), the parameters should be specified as shown in Figure 12. The ARP preemption priority is used to prioritize the assignment of a bearer. For application priority, the Quality of Service Class Indicator (QCI) assignment can be used.

Using quality of service, priority and preemption, the LTE technology can provide priority treatment to the MCC user with a pre-defined allocated capacity in an LTE MNO. Priority and preemption are different things. Priority gives to the user the possibility of accessing the channel with priority in the queue to allocate the service; meanwhile, the current service allocated to other user will not be interrupted by a user with higher priority, as higher priority just gives priority in the waiting queue; it is also possible to set up different levels of priority between users, that will give them different positions in the waiting queue. Whereas

preemption gives the user the possibility of interrupting the current service and allocating it to him; it is also possible to set up different levels of preemption between users.

User Priority	User Identification	Traffic Class	Barring (RACH)	Establishment Cause (RRC)
PS First Responders	PS Emergency; PS1 to PS5	12 - 14	BarringForSpecial	HighPriorityAccess
Commercial User Emergency	Commercial User Emergency	10	BarringForEmergency	Emergency
Commercial User Non-Emergency	Commercial User Non-Emergency	0 - 9	Low BarringFactor	Mobile Originating

Figure 12 - Radio access for EFRs and MNO users in a shared network (Borkar et al., 2011).

In the case of MCC, the dispatch center should always have the highest preemption level, since the center must be able to intervene at any time in the communications, interrupting communications, or even modifying the priorities and preemption of users in real-time (BroadMap, 2017).

2.2.1.3 5G Networks

The development of 5G was motivated by the increasing variety of connected devices. The International Telecommunication Union (ITU) grouped three different usage scenarios, namely Enhanced Mobile Broadband (eMBB), Massive Machine Type Communication (mMTC), and Ultra-reliable Low Latency Communication (uRLLC). Figure 13 shows some examples of envisioned usage scenarios according to the International Mobile Telecommunications (IMT) for 2020 and beyond (ITU, 2015). A comparison between IMT-2020 key capabilities and those of IMT-Advanced systems is shown in Figure 14.

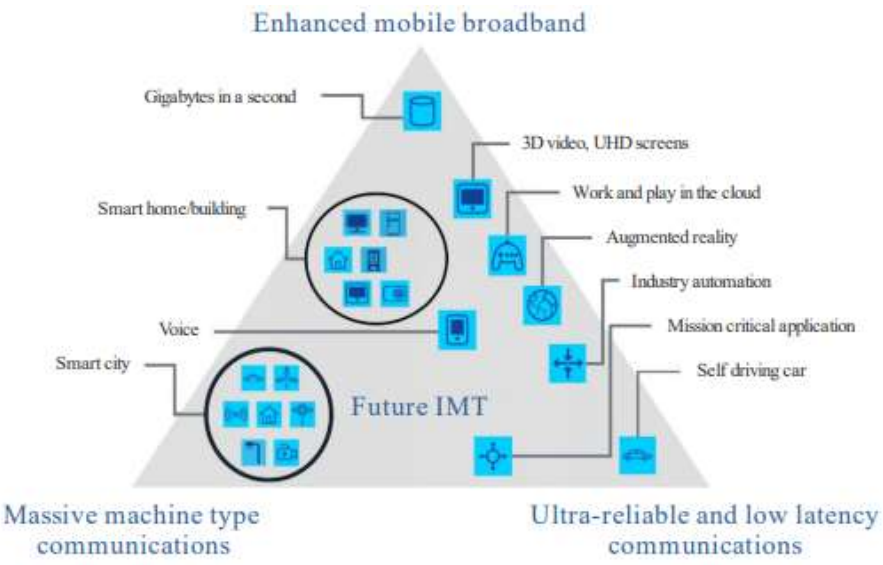


Figure 13 - Usage scenarios of IMT for 2020 and beyond (ITU, 2015, p. 14).

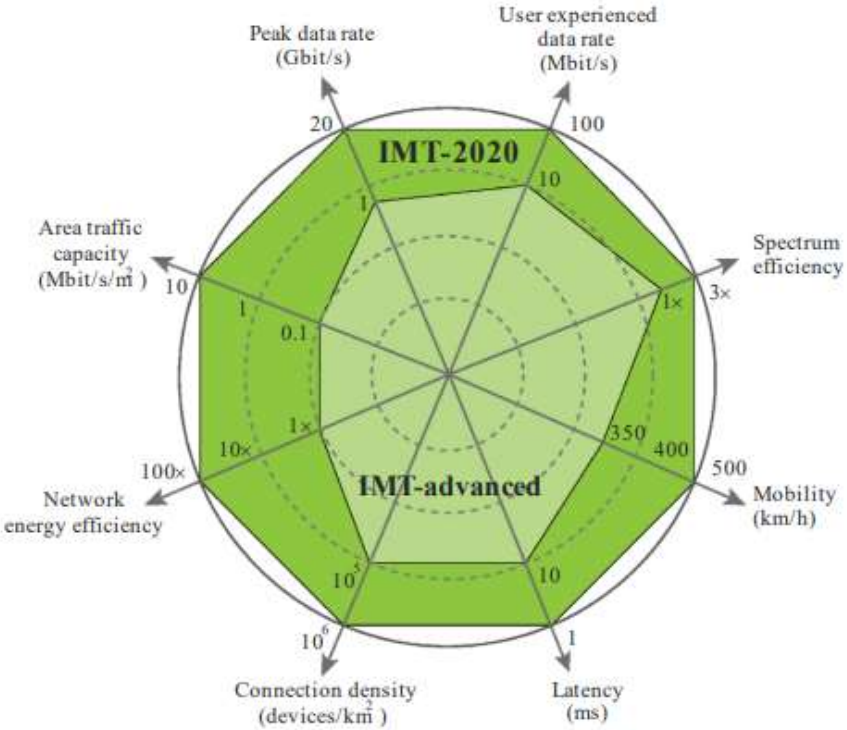


Figure 14 - Enhancement of key capabilities from IMT-Advanced to IMT-2020 (ITU, 2015, p. 16).

The architecture of 5G networks is more flexible than the previous generations, working with RAN virtualization, network slicing, and service-oriented architecture. Initially, most MNOs are implementing 5G anchored on the existing 4G architecture in Non-Standalone (NSA) mode. Subsequently they implement a Standalone (SA) mode, using frequencies below 6 GHz to enhance coverage, with better throughput than 4G, and frequencies above 6 GHz with high throughput and low latency, which are known as millimeter waves (mmWave).

5G supports the same modulation and coding scheme as LTE, Quadrature Phase Shift Keying (QPSK), 16 Quadrature Amplitude Modulation (QAM), 64 QAM and 256 QAM modulation formats for both uplink and downlink. Also, the 1024QAM is defined for 5G in 3GPP technical specification 38.214, related to physical layer procedures for data in 5G (3GPP, 2022). Facing the challenge of highest frequencies in propagation conditions, massive MIMO and beamforming are used in 5G to improve received signal strength and end-user throughput, also providing higher number of data streams and increasing cell capacity. These topics are detailed in section 2.2.1.4.

Network Function Virtualization (NFV) is another key aspect of 5G, separating physical network into multiple virtual networks and enabling network slicing, where the connections can be made possible according to the applications' requirements by dividing the available network resources into multiple logical slices, allowing the network to provide different classes of services to users and to "orchestrate communication services in a flexible way through logical networks with a lesser cost and time" (Thiruvasagam & Chakraborty, 2021, p. 12).

Multi-access Edge Computing (MEC) enables the provision of ultra-low latency services by moving computing processing to the network edge (close to the user's location). For provision of diverse latency-sensitive services, such as augmented reality, a set of VNF can be instantiating network slicing on top of MEC cloud servers. Software Defined Networking (SDN) allows decoupling control plane and user data plane from networking devices, together with NFV, and MEC makes the network more agile, scalable and flexible, supporting multiple use cases with different demands as eMBB, mMTC and uRLLC.

2.2.1.3.1 5G network architecture

For the deployment of the 5G networks, the 3GPP fixed some options. The option 3 is NSA deployment, where the gNBs are secondary nodes anchored by the eNBs acting as master node, the gNBs and eNBs are connected by the X2-interface, the radio access is connected to the EPC through the legacy S1-interfaces, and the EPC sees the gNB as a radio resource inside the 4G radio network, using 4G and 5G for user data traffic. Option 3 presents variations according to the data routing, namely option 3, option 3a, and option 3x. The option 3x is the more adopted by MNOs for NSA deployments, where the 5G gNB uses the 4G as the anchor point of the control plane, allowing UE to use the service enhancements provided by the 5G gNB. The frame structure of the digital multi-carrier scheme is the same, based on OFDM. 5G also has logical channels, transport channels and physical channels, like the 4G network. The physical channels are divided into data channels and control channels, in uplink and downlink.

2.2.1.3.2 5G Internet of Things

According to Li et al. (2018), the existing 4G networks have been used on IoT devices, matching the needs of IoT applications. Although, with the 5G networks, a massive expansion of IoT uses is expected, increasing the challenges such as large number of connection of nodes, the 5G enabled IoT (5G-IoT). The authors also pointed out that the requirements of 5G-based IoT will have a massive connectivity with a high number of IoTs; while 4G can provide a transmission speed of 1 Gbps, 5G can provide users with speed up to 10 Gbps, with reliable connection to thousands device at the same time. The 5G-IoT architectures are expected to provide logically independent networks, use cloud-based RAN, and simplify core network architecture for distinct use cases, leveraging ecosystems of highly heterogeneous smart devices.

The requirements of 5G-based IoT are high data rate for applications as Virtual Reality (VR), Augmented Reality (AR) and high-definition video streaming; high scalable and fine-grained networks, increasing scalability; very low latency for applications such as AR; reliability resilience; security; long battery lifetime; connection density allowing a massive number of devices; and mobility. Also, the 5G-based IoT architecture should satisfy some services' requirements, such as cloudification / network function virtualization (NFV), network management, and providing smart services based on big data analysis (Li et al., 2018).

2.2.1.4 MIMO, Massive MIMO, SU-MIMO, MU-MIMO and Beamforming

MIMO is a technique used in LTE and 5G to add a spatial dimension of transmission due to the multipath in the airspace caused by multiple antennas. Although, in 5G, MIMO has much more capacity than in 4G. This way, several parallel channels can be established between the eNodeB and the UE, increasing the data rate. This diversity can come from different techniques, such as antennas having a different polarization or being spatially separated.

The beamforming is another technique that uses directional transmissions toward a specific receiving device, improving the spectral efficiency by providing a better SINR. "It is the ability of a beamforming array to scan its beam towards a user, while at the same time suppressing signal strength in the direction of an interferer is what makes it such an effective tool for increasing capacity" (Powell, 2014, p. 17). That capacity makes beamforming antenna with higher gain than a MIMO antenna, due to its narrow beam.

While MIMO and beamforming have been proven to increase capacity, the methods they use require different antenna architectures. The columns of a MIMO array act almost independently from each other, with each column carrying part of the load. The columns of a beamforming array act as a team to carry the whole data load simultaneously (Powell, 2014). The same signal is sent from multiple antennas. Therefore, in a given location, the receiver will receive multiple copies of the same signal, and depending on the location, the signals may be in different phases, resulting in combinations that may be destructively or constructively combined. With MIMO, when the data goes through a channel that has multiple antennas for transmitting and receiving, the signal will be process at the receiver to estimate the input.

Meanwhile, mobile communication is increasing in use, thus congesting the low bands. To get more bandwidth, it is necessary to use higher frequencies that previously were not used for mobile communication. When the frequency goes up, that implies more bandwidth available, but the coverage is smaller, since the higher the frequency, the smaller the wavelength, meaning more propagations losses. Because of the wave size getting smaller, the antennas' elements also get smaller, and the power per element antenna reduces (there is less conductor in the element to support the power). That implies the need for more antennas, resulting in massive MIMO. Current frequencies for mobile communication are around 1 and 2 GHz, moving towards 6 GHz to 28 GHz for 5G. This will translate into the need for massive MIMO, resulting in narrow beams transmissions — more elements, more narrow beams.

While MIMO can increase user data rate due to several parallel channels, massive MIMO can also increase cell capacity due to simultaneous users using several parallel channels, and it can be combined with beamforming, improving SINR and cell capacity. In Figure 15, the antennas are using polarization diversity; the first antenna is transmitting in 2 ports and receiving in 2 ports (2T2R) though 2 parallel channels. If each channel has, for example, 50 Mbps, the 2 layers of MIMO will allow the user to have 100 Mbps. The second antenna has 4T4R, with 4 parallel channels. So, if each channel has 50 Mbps, the 4 layers of MIMO will allow

the user to have 200 Mbps. The third antenna is a massive MIMO 16T16R, with 16 parallel channels; meanwhile, most UE available nowadays are limited to 4 parallel channels, meaning the maximum user throughput will not change from the 4x4 antenna, but the cell capacity will increase 4 times, since with 16T16R it is possible to transmit 4 parallel channels to 4 users simultaneously. The same logic is applied for more TX/RX elements, such as massive MIMO antennas with 32T32R and 64T64R.

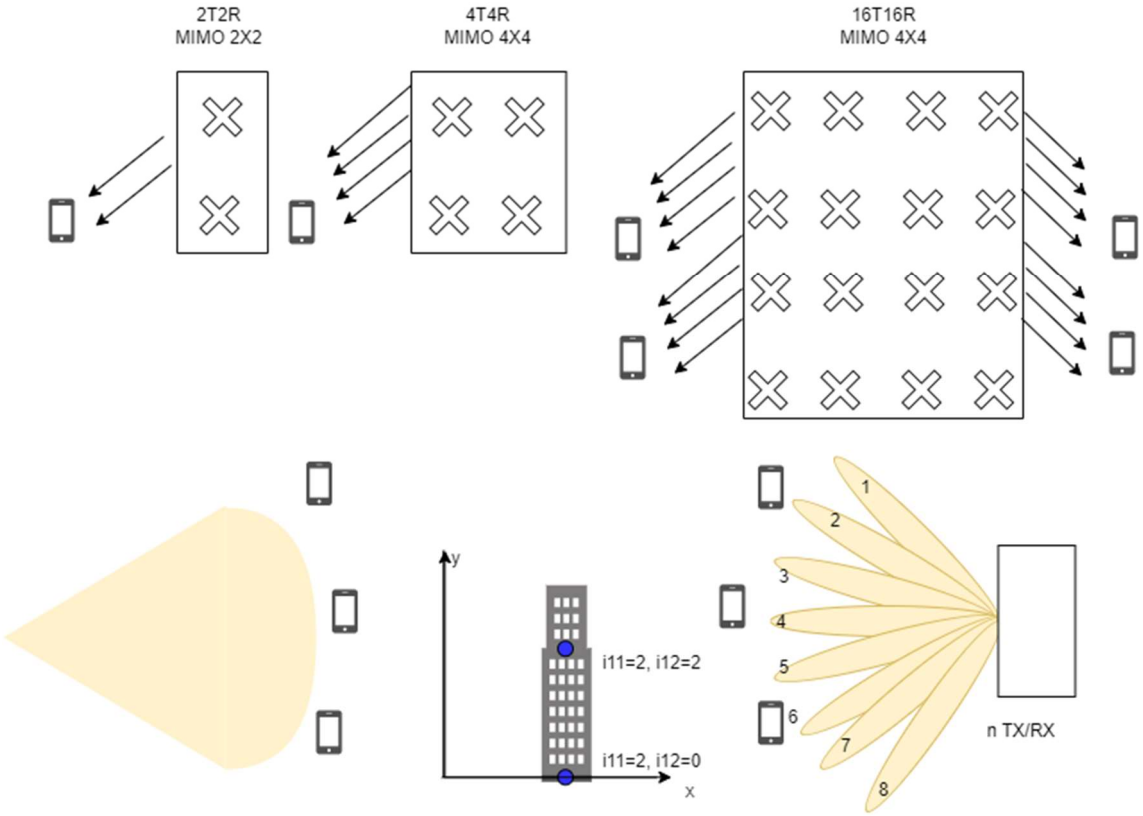


Figure 15 - MIMO and Beamforming techniques (Author).

With smaller array, a smaller TX element can generate beams with bigger beamwidth; meanwhile, with bigger array, the beam gets narrower. The more TX elements, the narrower and more directional will be the beam. Figure 15 shows in orange the coverage of a small array antenna compared to a bigger array antenna (massive MIMO) for the same azimuth. Normal beams are wider and generate more interference in the network, while narrower beams are more directional with less overlap, more gain and less interference, resulting in better SINR and throughput. Massive MIMO is suitable for places with high traffic, dense urban environments with high buildings and skyscrapers.

In MIMO working with single user (SU) MIMO, the cell capacity is split between the users receiving different resources blocks in frequency domain. For example, 3 UE could receive allocation of 50%, 30% and 20% of the RBs, so if the cell capacity is 100 Mbps, they will receive respectively 50, 30 and 20 Mbps from distinct RBs. The users can use 4X4 MIMO, but the data

will be split in frequency domain. The allocation of multiple beams to different receiving antennas of a single user increases the number of layers, intensifying the power of the receiving signal, and contributing to a better user throughput. With beamforming and massive MIMO, it is possible to have Multi-User (MU) MIMO, using multiple UE sharing RBs. Instead of having one UE using 50% and the second UE using 30%, both UE could use 80% of cell capacity, sharing resource blocks due to using different beams. In this way, even using the same RB, they will not interfere on each other, since there is enough separation between beams to decode the data. With that technique, beyond the benefit of multiple layers to the end user, improving the user throughput, the result will also increase the cell throughput.

According to Bouchenak et al. (2021, p. 371), despite the benefit of increasing throughput, massive MIMO "results in high interference caused by the large number of antennas installed on a small sized array. Crucially, beamforming is introduced to mitigate this problem", meaning a relation between the use of massive MIMO and beamforming, not motivated just by increasing the data capacity but also to improve the channel performance. MIMO schemes to be used are a decision made by the gNB based on the channel state information between transmitting antenna ports of massive MIMO system and receiving antenna ports of the user device, and could be categorized as stated below:

> MIMO schemes are categorized into Sounding Reference Signal (SRS)-based SU-MIMO, Precoding Matrix Indicator (PMI)-based SU-MIMO, and beamformed Channel Status Information (CSI), CSI-Reference Signal (RS) MIMO for low capability devices. The device's capability and radio field condition decide the best MIMO mode. In addition, when multiple users demand for high load traffic simultaneously in a TDD system, DL multi-user (MU)-MIMO solution, which allocates mutually orthogonal beams to the users, is able to enhance the cell throughput and users' experience (Samsung, 2020, p. 7).

There are different types of beamforming in 5G, and their complexity is increasing. First, the type of beaming differs from the type of amplification used before transmitting the signal in downlink. There is the digital beamforming, where beam weights are processed in baseband; analog beamforming, with the weights applied after power amplified in downlink in radio frequency analog beamforming, operating in a set of predefined static beams; and hybrid beamforming, by mixing analog and digital techniques. For frequencies bellow 6 GHz, the most common is to use digital beamforming; for frequencies above 6 GHz, such as 28 GHz, analog beamforming is preferred.

The beamforming weight processing in one or multiple Synchronization Signal Block Beam (SSB) beams, is one type of beamforming, forming a grid of beams covering the whole cell area, where it is possible to sweep the SSB beam. The number of beams transmitted will be equal to the number of SSB beams; it is possible to have different beam sets where each beam is cross polarized and can set two multiplexed streams.

In the beam refinement with CSI-RS, most cases are 1 SSB covered by 4 CSI-RS beams, called refined beams (Sousa et al., 2020), as shown in Figure 16. The gNodeB sends those beams periodically in downlink and the UE measures all beams and reports the strongest beams back to the gNodeB, which will send PDSCH data on one or several strongest beams. The PRACH needs to consider the beamforming. In 5G there is no continuous downlink control channel, meaning no always-on listening space in the uplink for common channels. The gNB periodically activates a receive beam to receive the Random Access (RA) messages from the UE. The UE infers from the SSB beam the time slot where the RA should be sent; the PRACH is also used for beam recovery. For purposes of beam tracking the UE will measure the RSRP from the CSI-RS or from the SSB.

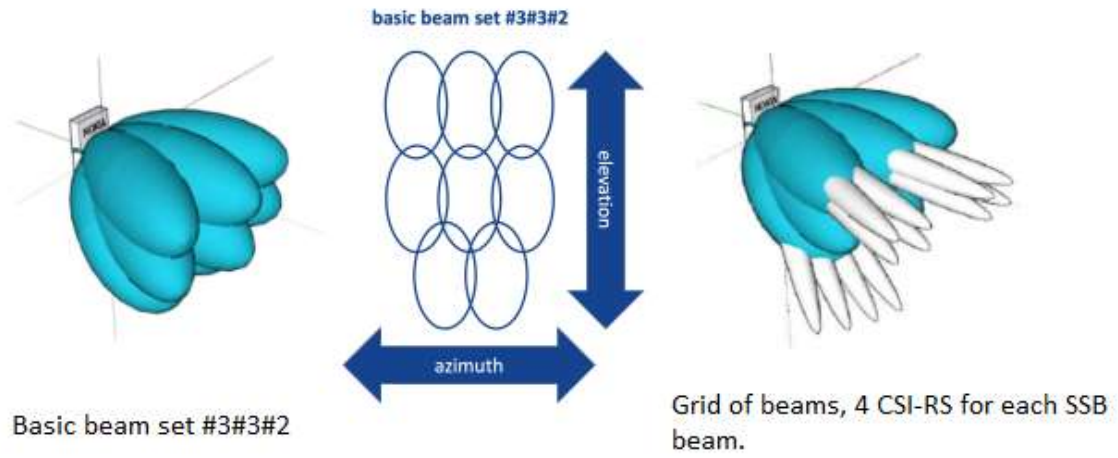


Figure 16 - Basic beam set and grid of beams, adapted from Sousa et al. (2020).

There is also a type of digital beamforming, the Precoding Matrix Information (PMI), where multiples beams can be used by the UE. In 4G, the base station constantly transmits common cell-specific Reference Signal (RS); in 5G, Channel Status Information RS (CSI-RS) is transmitted for the user's channel state measurement in a periodic or aperiodic way (Samsung, 2020). To choose the best beam, the UE will read the signal from the gNB, the CSI-RS reference signals, and send the Channel Status Information (CSI) feedback, which is composed by Rank Indicator (RI), Channel Quality Indicator (CQI) and PMI.

Based on the reference signals, the UE finds the PMI providing the best SINR; for every configuration there is a fixed number of PMIs. The UE will receive the reference signal, check the SINR of each output, and send to the gNB the PMI with highest SINR for PMI estimation. PMI sent by UE is not exactly a matrix, but some coefficients $i_{1,1}, i_{1,2}, i_2, i_{1,3}$. From those coefficients, the gNodeB will constitute the PMI matrix.

In the UE, this SINR will be converted to CQI for CQI estimation and sent to the gNB; based on that, the gNB will choose the beam the UE should use, which could be a different PMI from what the UE indicated, and the UE will continue to be able to read the downlink. In

Figure 17, the UEs indicates to the gNB, through the CSI feedback, that the best beams are 2, 4 and 6. This example shows only the PMI beam, without showing the CSI-RS beam.

Instead, the PMI is made up by some components indicating the horizontal and the vertical beams. In the example of Figure 15, there is one UE moving, indicating different positions at the time, and the gNB will choose a new beam according to that position. In legacy passive antennas, the signal is transmitted uniformly within the coverage direction, as shown on the left side of Figure 15. In that situation, the user could have good or bad signal depending on their position, without any beam adjustment.

The PMI beams are associated to the CSI-RS beams. For example, if there are 4 CSI-RS beams available, and each CSI-RS has 64 PMI beams, if the mobile is in CSI-RS beam 2, any of the 64 PMIs associated to that CSI-RS could be allocated to the UE. The gNB and UE still continue to take periodic measurements, so if a UE is moving, the PMI beams could change, and also the CSI-RS with inter-cell mobility and intra-cell mobility. Using the same, 4 CSI-RS beams with 64 PMI beams each, result a total of 256 beams for that antenna.

. The Synchronization Signal (SS), Primary Synchronization Signal (PSS), Secondary Synchronization Signal (SSS) and the Physical Broadcast Channel (PBCH) are transmitted on legacy SSB beams. 3GPP allows various digital beamforming configurations in 5G, defined in 3GPP (2022). The PMI is based on a codebook concept and each PMI value corresponds to a codebook index, given by the tables detailed in item 5.2.2.2 of the 3GPP report; the most commercially used nowadays are detailed in Table 5.2.2.2.1, Type I Single-Panel Codebook. The PMI will result in a vector, which represents the shape and orientation of the physical beams.

Multiple CSI-RS resources are not a user mandatory feature; some UE doesn't have that capability, and the system allocated dedicated beamformings to the UE. The schemes enable 32 ports into a possible subset of CSI-RS, and the UE can use one of the PMIs into the selected CSI-RS. Figure 17 shows PMI beams from 8 port CSI-RS (4 CSI-RS resources), just to illustrate that the PMI beams are associated to a CSI-RS resource. First, the UE determines the best CSI-RS resource — in that example, the resource 4. The 3D view of the antenna propagation should resemble the Figure 18, which represents the 3D response pattern in QPSK modulation for different numbers of users, ranging from 4 to 32, of a hybrid beamforming massive MIMO system in mmWave. The radiation patterns have more lobes as the number of users increases, and they are much more directive.

That is a simplification for better understanding of the antenna configurations using PMI beamforming and the estimation made by the UE. In fact, there is a mathematical complexity to understand the precoding matrix detailed in 3GPP TS 38.214, which are the combination of two matrices related to number of layers, antenna structure (array), and channel properties from reported values $i_{1,1}, i_{1,2}, i_2, i_{1,3}$, that are converted according to 3GPP tables and applied on the 3GPP codebook table to determine the resulting matrix W, which will be applied on antenna ports to transmit.

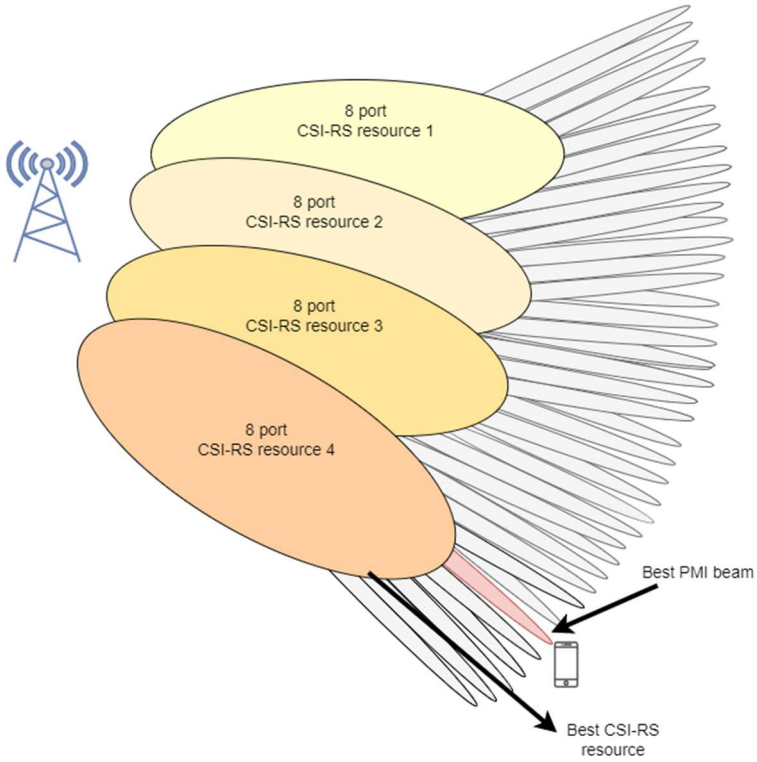


Figure 17 - PMI beams from 8 ports CSI-RS (Author).

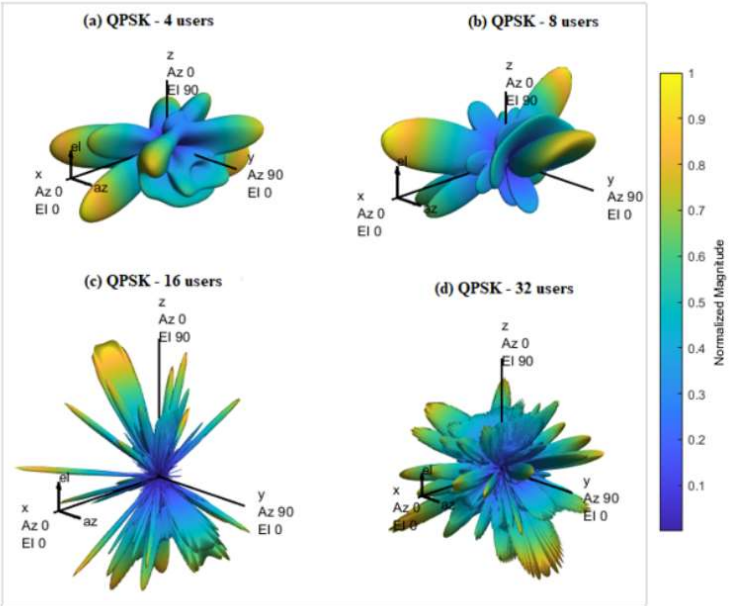


Figure 18 - 3D response pattern, extract from Bouchenak et al. (2021).

In Samsung (2020), simulations were made to compare gains over the cell average throughput with legacy 4T4R antenna, compared to some downlink MIMO schemes considering 3D urban macro channel model. 80% of the users were assumed to be inside of eight-floor buildings, each floor 3 meters high, for 3.5 GHz, 100 MHz channel bandwidth. The results showed that DL SU-MIMO with a 32T32R massive MIMO radio improves from 23% to

64% the average cell throughput compared to a 4T4R legacy antenna. The DL SU-MIMO 64T64R massive MIMO improves from 78% to 90%. The DL MU-MIMO layers for the 32T32R and 64T64R massive MIMO radio improve 77% and 136% respectively. The results showed that SU-MIMO and MU-MIMO can improve the throughput compared with legacy antennas, being a fundamental strategy for 5G.

2.2.2 Throughput

The bandwidth available is a determining factor of the maximum throughput rate achievable. Due to this large bandwidth, a certain spectral efficiency will be necessary to reach the expected data rate, and this efficiency determines the signal level requirements for reception. The frequency band used affects the propagation capacity of the radio signal, the propagation path loss due to the distance, and penetration losses with different losses by clutter, e.g., water, forest, dense urban environment, suburban, and so on. The signal over interference is also impacted by the signal received, which also affects the data rate to be achieved. That means, the frequency band, bandwidth, signal received, quality of the signal, interference, categories of the UE allowing better modulation and coding scheme, and the network load are the main inputs to be considered to measure the throughput achieved by an end user.

The LTE-Advanced introduced the carrier aggregation, allowing different bands to aggregate and improving the throughput, with the possibility of adding up to a total of 100 MHz of bandwidth from a maximum of 5 carriers (20 MHz for each carrier), from different bands that are not necessarily contiguous. It also allows MIMO with more capacity, until 8x8; introduced the Coordinated Multipoint transmission/reception (CoMP); and the Enhanced Inter-cell interference coordination, alleviating the interference and improving the bit rate.

To determine the approximate throughput rate in downlink and uplink, several factors should be considered, as mentioned above, as well as factors related to electromagnetic signal propagation in different environments, i.e., shadowing and penetration losses; the equipment that transmits and receives the signal, i.e., receiver sensitivity, power transmission, antenna gain and MIMO type; and interference factors, i.e., noise figure, thermal noise, etc. For this, the Radio Network Planning (RNP) is facilitated by the use of software tools to predict the behavior of the network with a certain rate of reliability, depending on the project scope.

The data rate is directly related to the achieved SINR. To calculate it, it is necessary to obtain the necessary power, and the interference plus the noise in reception. Then, a load model of the network should be applied. To predict signal, propagation models are used considering the environment and the quality of the available database (clutter classes, clutter height, digital terrain models, and 3D vectors). More quality databases mean the more precise will be the model, allowing results as multi-storey signal prediction inside buildings for different floors.

2.3 Information Technology used by PPDR Agencies

Currently, PPDR agencies use various information technologies to assist in their daily activities. However, even before there were computer technologies, the agencies sought to use science to solve the problems experienced at different times. In the case of the police, it was necessary to store and classify information to facilitate the identification of people. In the criminal area, the first widely accepted scientific method of identification and classification was developed by Bertillon (1883) in 1879; the anthropometry,[10] also called bertillonage, intended to identify repeat offenders. This method used a combination of physical measurements that had to be collected, meeting procedures meticulously described.

In addition to physical measurements, such as head measurements, the method also included frontal and profile photography, and registering of particular signs such as scars. Precise body measurements were performed on individuals, with the results divided into three categories and organized into classification sheets with different categories. With that, the number of sheets needed for cataloging was much lower than the alphabetic system used previously, and allowed a degree of precision that did not exist until then.

In 1902, Bertillon's system was in use in most countries that had any development in the field of criminology. This was the case of Portugal, where criminal anthropology was institutionalized in 1899, as described in the law of August 17, 1899, art. 12, which created anthropometric posts. Anthropometric posts begin to be installed in some buildings used in penal and criminal areas, namely in Lisbon, Porto and Coimbra (Antunes, 2019). In 1911, through the decree of May 12, 1911, art. 46, the anthropometric post of the Coimbra University was also responsible for acquiring criminal statistical data of all detainees in prisons, police stations and jails in the city of Coimbra, following Bertillon's procedures. Later, those posts also became responsible for the issuance of identity cards (Instituto de Antropologia, Universidade de Coimbra, 1985; Antunes, 2019).

In addition to the identification method, Bertillon also defined an archiving method, and founded the judicial identity system in 1893. Bertillon in France and Cesare Lombroso in Italy started the so-called positivist school of criminal anthropology (Santos, 2005; Antunes, 2019). Cesare Lombroso was a psychiatrist who was concerned with studying the criminal, giving them morphological characteristics. He created the theory of the delinquent man (1876), through the analysis of more than 25,000 prisoners, 6,000 delinquents and 400 autopsies, reaching the conclusion that those criminals had physical and psychological characteristics in common (de Molina & Gomes, 2012).

---

[10] In the 17th century, Johann Sigismund Elsholtz developed a measurement system to prove a relation between body measurements and some diseases, adopting the term anthropometry. From the end of the 18th century, the concept became broader, being defined as measurements on living persons or dead bodies for any purpose (Antunes, 2019).

Lombroso (2013) created a stigma of the criminal as one who had certain physical and moral characteristics, e.g., individuals with voluminous jaws, uneven ears, dark eyes and hair, facial asymmetry, lack of beard in men, too much hate, excessive vanity, among other physical, behavioral, psychological and social characteristics. He defended the idea that not all criminals were born a criminal, but the ones with those characteristics, the atavistic ones, were meant to be criminals since birth. In that sense, they should be separated from society even before committing a crime, due to their immutable characteristic of criminality.

In 1891, an anthropometric office was opened in the city of La Plata, Argentina. Working there, Juan Vucetich verified many irregularities in the collection of measurements from the Bertillon system, and innovated by collecting the ten fingerprints of prisoners in addition to Bertillon's measurements (Ferrari & Galeano, 2016). Vucetich classified fingerprint designs according to the indications of Francis Galton (1892), who developed the first fingerprint classification system through three design patterns: Laced (L), Arched (A), and Whorl (W), following an alphabetical classification of the ten fingers — for example, LLAWL LWWLL —, which is used in identification until the present day. In his book, Juan Vucetich (1895) demonstrated how to identify fingerprints through specific signs, thus seeking to identify and classify the samples.

The first case of identification of the author of a crime through their fingerprints occurred in 1892, when Vucetich identified Francisca Roja as the murderer of her two children. Francisca accused her neighbor of the crime; however, there were bloody fingerprints on her house's door, and the prints matched Francisca's, who was accused and sentenced (Mariano, 2018).

With the evolution of science, the police started to identify individuals also by means of their DNA. Nevertheless, according to Bina (2009), the estimate of a fingerprint being identical to another is 1 in 17,000,000 million, which makes it a unique form of identification and the most used in the police environment. Even in the case of monozygotic[11] twins, who have almost identical DNA, the fingerprints are the most effective way of individualizing them, since differences in DNA are rare in these cases, but the drawings formed on the twins' finger pulp will always be different.

The use of science by the police began due to the need to identify repeat offenders. The identification of people also facilitates criminal investigation, by using fingerprints and current DNA collection — procedures carried out at crime scenes through crime scene investigation experts, using equipment suitable for collecting and processing information. That allows a criminal process based on scientific evidence, with personal identification as well as storage and processing of information aided by the technology.

[11] According to Jonsson et al. (2021), monozygotic twins differ on average by 5.2 early developmental mutations, and approximately 15% of monozygotic twins have a substantial number of these early developmental mutations specific to one of them.

DNA databases also make it possible to cross-reference information, such as genetic material found at a crime scene that can be inserted into a database in the search for cross-referencing information to identify suspects. Until a few years ago, many people were convicted based only on the blood type found at the crime scene plus some other evidence, which might not identify the suspect in a unique way. Several mistakes have been made by Justice, some of them already identified by the Innocence Project (2022).

Several other data had to be stored and processed, in addition to identifying people, such as criminal offenders' data; stolen vehicles; missing persons; data from police investigations, such as telephone recordings authorized by the court; and countless other information is stored in databases by the police. This static information from a database can be used dynamically when associated with other sources of information, as real-time information. For example, a voice identified in a homicide audio can be searched in open sources as YouTube; a car registered as stolen in a database can be identified by its license plate, using cameras scattered throughout the cities; cameras with facial recognition integrated with police databases can help find missing people. The possibility of using static information combined with dynamic and real-time data can enable agencies to act more efficiently.

According to ITU-R (2003, p. 7),

> As PPDR operations become more reliant on electronic databases and data processing, access to accurate and detailed information by staff in the field such as police, firefighters and medical emergency personnel is critical to improving the effectiveness of the staff in resolving emergency situations. This information is typically held in office-based database systems and includes images, maps, architectural plans of buildings, and locations of hazardous materials systems. (...) Moreover, in disaster and emergency situations, critical decisions to be made by controlling authorities are often impacted by the quality and timeliness of the information received from the field.

Some software currently used by the police uses the combination of existing data from police databases compared to open source and big data, allowing numerous analyses, such as comparison between a voice obtained in a criminal investigation with videos on YouTube; categorization of possible relationships between people from analyzed videos; processing of audios and videos available in database and open source with transcription of dialogues and contextual search; in addition to the use of artificial intelligence combined with these various sources of information.

The PS big data integration system with multi-source heterogeneous data association technology can be used to quickly organize information about local residents and information on fugitive suspects, tracing suspects and handling accidents; also for court management, as nowadays it is common for people to use social media to post videos or comments about what happened after accidents, incidents and disputes, which can be used in court for better understanding the situation through the local case history (Yu & Wu, 2020).

For disaster situations, in the past, much of the information received by the agencies was about events when that had already happened, without an accurate reading of what happened and how many people were affected. Information technologies currently makes it possible to even avoid disasters through the reading of sensors — as in the case of smoke detection by a sensor that triggers measures to contain the fire.

Through ICTs, as verified in the SLR, it is possible for agencies to act efficiently in disaster situations, with better understanding of the real-time data and helping in the emergency decision-making process. For example, a system can receive and process information such as coordinates, type of incident and number of victims, collected from social sensing, and send a radio alert to the rescue services with optimized route details and the location of the nearest emergency centers. The system can also be linked with drones in a 5G network, sending alert and rescue assistance to the population.

As highlighted by Lopez-de-Teruel et al. (2019, p. 1), "computer vision, big data analytics, and machine learning algorithms can then be used to generate machine-based knowledge which can drastically speed up response times for public safety interventions (e.g., fires and crimes)". Big data can be used to support disaster events, such as analyzing big data from social sensing, remote sensing, sensors with context-aware computing, high resolution maps, on-field video transmissions, real-time monitoring, and other sources that could support establishing an early warning index system.

According to Wu and Yu (2020), when big data information is not used in emergency situations, decision-making is mainly based on the working experience of the commander, which may lead to errors in the decision-making process. Although, with the use of proper information systems, more on-site information can be collected, improving the accuracy and scientificity of the decisions during crisis, and leading to rational implementation strategies and reliable recovery measures in the post-event phase.

2.4 The information and communication technology society

The present is interactive, behaving as a network and it has the evolution of society's relationship with information as its locomotive — to the maximum point that today's society is known as the information society, where perceptions and the speed of events in information technologies impact the volatility of the knowledge and in the reality, which seems to change human relationships with the world and with machines (Jorente et al., 2009; Capurro et al., 2003; Buckland, 1991; Barreto, 1997; 1998; da Silva & Ribeiro, 2002; Zins, 2006; 2007; Bauman, 2003; Burke, 2003; Castells, 2002).

The current society is also known as the "Surveillance Society", a concept discussed by several authors such as David Lyon (2018) and Zygmunt Bauman (2014). According to Lyon (2018), in the 21st century, surveillance is characterized by the active participation of people,

being a way of life, thus characterizing a culture of surveillance that proliferates in society, ceasing to be an external component where everyone gets involved, consciously or not, moving away from the idea of discipline associated with surveillance, and becoming something internalized and common in daily life.

This normality is in part fueled by a generalized fear provided by some Government agencies, with the state assuming the role of what resembles that defended by Günther Jakobs, when he creates the concept of the criminal law of the enemy[12] (da Silva & Horita, 2017). This was mainly accentuated after 9/11, which contributed to creating a generalized feeling of insecurity and accentuating the fear of already stigmatized social groups, e.g., the Arabs.

Knowledge that used to be centralized is now distributed. The information available through digital media has proliferated through the internet, it can be accessed from anywhere — which also modified the forms of control and censorship. The Chinese State is a current example of government controlling of online content, with page blocks, some pages being automatically redirected to equivalent sites, internet providers under government control, inspection of content accessed by users, and application of punishments ranging from fines to imprisonment. It's the so-called Golden Shield Project (GSP), which officially started in 1998, with increased surveillance by the communist party to contain a possible countercoup from the opposition. In 2013, it was estimated there were more than 2 million people working on the GSP, doing some kind of content verification and censorship (Exame, 2013; Punyakumpol, 2011).

Despite unofficial control, the USA also performed surveillance through a global surveillance system developed by the National Security Agency, as revealed by Edward Joseph Snowden, a former analyst at the Central Intelligence Agency (CIA), who also worked as an NSA agent and made public details of various programs used by the NSA. Edward J. Snowden (2019) revealed how he helped to create this worldwide espionage system through the collection of phone calls, text messages, emails and even images from laptop cameras in any country, resulting in a mass surveillance system through the invasion of people's privacy and other government's information, touching citizen's individual freedom as well as the sovereignty of nations. Snowden's revelations caused diplomatic unease between the USA and allied nations, which culminated in the restructuring of the NSA.

[12] Criminal law of the enemy is a concept introduced in 1985 by the jurist Günther Jakobs that differentiates the criminal law of the citizen, in which, by maintaining the status of citizen, he has guaranteed due legal process. And the criminal law of the enemy, in which, the individual who puts society at risk, such as a terrorist, is constitutionally unprotected, as an enemy of society (da Silva & Horita, 2017).

2.5 Surveillance culture

Even though the concept of the surveillance society is recent, the ideas behind it are old. In 1787, Jeremy Bentham developed the idea of the panopticon, which would be an institutional building where people are kept under inspection, designed especially for prisons, but also applied to hospitals, schools, popular housing for poor people, factories, workhouses, hospices and industries. The essential idea of the panopticon is central surveillance. According to Bentham, people kept in an institution should be constantly watched; as the number of inspectors to make this possible would become unfeasible, the closest option would be for the prisoners (in case of a prison) to feel constantly watched (Bentham et al., 2008).

The idea of the panopticon is based on the idea of the inspector being something central and able to watch the inmates without being seen by them. The inmates would never know when they were being watched, leading them to believe that they were constantly watched. For the inspector to have this central position in the prison, capable of seeing but not being seen, Bentham drew a circular building with the inspector in the middle, allowing them to easily see all the cells. The inmates' cells would be along the circular walls, with windows on the outer wall and iron bars for observation (Bentham et al., 2008).

Some buildings were built using Bentham's idea, such as the first psychiatric hospital in Portugal, Hospital Miguel Bombarda, in Lisbon, one of the few circular panoptic buildings built in the world; the Lisbon Penitentiary, in accordance with the radial panopticon star-plan model (Direção Geral do Patrimônio Cultural, 2011); and the Presídio Modelo, in Cuba.

The best-known analysis of Bentham's panopticon project is Michel Foucault (2004), where the author discusses the "panopticism". In the book "Discipline and Punish" (1975), Foucault discusses topics related to surveillance carried out in panoptic spaces by a disciplinary society and the games of force and power in the social sphere. Several authors propose a contextualization of the term for the present, where surveillance has become a central theme in the analysis of power, enhanced by technological ubiquity, e.g., synoptic (Mathiesen, 1997), post-panopticon (Zygmunt Bauman, 2003), digital panopticon (Bessi et al., 2007), and electronic panopticon (Lyon, 1994; Pereira et al., 2013).

Power has become extraterritorial, freeing the holders of power from the limiting techniques of the panopticon, which leads Bauman to coin the term post-panopticon to describe the present where, unlike the panopticon, the holders of power can escape at any time, becoming even inaccessible — a movement reflected in the current wars of liquid modernity, where conflicts through land forces are avoided and targeted stealth bombing attacks are prioritized; where the main point is not the conquest of a new territory, but "the destruction of the walls that impeded the flow of new and fluid global powers", going beyond the military branch as "a promotion of free trade by other means" (Bauman, 2003, p. 18).

In the society with synoptic style described by Thomas Mathiesen (1997), this promotion of free trade results in people who control themselves through self-control, with the spectacle replacing panopticon supervision, however, maintaining the same power. All are inspectors and the current obedience is to standards, which no longer needs coercion to be achieved. In the so-called democratic capitalist society, the media seduction of commerce replaces coercion, and individuals are at the same time coercive and coerced, "under the guise of free will, instead of revealing themselves as an external force" (Bauman, 2003, p. 101).

There is still objectivity and subjectivity behind these technological devices. The external forces that dictate disciplinary practices and establish a new social order are often subjective, masked as free will, as described by dos Santos and Portugal (2019, p. 37):

> The presence of technological surveillance devices such as security cameras, electronic passwords, biometric, voice recognition and even iris reading is undeniable. These artifacts are ostensibly distributed in everyday experience and are present in all spaces of life in large cities. However, these tactics of control do not exclude the logic proper to the panoptic paradigm articulated with biopolitics; discursive practices of truth are articulated with disciplinary and biopolitical practices, inscribing modes of functioning and appearance of objects and subjectivities.

Studies on the surveillance society also use the term "Orwellian" to relate aspects associated with authoritarianism and surveillance. This term emerged from the novel "1984", published by George Orwell in 1949, that creates the idea of the "Big Brother", where the supreme leader of the fictional Oceania controlled the population through screens spread like double mirrors in public and private places, monitoring the population. The hero of the novel is Winston, who works in the Documentation Department of the Ministry of Truth and whose job is falsifying records of history to shape them according to the Party's interest (Orwell, 2009).

The surveillance society is more suited to an external point of view of surveillance. However, nowadays surveillance is disseminated by everyone, being characterized by a surveillance culture, inside facts of modern life, like people using social networks to monitor the way of life of others (and also trying to compare it with their own life and habits); normalizing the increasing surveillance of states for fear of certain social groups that are generally stigmatized; the wholesale surveillance that treats people as potential consumers, using data to build profiles aimed at marketing; the increasing use of wearables by people, such as sensors on the body to measure performance during exercise; the classification of people according to their behavior, from the Uber app driver to the classification of people by some governments — which can lead, for example, to choosing who should have more rights to access services according to a score (Lyon, 2018).

In this regard, it makes sense to expand the discussion of the panopticon outside the confined spaces architecture idealized by Bentham, bringing Foucault's thought of the power

relations of panoptism to the present day, added to the ubiquity of technological tools. This point of view helps in the study of our current society and in the identification of the prohibitionist and punitive policies of the state, in a "space in the which is increasingly difficult to know who watches the watched" (dos Santos & Portugal, 2019, p. 46).

Technologies changed the relationship between cities and individuals. Virtual communities are formed using cyberspace, surpassing the need for physical locations and social relationships through face-to-face interaction. In this way, there is a new collectivity based on information and a sociability based on individualism, fed by an increasingly consumerist culture, where the individual becomes a social network profile, subject to categorization and control. In addition to buying goods, the individual also becomes the commodity itself, within a surveillance culture resulting from market and power relations. Digital cities emerge with different social relationships, "inhabited" by virtual communities under constant surveillance in all cyberspaces.

In this context, new challenges begin to exist for non-virtual cities. The culture of surveillance brings challenges to the dignity of the human person and to democracy, as described by Rodota (2008), with a fluid surveillance, typical of the liquid society described by Bauman (2014). It is characterized by the proliferation of control devices, such as surveillance cameras, with a notion of the State's omnipresence against imminent threats. Influenced by the fear of surveillance by "enemies", the society accepts more surveillance as a measure to protect surveillance itself, as voluntary servants of the State's invisible surveillance. That society seems increasingly guided by the criminal law of the enemy.

The issue becomes even more complex when analyzing who actually holds the information. The State has access to part of this data; however, large companies such as Google, Instagram and Facebook possess the information that transits in digital cities. Those companies use and market these data for the most varied purposes, including political activities on a global scale, which can impact the political and economic autonomy of national states. For example, Cambridge Analytica, a British company that combined data mining and analysis with strategic communication, would have influenced the US presidential elections in 2016 (Lewis et al., 2018; NBC News, 2018).

Individuals are increasingly exposed while the invasion of privacy becomes more difficult to regulate, due to the combination of corporate giants owning the data, the global breadth of cyberspace, and the relationship with the states' policies (Pinto, 2012). A change in the space-time relationship brings new challenges, especially in the legal sphere, impacting the sovereignty of nations as well as individual guarantees. The society arranged in network permeates all areas of everyday life with a real impact on society (Castells, 2002). In this sense, when analyzing present and possible ICT scenarios, this research also contextualizes and questions the new relationship between cities, individuals, ICTs, and government.

3

Systematic Literature Review

This section aims to identify the state of the art on the topic and to assess the feasibility of applying methods and methodologies used in researches about related topics. The keywords were chosen by bibliographic review and application of bibliometrics laws. After choosing the keywords, an SLR was carried out in three different databases, aiming to identify relevant publications from the last five years.

The Cochrane Collaboration (2022) method was used due to its representation, with more than 9,000 SLRs published in the healthcare field, and to its consolidated methodology and structure, which can be replicated in other areas. According to this method, seven steps must be followed, namely: 1) research question; 2) location and selection of studies; 3) critical evaluation of research; 4) data selection for analysis; 5) data analysis and presentation; 6) data interpretation; 7) improvement and update.

The first step was presented in Chapter 1. For the second step, the keywords to the SLR should be identified, this can be done with the combined use of the bibliographic review and bibliometrics. Bibliometrics is the support for the science metric study, providing subsidies for identifying the most relevant studies, terms and researchers in the area, according to the incident use of bibliographic citations (Zanine et al., 2012).

From bibliometrics, the Laws of Bradford, Lotka and Zipf can be used, respectively, in the measurements of journal productivity, authors' productivity, and frequency of words in a text (Guedes & Borschiver, 2005). In this research, a bibliographic review combined with Zipf's Law is used to identify the keywords, selecting the most representatives in the research area. After the selection, the SLR was performed on scientific databases.

Bibliometrics was performed in the scientific database Web of Science, using the expression "Mission-Critical Communication", with time stipulated in the last five years until May 29, 2022, resulting in a total of 22 articles with 150 keywords; the term that appeared the most was Mission-Critical Communication, with 9 appearances. The application of Zipf's Law resulted in 7 terms, whose frequency varies from 9 to 3 appearances, they are: 5G mobile

communication; Edge computing; interference; Internet of Things; mission-critical communication; Reliability; unmanned aerial vehicle (UAV).

It was also verified the most used terms within the bibliography referring to the research topic in the fields of Electronic Engineering, Telecommunications, Technology Assessment, User Experience, and Smart City. The most cited terms that do not appear in the previous selection and should be included are listed below. 11 terms were selected. By analyzing which terms could be related to the research and joining terms by similarities, 6 of them were chosen as keywords for carrying out the SLR, marked in green in Figure 19.

Terms	Synonyms found in the literature review
5G mobile communication	5G
Internet of Things	
Mission Critical Communication (MCC)	MCC
Land Mobile Radio (LMR)	
Long Term Evolution (LTE)	4G, LTE, Long-Term Evolution
Public Protection and Disaster Relief (PPDR)	Public Safety, PPDR
Incident Response	
First Responders	
Usability	
Smart City	Safe City, Smart Cities, Safe Cities, City Safety
Technology Assessment	*Technological Assessment*

Figure 19 - Terms used on the SLR (Author).

3.1 Use of keywords to perform SLR

From the combinations of keywords with logical operators, strings are created for searching in the databases, the combination of the 6 terms without repetition resulting in 57 search strings. The choice of the databases was according to the themes addressed, relevance and number of indexed works, namely SCOPUS, Institute of Electrical and Electronics Engineers (IEEE), and Web of Science. All strings used, as well as the results found, can be consulted in Appendix A.

After searches in the databases using strings, it was necessary to establish the criteria to be used to decide whether to include a paper. These criteria are used as filters, according to the step 3 of Cochrane Collaboration (2022) methodology. Four criteria were applied in this research, namely:

1. First criterion: Filtering considering a time interval (the last five years), in the 3 selected databases, for all the 57 strings. This search returned 59,552 matches in the Scopus database, 5,387 in the Web of Science database and 4,718 in the IEEE database, totaling 69,657 publications.
2. Second criterion: Reading the title of all articles found in the combined search of 3 or more strings, checking if they can be contextualized in this research by reading the abstract of the articles that, from the title, seemed to be contextualized. This criterion resulted in the verification of 180 works in the

Scopus database, 49 in the Web of Science, and 57 in the IEEE database, totaling 286 publications. Eliminating repetitions, it resulted in 146 publications.

3. Third criterion: Only studies that have met the previous criteria were analyzed for this third criterion, which is reading the introduction and conclusion to verify if they can be contextualized in this research. This step resulted in the selection of 41 papers that should be fully read, according to step 4 of the Cochrane Collaboration (2022) methodology.
4. Fourth criterion: Only the papers that have met the previous criteria were analyzed for this fourth, which is the submission of a cross search. The cross search consists of verifying the references cited within the researches that met all the above criteria. Then, a verification is carried out if the cited research was also found through the searches with strings; if not, that should be fully read (Almeida et al., 2012). This analysis resulted in the inclusion of 38 additional papers.

3.2 Data selection for analysis

The 79 researches selected for analysis are those that resulted from the application of the third and fourth criteria from the previous topic. A complete reading of those articles was carried out, with the objective of searching for content within the contexts of the keywords used in the search strategy. The content is presented below in the form of state of the art on the subject, following steps 5 and 6 of the Cochrane Collaboration (2022) methodology. Also, other relevant papers and technical reports were included in the state of the art on the subject, according to their relevance for this research.

3.3 Gaps

The literature review showed the existence of several technological solutions for the PPDR field. Also, due to the constant evolution of the ICTs, new solutions are to be expected. However, there is a lack of works that present the various solutions and possible applications for communication and information in an integrated way, focusing on applied cases. After all, the cities have different demands that should be properly addressed, avoiding "one size fits all" solutions for Smart City strategies in order to help the decision-making process of governments and agencies.

This evaluation of ICTs for use by PPDR agencies must be performed in a broad way, in addition to the technical aspects, since the same technological integrations that aim to improve the performance of agencies lead to debates related to the classification of information by PPDR agencies, identification of people, access to information, privacy, ethics, legal affairs, among other aspects that could impact the society. There is a lack of technological broadening

analysis, which includes the perspectives of different actors, better understanding of the activity, and possible pathways for the digital transformation of MCC considering Smart City.

Technology Assessment (TA) has been defined as a form of research that examines the consequences of the application of technology, considering different aspects, for example, societal, ethical, legal and economic, intending to provide information on policy alternatives to policymakers (Banta, 2009). Also, the construction of scenarios is part of the TA approach (Tran & Daim, 2008), enabling a better understanding of the solutions[13]. In fact, there is a lack of TA studies in the MCC field considering Smart City scenarios, the Smart City Public Safety Emergency Management. Also, there is a lack of a deep understanding of what Smart City Public Safety Emergency Management is and its relationship with MCC.

3.4 Hypothesis

The goal of smart and sustainable cities involves the construction of urban spaces where people can have a better quality of life. The United Nations (UN) have defined 17 Sustainable Development Goals (SDGs), launched in the 2030 Agenda, that seek to promote a better life for all people. The SDG 11 is to "make cities and human settlements inclusive, safe, resilient and sustainable", highlighting items 11.5 — "by 2030, significantly reduce the number of deaths and the number of people affected by disasters" — and 11.7 — "by 2030, provide universal access to safe, inclusive public spaces" (UN, 2015). Studies found in the literature review suggested that ICTs could help the cities to achieve the SDG goals.

Considering the goal of creating safer and more resilient environments, improving population's quality of life can be achieved and/or facilitated by PPDR agencies using ICTs to provide a better performance of their activities. The studies found in the literature review indicate that, to achieve this, it is necessary to use ICTs in an integrated and interoperable way, through actions coordinated by Command and Control Centers (CCC), receiving information from cities and agencies to optimize management and assist in decision-making, aiming to improve the population's quality of life and increase the efficiency of the cities' operations and services. This way, the hypothesis 1 of this research is: the use of ICTs by PPDR agencies consider Smart City scenarios, through a Smart City Public Safety Emergency Management.

Hypothesis 2: it is possible to identify indicators for assessment of the ICTs used by PPDR agencies, intending to verify if using appropriate ICTs in a Smart City scenario bring positive impacts in society, helping the cities toward the SDGs (measurements of the Smart City Public Safety Emergency Management).

---

[13] According to Bergamaschi and Ferasso (2020, p. 55), "Scenario planning is about making choices today with an understanding of what might happen to their actions in the future" when several questions should be considered as what are the driving forces? intending to identify the main theme, forces and environmental trends, logical scenarios, implications, the main indicators and flags, etc.

Hypothesis 3: it is possible to build scenarios for MCC considering Smart City environment through a systemic view and better understanding of the activity, in a Constructive Technology Assessment (CTA) approach. According to Versteeg et al. (2017), CTA aims to align expectations of a broad range of stakeholders, involving them in the design process of new technologies, intending to better suit the society needs. In that sense, this approach considers society both as an actor in the ecosystem and as a recipient of technological application, acting in the mechanisms of application and control of the technology. This way, technology is applied through social innovation, "understood as an innovative practice with the aim of creating the broadest possible positive impact on society" (Bencadirno & Greco, 2014, p. 39), in order to strengthen democracies and institutions, and contribute to a sustainable social development.

Hypothesis 4: By mapping a general MCC scenario considering Smart City environments then applying the appropriate frameworks, it is possible to build scenarios for applied cases. The construction of scenarios should consider a broad view and an integrated performance of the PPDR agencies, adding transparency and scientificity to the decision-making process made by the CCCs and the PPDR agencies.

Through an integrated performance of PPDR agencies, using appropriate ICTs in Smart City scenarios, working in a Smart City Public Safety Emergency Management, PPDR agencies can provide better services to guarantee Public Safety and effective actions in emergency situations, helping the cities to reach the SDGs. Although, for that affirmation to be confirmed it is necessary to measure the impacts of that use. In this sense, the framework to the scenarios' construction shall map some indicators for assessment of the Smart City Public Safety Emergency Management.

3.5 Summary of gaps, hypothesis and objectives

Figure 20 summarizes some research gaps that this work intends to help resolve, as well as research objectives, research questions, and the initial hypothesis that this study sought to validate.

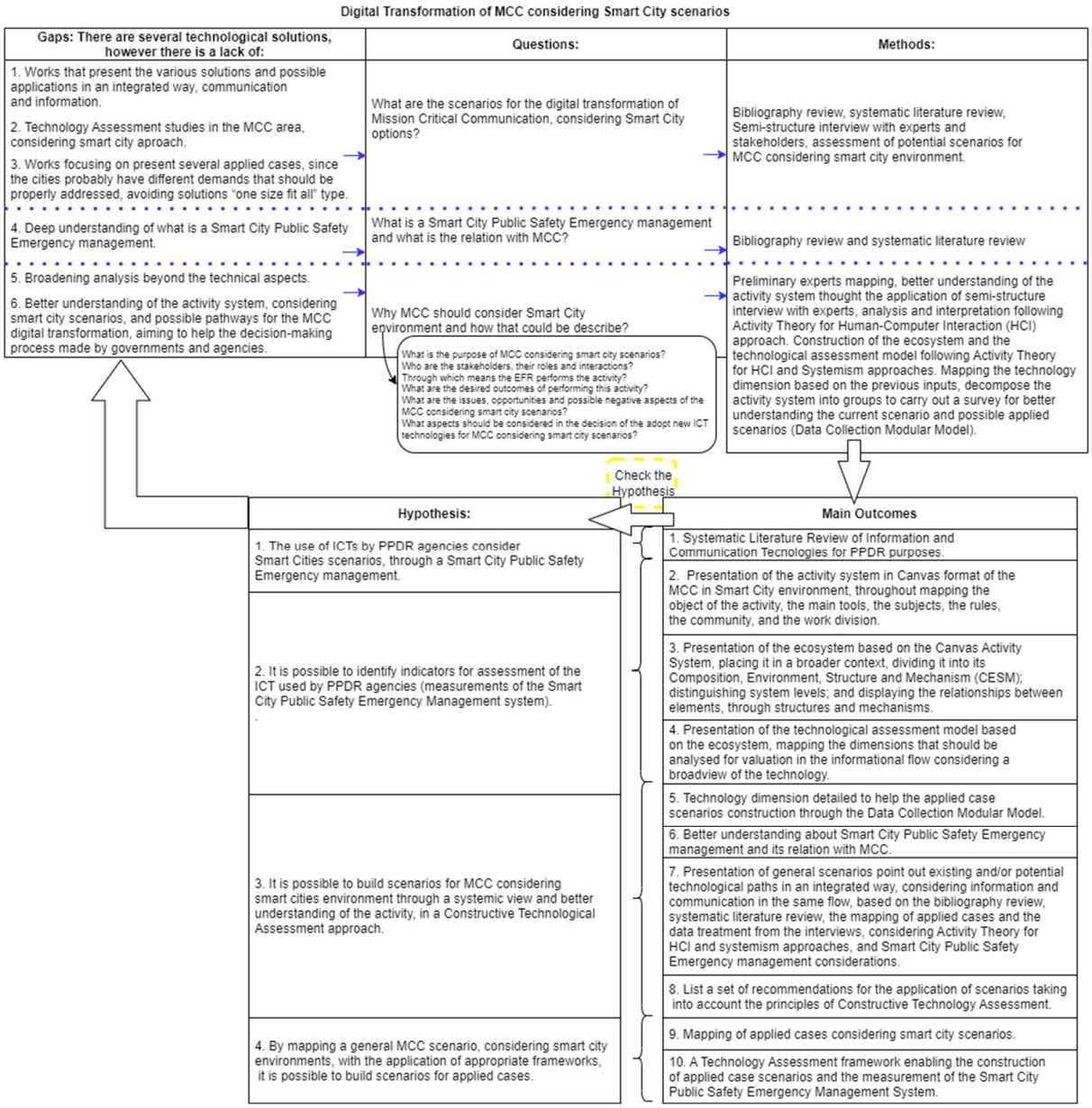


Figure 20 - Research gaps, objectives, questions and hypothesis (Author).

4

CONSTRUCTION OF SCENARIOS BASED ON THE SLR

This chapter presents the state of the art related to the theme of this research, intending to construct scenarios based on the Systematic Literature Review (SLR).

4.1 Information Technology

In the PPDR field, there are several motivations for using information technology to help society, from reducing crimes rates to responding to emergency situations. Nevertheless, to make an informed decision about which information technology PPDR agencies should use, one needs a better understanding of the types of data to be collected, the sensors to be used, computation techniques, and data mining tools available to assist in the data mining process. This process aims to gather knowledge from databases, visualize information through classification and real-time analysis, and then decide about which information should be shared with the communication technology system, and how. In that sense, this section intends to present an overview of the Cyber-Physical Systems used for PPDR purposes.

According to Wei & Sheng (2019, p. 1), "in the context of rapid development of information technology, intelligence and big data technology, it is necessary to optimize the integration of various types of scientific and technological resources to improve the timeliness and accuracy of urban smart emergency systems and improve the level of social and government emergency management".

The term IoT stands for Internet of Things. The first IoT device — a toaster that could be turned on and off via the Internet — was created in 1990 by John Romkey. In that same year, Neil Girchenfeld described the IoT principles in his book "When Things Begin to Think". In 2005, the first report on the IoT topic was published by the International Telecommunications Union

(ITU) (Al-Sarawi et al., 2020). The standardization of IoT is being led by the industry and IEEE's IoT architecture working group, the P2413 project on standards specifications (Atat et al., 2018).

The increasing number of devices such as smartphones, sensors, Radio-Frequency Identification (RFID), with their integrated communication and interactions, has created global Cyber-Physical Systems (CPS) applicable to different areas. CPSs are systems that integrate computation, communication and control across networks and physical processes. Through these systems, it is possible to represent the reality of the physical world in digital environments. IoT allows different CPSs to be connected for information transfer. For a better understanding, Atat et al. (2018) presented a CPS taxonomy, providing an overview of data collection, storage, access, processing, and analysis on big data for CPS, intending to provide a panoramic summary of different CPS aspects, including different security solutions and different use contexts.

The data acquisition is performed by sensors. There are two main sources of data: context-aware computing and communications, and social computing. Context-aware computing and communications consist in raw data collected by virtual and physical sensors using logical sensors and web services technology, as the data used for weather information. Data collection can be performed by physical sensors, virtual sensors, logical sensors, middleware infrastructure, context servers, or manually.

The sensors need to engage in context-aware computing to provide relevant information that could be interpreted and analyzed. In this regard, sensors need to store processed meaningful information, which can be done by themselves or by means of other artifacts, such as toolkits or middleware platforms. Then, the information can be classified into primary and secondary contexts, which are related to how the data were obtained — for example, reading RFID tags directly from the devices is primary context, while reading from the industrial plant's database is secondary context (Atat et al., 2018).

Social computing / social sensing is a type of crowd-sensing in which data are collected from users that share their sensed data using their own smartphones, shaping the notion of mobile big data. That differs from big data in a computer network due to specific characteristics. For example, nearby subscribers may exhibit mobility patterns and behaviors that can be used by the MNOs to measure traffic and network quality, and to perform optimization. Habits, opinions, notifications and interests can also be shared and used to construct a social community, which can be beneficial in emergency situations.

Remote sensing is a type of sensor that could be used, for example, to collect data from distant sensors, for purposes such as earth observation, oceanography, and others. Remote sensing can have real-time processing, as proposed by Rathore et al. (2015), analyzing real-time remote sensing big data using the Earth Observatory System.

In disaster management, geospatial information generated from satellites can be used for geospatial solutions, as shown by Lwin et al. (2019). The authors discuss the establishment

of a city geospatial dashboard, which is part of the core project development of a comprehensive disaster resilience system and collaboration platform in Myanmar. The system can collect, share and visualize geospatial data collected from satellites, IoT devices, and other big data sources. The intention is to gain understanding of human mobility patterns in space and time, to improve disaster preparedness and emergency responsiveness.

Social sensing can be also used in crime analytics and predictive policing, with the use of geolocated tweets to predict incidents, mobile phone location to construct predictive models of crime hotspots, neural networks trained on Google Street View images to rank neighborhood crime levels, and crime tips received from social networking platforms. The use of social sensing data combined with synthetic data and crime report data from the police can provide crime analytics and predictive policing (Mohler & Brantingham, 2018).

Xie and Yang (2018) proposed to use social media data to enhance disaster response. Interactive communication and user-generated content of social media include a diverse array of mobile-based tools. Since most social media data have information on time and geographical position, they are useful for spatial-temporal analysis. Also, social media can be used as a near real-time disaster data source for the current Geographic Information System (GIS) applications in disaster scenarios.

Atat et al. (2018) listed two different social computing tools: participatory sensing and crowd-sensing. In participatory sensing, users collect and share information using their own devices. However, the trustworthiness of the collected data could be an issue. The level of user's engagement to share information could compromise the amount of data collected, and the sharing of personal information could also be an issue for privacy and data protection.

Despite the challenges, involving citizens in public affairs through participatory design and participatory sensing could contribute to the achievement of successful e-government applications. Kyakulumbye et al. (2020) propose a smart city digital model premised on participatory design for PS requirements, gathering to advance a participatory design-sensing architecture IoT for Kampala Smart City. The paper suggested a framework for operationalization of e-government for citizen applications through smart mobile phones and similar affordable sensing devices.

According to Kyakulumbye et al. (2020, p. 8), "participatory sensing is a concept of communities and other group of people contributing sensory information from the sensing layer (situation around them) aimed at jointly addressing issues affecting them at the application layer". The participatory sensing is linked to the topic of Digital Participatory Platforms for Civic Engagement, addressed by Coscia et al. (2020), and it is aligned with the participatory design approach, demanding citizens and stakeholders to the construction of the project life cycle (Kyakulumbye et al., 2019).

Song et al. (2017) provides a scope of crowd-sensing for smart cities, classifying it into two categories: personal sensing and community sensing. Personal sensing aims to collect

information related to user activities through smart device's user; community sensing data is collected from smartphones to monitor environmental phenomena about a topic, such as traffic conditions. It can be subdivided into participatory sensing and opportunistic sensing, according to the mode of user involvement.

In a crowd-sensing application, users can be both publisher and consumer of data, what brings crowd-sensing closer to a Constructive Technology Assessment (CTA) approach, for example, in a crowd-sensing-based real-time public transport information service. The task can be also initiated by smart devices of the crowd by requesting task execution at the server and sending sensed data, for example, with the detection of pollution in a certain area that the user passed by, with that detection sent to the server, it could initiate sensing application, assigning it to other smart devices in the same region.

According to Song et al. (2017), crowd-sensing can be divided into three domains: infrastructure, which is related to public infrastructure; environment, for example measuring pollution levels; and social, where participants share their data to provide better understanding of a community topic, e.g., bike route quality. The author categorized PS in the infrastructure domain, mentioning cases where crowd movement patterns were monitored to detect dangerous events, such as riots and high crowd levels.

Mobile crowd-sensing (MCS) is a type of community sensing. Collecting data from mobile devices (mobile sensing), "MCS uses social sensing via integrating and fusing the contributed data from mobile devices with that of the mobile social network services in order to provide solutions to more complex queries" (Atat et al., 2018, p. 5). For example, drivers can use information about traffic conditions in a participatory sensing network, with data collected from vehicles, residents, authorities' recommendations, and so on.

The architecture of MCS consist in servers, deployed by a government agency or a commercial organization, that demand tasks to be executed by smart devices of the crowd, generally, by choosing the devices where the sensing task is to be executed. To start sensing in a participatory sensing, the user may agree to the task; in opportunistic sensing, the device may automatically respond and send periodically data to the server.

Although, a sufficient number of participants is needed to ensure MCS applications have a good performance; therefore, some incentives could be adopted to attract participants. According to Zhang et al. (2016), incentives are divided into three categories: entertainment, when the sensing tasks are turned into a game; service, when participation is exchangeable for services; and monetary, when participants received money for their contributions. In the cloud-based crime reporting system proposed by Shih et al. (2019), the users are encouraged to participate through financial rewards.

About incentive mechanism and task allocation, Yang et al. (2020) proposed the CEDAR, a cost-effective crowd sensing system for detecting and localizing drones. The system intending to solve public security and privacy breach issues caused by drones, such as,

smuggling, intrusion, and illegal surveillance. The traditional approaches to perform it is through high costs tools as radar and computer vision. With CEDAR the authors proposed a way of detecting drones by smartphones, since drones use Wi-Fi to communicate with ground control stations. CEDAR uses detection algorithm exploiting historical Wi-Fi and MAC address used by drone manufacturers. CEDAR also uses received signal strength to localize the detected drones. To incentive the participatory sense the authors design an incentive mechanism based on online auction that guarantees truthfulness and consumer sovereignty. On the auction process the auctioneer selects the user with the highest contribution and gives the reward to him/her, while others have no payments. The detection rate in the CEDAR experiments reaches 86.7%, even without any prior information about drones.

The data collection type in MCS is crowdsourcing, which is "a process of acquisition, integration, and analysis of big and heterogeneous data generated by a diversity of sources in urban spaces, such as sensors, devices, vehicles, buildings, and human" (Xu et al., 2016, p. 1). Crowdsourcing allows mobile phone users and social network users to share data from their sensors, for example, traffic condition and pollution level. Anyone that shares information via social network could be seen as a social sensor, providing information that could be used during a fire emergency or traffic conditions.

Jilani et al. (2019) proposed an approach using participatory sensing on crowdsourcing, leveraging multiple smartphones users to collectively report emergency events, and an application framework emergency event reporting in smart cities using crowdsourcing. One of the most important challenges in emergency situations is the real-time information sharing between various stakeholders such as PPDR agencies, emergency medical services, hospitals, and the dispatch center. The paper proposes that volunteers within the vicinity of an incident can trigger an alert notification to the rescue services. The system will receive and process information such as coordinates, type of incident, and number of victims, sending alert to the rescue services with optimized route details, and the location of the nearest emergency centers. Spatial information can be collected from Global System Position (GPS), temporal information from smartphones' watches, and cameras can provide additional information.

After the information is collected, a decision-making analysis is needed through integration, filtering and visualization of the data collected. The result of the decision-making module is to generate an alert with the information collected to the respective rescue services, and the fastest route to the emergency location. The generated alert can also disseminate information to the public nearby the emergency situation, as how to support the rescue operation, or information to avoid the location by taking another road to their destinations. That could be done through Short Message Service (SMS) to mobile phones.

Felemban et al. (2020) proposed a big data framework that collects mobile sensory data from pilgrims, by providing them location-based context-aware services through a mobile application. The data collected is used to study pedestrians' flow rate and patterns, intending

to propose solutions to crowd related challenges as emergency evacuation plans. That could be a challenge for many cities as the study case of the article, Hajj, an annual pilgrimage to Mecca by Muslim, where more than 2 million pilgrims from more than 114 nationalities encamp in Mina for five days. The paper presents a big data framework that captures pilgrims' information through mobile phone sensory data, while they were offered multiple services through a mobile phone application. Then the data collected are stored in big data repositories for extracting trip information about individual and groups information.

Xu et al. (2016), proposed the 5W (What, Where, When, Who, and Why) model. To answer the 5Ws the Weibo social media's users are the target of crowdsourcing, collecting spatial and temporal information to detect the real time event of an emergency situation. The emergency event is shown as a GIS based annotation. Social network messages as "a car accident just happened", "I see a car crash now", are used for detecting real time events, and the GIS information is extracted from the social network check-in information. The temporal information can also be extracted from the posted messages, the picture shared could have relevant information about the event, the participator identity could also be detected. The reason of the event happened could be revealed from the shared information as "now a car has crossed the red line and hit a pedestrian".

From citizen's point of view MCS has some issues about security and privacy, since the owner of the data center collect sensitive data from users as location, and ambient sound. Such data can be used, for example, to detect behavioral patterns or routes of individuals. According to Song et al. (2017), the privacy could be preserved if the sensing data collected is anonymous, that is possible by removing the private part of the user data before sending it. Several papers discuss architectures that provide a privacy-preserving approach for crowd-sensing applications as Li et al. (2020), Messaoud et al. (2019), and Li et al. (2021). Wang (2022) summarizes existing privacy-preserving research to provide a reference in privacy protection research from the perspectives of participant recruitment; location; data; task allocation; and incentive method.

For PS, Mohler and Brantingham (2018) provide a framework for deploying predictive crime models based upon crowd-sourced information and protect individual privacy. The authors illustrate the methodology combining data from Los Angeles crime report, and PS posts from Nextdoor in Indianapolis. Another contribution of this paper is a framework for sharing of information about crime tips between private companies, PS agencies, and the public. The authors used 805,523 events from crime report data collected between 2009-2014 in Los Angeles; and 115 posts from Nextdoor social network, tagged as PS, between July 1st and December 7th, 2017, from Indianapolis. The experiment showed that with the use of crowd-sensing applications it is possible to have accuracy in space-time criminal incidents models, while maintain user privacy and process transparency (Mohler & Brantingham, 2018).

The security and privacy are also a concern for crime reports platforms, according to Tzay-Farn Shih et al. (2019), the primary requirements for crime reporting system are that the people who inform the crime should provide their real identity and that identity should be protected by the system, allowing the reporter to do report anonymously. The authors developed a cloud-based crime reporting system with identity protection, which combines digital certificates, symmetric keys, asymmetric keys, digital signatures, and a design verification mechanism, intending to reduce the unreported crime. Since the reporting system uses a cryptography mechanism for improved security and identity confidentiality, the users can inform the police anonymously.

Users are encouraged to participate through financial rewards, when is confirmed by the police officer superiors that the details of the report are sufficient for the reward, the financial system will remit the reward to the informer's account. For that, before a user have access to the platform, they must go to the digital certificate management center to get an identification card. That is possible because the infrastructure proposed include the reporting server, the cooperating payment server, and the certificate authority server. The system also prevents cases and reports being erased and ensures data integrity. The system is also designed to be robust against abusive use and can preclude false reports. The proposed system is able to use an impartial third-party organization to confirm an informer's identity and protect the informer's privacy and security (Shih et al., 2019).

4.1.1 Data mining tools, real-time big data analytic tools, cloud-based big data analytic tools and cloud computing

After the data is collected by the sensors, it needs to be transformed into manageable sizes to extract useful information. That could be done by data mining tools, real-time big data analytic tools, and cloud-based big data analytic tools, such as MapReduce, Storm and BigTable (Atat et al., 2018).

MapReduce is a programming model that can process big data in parallel on multiple nodes, it uses mapping and reducing, dividing tasks into small parts and assigns them to many computers. The results are collected at one place and integrated to form the result dataset. Storm is a distributed real-time big data-processing system. BigTable is a database system developed by Google, it is a scalable NoSQL[14] database system that works on distributed cluster systems. There are several papers about that and other tools intending to deal with big data, as well as its applications and use cases.

[14] Umbrella term representing non-relational databases that provide a mechanism for storing and retrieving data distinct from tabular relationships in relational databases.

Big data is a collection of large datasets that cannot be processed using traditional computing techniques. Intending to deal with the large amount of data, the cloud computing is a big part of the equation, in the means that facilitates the storage, processing, management, and also applying analytics on the sensing data from citizens. The cloud computing model provides availability of virtually storage and processing capabilities, enabling to deal with the big data. The cloud-based platform shown in Tzay-Farn Shih et al. (2019) is an example of the use of the cloud computing applied for PPDR purpose.

According to the National Institute of Standards & Technology (NIST), a US Government entity that formally defines standards: "cloud computing is a model for enabling ubiquitous, convenient, on demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" (Mell & Grance, 2011). According to Atat et al. (2018, p. 73610),

> Integrating cloud computing in IoT can take the processing of sensing data streams to the next level to provide ubiquitous sensing services beyond the capacities of individual things. When combined with artificial intelligence, machine learning, and neuromorphic computing techniques, it is envisioned that new applications will be developed with automated decision-making, which would revolutionize the field of smart cities, industrial plants, environmental monitoring and others.

The cloud computing offers the parallel processing of the data chunks on dedicated servers, MapReduce tool proposed by Google is an example of parallel processing. Despite MapReduce offers advantages over conventional processing methods, it is not very effective to handle a large amount of data because of factors as scalability, latency and availability. Another solution is processing on cloud centers as a service, which offers users to rent computing and storage resources in a pay-as-you-go manner, where, even with users sharing a common hardware, the machine virtualization appears exclusive to them (Atat et al., 2018). Another import concept related to cloud computing is Cloudlets, which are a small-scale cloud data center, located at the edge, closer to the users, intending to increase the response time of applications by reducing latency (Marinescu, 2018).

Meanwhile, the high data traffic driven by network users using resources as mobile video and social media applications demands high use of mobile network operators. That demands new solutions to improve backhaul resources to be able to deal with big data environment. The current approaches to cope with the enormous data volume are rather than caching data from the cloud, performing the caching at the edge of the mobile networks.

In Mkhwanazi et al. (2020) there is a proposal of a platform intending to be a crime reporting system with identity protection, but for that, the authors use devices at the Edge. The paper proposes an automatic crime reporting and immediate response system based on

system integration combining Raspberry Pi[15] (installed in police vehicles and capable to display crime details such as type of crime and location); Microsoft IoT; mobile application; and web application. The platform intending to reduce the unreported crime due several problems in poor countries as, no law enforcement in the region, or people being scared to reveal their identity to the police, or lack of evidence to help the police. The goal is to assist informers to report crimes and providing some evidence about crimes to the police, as audio recordings or photos, anonymously, by using their mobile phones. Their identities must be protected and encrypted. Another goal is to help the police providing data about crime and allowing the information to reach the dispatch center.

According to the authors, the approximate time for a user reporting crime is 3 up to 4 seconds, the report reaches the dispatch center in less than 30 seconds, and the approximate time for police to retrieved crime report details is 4 seconds. The dispatch center should validate the information and send back to the police vehicle that will be able to view the crime details. When someone report a crime, the system checks the police around the area where the crime is being reported and send the crime details, as coordinates, to the Raspberry Pi in police vehicle. The system also does some calculation about vehicles distance and crime location to allocate the nearby vehicles to the occurrence (Mkhwanazi et al., 2020).

4.1.2 CPS Big Data Caching - Mobile Edge Computing

Edge Computing distributes computing functions between cloud and network edges. According to IBM (2022), "edge computing is a distributed computing framework that brings enterprise applications closer to data sources such as IoT devices or local edge servers. This proximity to data at its source can deliver strong business benefits, including faster insights, improved response times and better bandwidth availability".

The concept of Mobile Edge Computing (MEC) is a key factor in enhancing the QoS, by reducing core network traffic, and ensuring that services follow the mobility of users. Allowing data to be access anytime, anywhere with reduced latency. MEC reforms the cloud hierarchy by pushing computing resources in the proximity of users, reducing traffic bottleneck towards the core network (Taleb et al., 2017). The term MEC was standardized by European Telecommunications Standards Institute (ETSI), according to ETSI, MEC is defined as "Mobile edge computing provides an Information Technology (IT) service environment and cloud computing capabilities at the edge of the mobile network, within the Radio Access Network (RAN) and in close proximity to mobile subscribers" (Hu et al., 2015, p. 4).

In Abbas et al. (2018), it is possible to see an overview of the relevant research and technological developments in the area of MEC in last years. The authors pointed out that

[15] Low-cost minicomputer with the size of a credit card, interoperable with input and output hardware devices.

video analytics can be used in surveillance cameras for same applications in disaster and security matters, such as, detect car accident, and face recognition to identify someone that commits a crime, transferring his photograph to intelligent cameras to trace his steps. Also presented ocean monitoring researching to cope with any ocean incident in advance, for example, a tsunami.

> Implementing MEC near the mobile devices can elevate big data analytics with the help of network high bandwidth and low latency. For example, instead of using the typical path from an edge device to the core network, big data can be collected and analyzed at the nearest MEC environment. The result of big data analytics can then be passed to the core network for further processing. This scenario will perhaps also accommodate data coming from several IoT devices for big data analytics (Abbas et al., 2018, p. 455).

MEC are translated in geo-distributed servers or virtual servers, that could be deployed through 5G, 4G or a multi technology (2G/3G/4G/5G) base stations, installed at places with high mobile users premises, as big commercial centers, using MNOs elements as small cells, femto cells, and base stations. Small cells and femto cells are solutions developed to cover small radius with high throughput, enhancing QoS and Quality of Experience (QoE).

The MEC approach allows intelligent services at nearby locations to the mobile users, reducing latency. Which makes possible the use of latency-sensitive applications, as augmented reality, and also, release backhaul processing, as the use of contextual information to predict users´ behavior, making the right content closer to the users, allowing computation offloading. Meaning, migrating computing tasks to servers in different areas.

According to Zeydan et al. (2016, p. 36), the major challenge for backhaul network is wireless video on demand traffic, due the fact that users access contents in asynchronous way (different from TV), whenever they wanted. The data traffic streaming from diverse domains also meets the big data framework, and the 5G network characteristics can help to deal with big data. In that sense, the MNOs are designing user-centric networks, with decentralized and flexible network architectures where "big data brings about a new kind of information set to network planning which can be interconnected to get a better understanding of users' behavior and network characteristics (location, user velocity, social geo-data, etc.)".

An experiment conducted in Turkey, in an MNO with 17 million subscribers, with data collected from several base stations in hours of time intervals, showed that human behavior is highly predictable, and that a proactive caching at the edge architecture of the 5G network, using data analytics and Machine Learning (ML) tools to content popularity estimation, can optimize the network (Zeydan et al., 2016).

The MEC or fog computing allows the RAN to play roles that in the earlier networks, as 2G and 3G, was just possible by the centralized database. With 4G and 5G it is possible the edge processing over wireless networks, providing a better user experience. In 5G, with

characteristics as incorporates SDN; Network slicing; and NFV, virtualizing controllers to support new services, the RAN can carry out storage, control and processing as an edge approach, through distributed cloud computing capabilities near to the base stations. That could make sense in places with high data traffic, allowing data to be closer to users, improving the user experience in 5G compared with 4G.

Although, for that approach have a good efficiency is necessary that the right content to the users is at the edge. Engin Zeydan et al. (2016) proposed a solution to predict users´ spatial-temporal demand through a Hadoop-based big data processing platform. Intending to improve users' QoE by latency reduction, the authors proposed collecting contextual information, as location information, and user's viewing history, to analyze users' behavior from enormous amounts of streaming data, and exploiting proactively caching strategic contents at the edge. For PPDR response, according to Zahid et al. (2019, p. 619):

> (...) the need for reliability, availability, and security of information has forced us to provide out-of-the-box solutions. To reduce the burden of computing on the cloud, the concept of edge computing and fog computing has been extended. This concept provides a way to distribute some of the computing functions to the edge of the network where most of the data originates and is consumed, which is the case with many critical incidents related to Public Safety operation.

Intending to predict visitor distribution for large events, Violos et al. (2019) examines two sets of supervised ML techniques to predict the visitors' distribution. The authors evaluated the analysis using real data from a large music event, with 300,000 visitors over the whole weekend, the Das Fest music festival, that takes place every year in Karlsruhe, Germany. To enrich the prediction, they also used and evaluate open data such as the weather and the popularity of artists. To collect data, IoT devices were installed in the festival area, and a mobile application providing useful information were offered to the visitors.

Despite mobility prediction techniques for next time steps have long been exploited by using probability distributions of the next move, according to Violos et al. (2019), Markov chains and Lyapunov optimization method are not suitable in the context of large events, since "they operate based on a predefined set of visitors in the area of interest. However, visitors may come and go at any time". The paper proposed the use of ML techniques, which reduces the problem into classification and regression tasks, intending to predict, for each point of interest, how the visitors will behavior. According to the authors, fog architecture can cover many needs of the large events as, estimate the current number and the distribution of people in a certain area. The data from fog architecture can also be combined with open data to enrich the predicting models. In the applied case, were used IoT devices placed in the environment, with a signal strength indicator sensor connected to a Raspberry Pi.

The prediction of visitors' distribution in the next time steps could also help the PPDR agencies in big events as Olympic Games and Football World Cup. In big events the PPDR agencies should have contingency plans for crisis situations, such as an evacuation or other emergency scenario. That also shows the complexity of PPDR operations, since for that user case the mobility prediction techniques largely used by mobile and wireless networks could be not suitable, being necessary to analyze each applied case. Big events have certain type of requirements as zero delay tolerance, and large population density. In that sense, Cui et al. (2022) explorers how the integration of 5G technology, big data analysis, artificial intelligence and intelligent monitoring equipment can help in the security of big events.

Zahid et al. (2019) proposes a model of computation and communication for PS network based on the integration of fog/edge computing, IoT, and the FirstNet network, through a platform for highly qualified people in training and researchers, intending to develop and test their ongoing research work. The authors created a test-bed scenario using cellular and trunked-radio networks, performing experiments using Wi-Fi access points/routers to configure the communication between various nodes, each sensor supported by computing devices like ESP32[16] and Raspberry Pi Zero, with computing capacity to process information as video processing. The goal is to extract useful information from data collected to help the managers of PPDR agencies to act in incident situations based on data science supporting the decision-making process. The test-bed scenario uses Raspberry Pi 3 as the fog/edge node receiving data from the sensor nodes with Raspberry Pi Zero, performing edge computation as data formatting and, through MNOs, reached the CCC providing situation analysis.

According to Zahid et al. (2019), in FirstNet there are four building blocks connected to each other enabling data changing between FirstNet, access points, cellular network, and Internet. The first block is composed by remote controlled sensors as drones; the second block is composed by the EFRs using smart devices as smartphones; the third block is the CCC, which are connected to PPDR agencies vehicles through FirstNet radio communicator (over LMR or 4G network or dual-mode radio).

The CCC must also be aware of crises situations in real-time; operated data collection/analysis tools to help in the decision-making process about actions that should be performed in such situations; and have access to relevant data basis to help the decisions. The last block is the data center that received and process information from the other blocks and contains relevant information capable to help the EFRs on site incidents, also provides cloud computing resources (Zahid et al., 2019).

For that infrastructure the major challenges are designing required applications for edge nodes intending to achieve good performance related to reliability, security and

[16] ESP32 is a low-cost, low-power microcontroller with an integrated Wi-Fi in some models, and Bluetooth.

interoperability, pointing out that security mechanisms and processing off-loading from cloud to command centers is a challenge that will require to the researchers' additional efforts. The hierarchy of distributed computing is another challenge. The idea is to use separating nodes, some to be deployed at the disaster location and some to be employed at the CCC, having distributed processing in three levels, disaster location, CCC and the cloud. That separation levels suits the operational environment that involves multiple PPDR agencies, since all of them have their own edge nodes on disaster location, and should converge to the CCC or cloud, depending upon the type of operation (Zahid et al., 2019).

4.1.3 CPS Big Data Communication

Big data consists of a large and complex data set generated by sensors and crowd-sensing, and may be structured or nonstructured, in which, through data analytics tools, useful information could be used to different segments. Capturing real-time conditions from big data in a massive high-density environment could be a challenge, since data collections and transmissions have different flows of information and characteristics. Some communications can be done by the terminals, dealing with big data as Machine-Type Communications (MTC) and Device-to-Device (D2D) communications, intending to accelerate the speed of big data delivery. For MC purposes that are also called mission-critical MTC (mcMTC), with requirements as low latency, ultra-reliability, and availability. Mohammed et al. (2019) presents a review of mcMTC on 5G technologies, highlighting challenges, requirements and future aspects.

MTC or Machine to Machine Communication (M2M) is a technology defined by 3GPP (3GPP, 2021), that allows communication between machines used, for example, by IoT devices. Vehicle to Everything (V2X) communication is a type of MTC. About standardization, oneM2M (2022) is a global initiative, a 3GPP Interworking project, that develops open standards for IoT intending to provide a unique architecture for M2M interoperability, as a special form of M2M/IoT platform.

About use cases of M2M dealing with big data in a PPDR scenario, in Kunz et al. (2018) is presented some development on M2M platform with Cellular IoT (CIoT), considering a traffic accident data collection scenario using V2X communication. The authors discuss how that platform can be adopted in 5G networks. When an accident occurs, the vehicle reports the accident to oneM2M platform through a wireless network or Dedicated Short Range Communication (DSRC) to a fixed infrastructure installed on roads, called Road Side Unit (RSU). Then the RSU send the data to the oneM2M platform. The authors suggested an M2M device, Intelligent Transportation System - Station (ITS-S), to be installed in the vehicles, with computing capabilities to collect and send the information.

The platform validates the accident and send the information to the dispatch center. The EFR can demand more data from the accident through oneM2M platform in communication

with the vehicle, and other entities within the accident as other vehicles, fixed infrastructures or pedestrian's devices. The integration of oneM2M as an M2M/IoT platform and 5G CIoT for V2X services could speed up the action of the EFR in crises situations, and provides on-site real time information, without demanding much network traffic, since the most part of the big data was handled by M2M platform. That could be also useful in big events, with IoT applications sending data to the platform, or using the Group Management (GMG), also defined by oneM2M, with the function of handling Group related IoT/M2M services, with features definition as creation of a group and management of group members (Kunz et al., 2018).

The M2M communication running over MNO 4G and 5G, allowing the networks to provide new services, although, bring complexity to the networks, as excessive signaling traffic at the network. Intending to deal with that challenge, several papers, such as Wu and Mastronarde (2018), suggest offloading the MTC traffic onto device-to-device (D2D) communications links, also a communication type 3GPP defined for 4G and 5G (3GPP, 2018). That could solve part of the problem when the devices are close to each other. That type of communications can accelerate the speed of big data delivery, specially, when used together with SDN, which allows the separation of control and data planes.

4.1.4 Big Data Analytics

Big data analytics is a process of extracting meaningful information from raw data, as the application of analytics on the sensing data, intending to solve the challenge of analyze the collected data, and build the knowledge base to provide the ability to respond to the emergency situations with intelligence. There are three main methods of big data analytics, namely data mining, real-time big data analytics, and cloud-based big data analytics.

The process of extracting useful information from big data is referred as data mining. But before data mining is applied to the data, is necessary to reduce data complexity to facilitate the data mining process as dimensional reduction, neural network, Knowledge Discovery in Databases (KDD), and techniques as clustering, classification and frequent pattern. Clustering, for example, aloud the nodes to exchange information between each other, intending to identify whether the information should be grouped, depending on the needs of the IoT applications, such as in smart homes. Hadoop is an example of open-source tool used for data mining, which uses MapReduce as framework (Atat et al., 2018).

Real-time analytics is the production of useful information from real-time streams data. Before real-time analytics be applied, the real-time streams need to be converted into a structured form data. Hadoop is also an example of real-time analytics tool, Storm is another example, according to Atat et al. (2018) compared with Hadoop, Storm is easier to operate and more scalable.

In Toure (2017), a real time terrorism data collection system is proposed to predict terrorist incidents and help the agencies to define counter-terrorism measures. The proposal includes terrorism data summarization to better analyze root cause analysis; cluster analysis of terrorist attacks intending to find groups with similar patterns; a risk model that uses data collected; and a prediction method that uses the risk model proposed and Markov Chains.

Twitter or social media data can also be used in a real-time analysis to provide useful information for PPDR agencies, as proposed by Xu et al. (2016) and Xie and Yang (2018), collecting data from Weibo social media (a Chinese microblogging website). Mohler and Brantingham (2018) provide a framework for deploying predictive crime models based upon crowdsourced including information from a social media network, Nextdoor (PS posts in Indianapolis, EUA). A real-time crime model is maintained on a server, when a user reports a crime in the social media, the user's post is categorized, and model parameters are updated.

Jilani et al. (2019) propose a solution based on real-time information capture from the Citizens Emergency Response Portal System (CERPS), developed to employ crowdsourcing while using social media. Other applications that can be used for PPDR purposes are real-time or near real-time big data analysis architecture, for vehicular networks and big data video analysis. To have a better understanding of the real-time data and help in the decision-making process, the representative form of the data is an important part of the process, that could be facilitated by tools as GIS.

Cloud-based Big Data analytics is a scalable architecture to perform analytics on big data imported from the cloud. Yetis et al. (2016) demonstrated the use of cloud computing big data analytics using Map-Reduce approach, to store and visualize the crime incidents that happened in the City of Austin. Resulting the most occurred crime type in the city, the address with the highest number of crime incident, the amount of crime incidents, and the most happened crime for that address. The big data were obtained from the official page (https:// data.austintexas.gov) of the historical crime data made available by law enforcement to public. The paper intending to decrease the complexity to handle the huge amount of data from these databases about crimes and helping in the prevention of crimes by modeling the results. Google's cloud computing platform is the most popular tool for cloud-based big data analytics, consists of Google File System (GFS), a distributed file system for big data storage; BigTable, for big data management; and MapReduce for cloud computing.

4.1.5 Security issues

About cloud-based solutions for PPDR purposes, while data storage in the cloud offers several advantages as availability and scalability, it increases the chances of malicious attacks as well as the concerns about leakage of private data and sensitive information disclosure, since the cloud operators can access this information; there is also the risk of unauthorized access. These

concerns leading to questions about the feasibility of cloud data storage uses for governmental agencies, especially in PS affairs.

There are several papers about security and privacy issues of cloud computing, fog computing, and in M2M communications. The security solutions for cloud computing may not be directly applicable to fog computing, as the fog devices are located at the edge of the networks, leading, for example, to and Man-in-the Middle attacks and wireless attacks as jamming. About end users, the leakage of private data is the biggest concern.

There are different security solutions proposed for big data storage, access and analytics as, first splits files into encrypted parts and store it in distributed cloud servers (Gai et al., 2016); classifying data according to privacy level and determine whether data packages can be encrypted under the timing constraints (Gai et al., 2021); secure data transfer schemes, additional authentication, access control strategies (Xu et al., 2019); identity privacy-preserving public auditing mechanism for cloud-based data to guarantee the integrity (Zhang et al., 2021).

Yang et al. (2020) made a review of the literature on data security and privacy issues, data encryption technology, and applicable countermeasures in cloud storage system, summarizing data encryption technologies and protection methods. This paper can be used as a reference to have a better understanding on cloud storage, requirements of data security and privacy protection in cloud storage, and data security for cloud storage.

Blockchain techniques can also improve data integrity, helping mechanism to resist against malicious auditors (Zhang et al., 2021). Machine Learning (ML) can also improve the security solutions by automating many security-related tasks through the process of training datasets, that could allow the detection of future security anomalies (Zhang et al., 2021). Below is describing one application of ML in PS and some issues about it.

> (...) the joint data analysis of the Department of transportation and the Department of public security is also conducive to reducing the occurrence therefore, the combination of ML and cloud has become a new focus. But now there are two problems: 1) departments that do not trust each other may refuse to share data in order to protect their own data security. 2) In the face of massive cloud data, users with limited resources may not be able to carry out effective data mining and model training because of the high cost of computing and communication. Outsourced the model training calculation to the cloud will increase the risk of leakage of key parameters of its own model (Yang et al., 2020, p. 131736).

There are some researches on cloud based ML with security and privacy focus as Zhou et al. (2021), that proposed a neural network privacy training scheme with homomorphic encryption scheme to protect the privacy of data, and Hassan et al. (2019), that presents a privacy-preserving ML scheme for multiple data providers. Although, according to Yang et al. (2020, p. 131736), that made a review on the data security and privacy protection for cloud storage, the efficiency and security of these programs are not satisfactory. The authors pointed out two research directions in that field for the future:

> 1) Design a more secure privacy protection scheme to ensure that sensitive information in shared data is hidden, especially data involving highly sensitive information such as government data and medical data. 2) Design efficient and secure outsourced privacy protection scheme to support more machine learning algorithms (such as incremental learning).

The use of appropriated methods and techniques can improve the security in terms of data confidentiality, integrity and availability, access control, data sharing, leakage of data, data deletion and privacy protection, as demonstrated in the security analysis of some papers (Zhang et al., 2021; Xu et al., 2019; Yang et al., 2020; Gai et al., 2021). Nevertheless, "a single security solution is not sufficient to ensure a robust system against attackers. It is quite necessary to incorporate different strategies to face security flaws that stem from poor systems designs" (Atat et al., 2018, p. 73619). Combining different techniques appears to be the best solution, being necessary to evaluate for each applied case.

4.1.6 Predicting disaster

According to the Economic and Social Commission for Asia and the Pacific (ESCAP),

> Disaster resilience can also benefit from rapid advances in technology. Even the poorest countries can be empowered by smart digital technologies. Artificial intelligence and big data techniques, for example, can build a live picture of rapidly developing events by merging satellite imagery with data from mobile phones. At the same time, digital identity systems can offer more ways to deliver essential social protection services, before, during and after disasters (ESCAP, 2019, p. 4).

The data that could help to predict disaster is often unstructured, for this, the use of ML can improve management disaster system. According to Chamola et al. (2020), ML is an application of AI to make further predictions using algorithms working on characteristics of available data. "The accurate prediction of a disaster lies in analyzing spatial and temporal data of an area and predicting the characteristics of a disaster" (Chamola et al., 2020, p. 4) that could be the rise in water level that could lead to a flood, the magnitude of an earthquake, etc.

The data collected by IoT devices can be process by ML algorithms to provide greater accuracy in disaster prediction. In Anbarasan et al. (2020), ML is used for the detection of flood disaster, based on IoT, Big Data and Convolutional Deep Neural Network (CDNN). The input data are taken from Big Data, the repeated data are reduced by using Hadoop Distributed File System (HDFS) map-reduce, then the rules are generated based on a combination of attributes. The last stage is using the CDNN classifier to verify the chances for the occurrence of flooding. The proposed method utilizes as input the Next-Generation Radar (NEXRAD), together with National Oceanic and Atmospheric Administration (NOAA), constituting a group of weather radars to detect winds and atmospheric precipitation.

A variety of IoT systems can be used to predict disasters, e.g., Internet of Underwater Things (IoUT), which is able to sense locations in the underwater environment, process the data locally, and transmit data via underwater wireless communication, as described by Coutinho et al. (2020). The paper discusses how IoUT can help humanitarian needs in mitigating disasters. The Early Warning Systems (EWS) makes use of data for predicting emergency situations using Emergency Management Information System (EMIS), providing real-time information to the EFRs, Emergency Alert Service (EAS) and to the population. To provide early warning information, communication and cooperation are required in different levels, such as regional, national and global, which can be facilitated using integrated ICTs (Mohan & Mittal, 2020).

A survey of disaster and pandemic management using ML is shown in Chamola et al. (2020), where it could be found reference for articles using IoT and ML-based models for disaster prediction as flood, rainfall, tropical cyclone intensity, sandstorm, storm intensity, fire outbreaks in forests, among others in different cities applications. Using a variety of ML technology, and a variety of type of sensors as remote sensing, android based sensors, satellite, IoT and UAVs. Sensors installed in offices, homes, or other public places as for heat, smoke and radiation, can also be used for detection. With accurate information early signals can be delivered to the population at the right time, avoiding causalities.

The use of Unmanned Aerial Vehicle (UAV)s solves the accessibility in areas that are difficult to reach and monitor, and have been used to capture images, mapping real-time data and monitoring nearby activities. In Yim et al. (2017), a Smart-Eye platform, that detects disasters (e.g., forest fire, flood) is proposed, using UAV equipped with a camera, and multiple sensors to monitor the disasters in real time. The UAV uses LTE to communicate with Smart-eye center, and image stitching technology comparing real-time images with the previous images of an area. The UAV monitoring by using Closed-Circuit Television (CCTV) cameras, which makes the solution much cheaper than those of satellites. In Chamola et al. (2020) are presented solutions using UAVs to help in disaster prevention and during disaster.

The cameras can be used during disaster, as proposed in Wei and Sheng (2019), using video surveillance images. The authors propose an image quality-based framework to improve the performance of those cameras, then, design an urban intelligent emergency system, analyzing emergency evacuation of a social group for data acquisition. Then, treating the data using image quality assessment and convolution neural network, and classifying the dataset. Which makes possible to obtain evacuation parameters and improves the timeliness of information transmission in the evacuation process.

Crowd evacuation is also discussed in Wang et al. (2019), where a reinforcement learning method is introduced for crowd evacuation improvement and assistant decision support. There are a variety of papers about applications of ML models in crowd evacuation, find a safe zone route, and evacuation route planning in various scenarios as avalanches, earthquakes, hurricanes, fire hazard, fire outbreak, as listed by Chamola et al. (2020). Fang et al. (2021)

investigate the IoT applications in building fire evacuation, which increase the evacuation by making decisions of escape routes based on the real-time fire information.

Although, the use of cameras for collecting data for crowd evacuation affects people's privacy. In that sense, the solutions should analyze and processing information without the risk of violated public's privacy, being criterions about cameras solutions, or using other solutions in order to avoid privacy issues, as using radio waves of a user's smartphone, instead images from cameras, as proposed by Shibata and Yamamoto (2019), measuring the strength of waves by sensors to estimate crowd density by utilizing ML techniques.

Using ML techniques there is also numerous researches about post-disaster management, to calculate the losses, minimize future disaster risk, and plan measures for the recovery of the area affected by the disaster, as the one used in 2010 Haiti earthquake for detection of urban damage using remote sensing and ML algorithms (Cooner et al., 2016). Also, the one proposed by Sublime and Kalinicheva (2019), using the 2011 tsunami in Tohoku as a case study, to evaluate the extent and the severity of the damages. The solution analyzed satellite images taken before and after the tsunami and applied an unsupervised deep neural network to detect non-trivial changes in images, and process to detect areas of interest such as flooded zones. Also, works collecting information about survivors, highlighting areas with risk, identifying tweets that could be helpful is post-disaster situations, and so on, using sensing as remote sensing, social media and UAVs, as listed by Chamola et al. (2020).

In Ahmed et al. (2019) a disaster response system based on IoT and D2D using 5G networks is proposed, resulting in increasing responsiveness, resilience, reliability and scalability. Qadir et al. (2021) examines UAVs path planning and 5G communications addressing disasters in Smart Cities, concluding that the most research cases are related to post-disaster solutions and use conventional and learning-based algorithms with applications to localize victims and optimize routes. An IoT-powered UAV-based Smart City management system is also recommended, where all the Smart City key components are integrated to address disasters.

From the papers review it can be understood that predicting a disaster, delivering early signals, determining crowd evacuation routes, calculate the losses, minimize future disaster risk, and plan recovery measures for the area affected, are all phases in a disaster event. Where, big data collected from a variety of sensors, and ML algorithms to process data and delivery results, can be used to overcome issues and improve the emergency management system. Although, privacy issues should be observed when collect public data.

4.1.7 Predictive policing and bias issues

One of the biggest concerns about the use of crowd-sourced information, combined with artificial intelligence, is the algorithmic bias in predictive policing models. Lum and Isaac (2016)

discuss the predictive policing systems, based on an analysis of geographic location and arrest data, the predictive big data systems, used by law enforcement to try to prevent crime before it occurs. The authors consider the social consequences when these systems are trained using biased data and pointed out some concerns as:

> the apparent conflict with protections against unlawful search and seizure and the concept of reasonable suspicion; the lack of transparency from both police departments and private firms regarding how predictive policing models are built; how departments utilize their data; and whether the programs unnecessarily target specific groups more than others. But there is also the concern that police-recorded data sets are rife with systematic bias (Lum & Isaac, 2016, p. 14).

Predictive policing is defined as "the application of analytical techniques – particularly quantitative techniques – to identify likely targets for police intervention and prevent crime or solve past crimes by making statistical predictions" (Perry et al., 2013, p. 16). Police departments in many countries are increasingly utilizing software to identify future offenders and forecast criminal activity and future crimes.

The predictive policing software are designed to learn from big data and reproduce patterns, the problem arises when the biased data is used to train the predictive models, resulting in discriminatory policing. The use of crowd-sourced information combined with police database could not result in a good prediction base, since decades of criminological research already prove that police databases are not a census of criminal records, and nether a representative random sample, and also, many researchers believe that reported crime data are contaminated by measurement error (Levitt, 1998; Lum & Isaac, 2016).

The debate about the trustiness, effectiveness and usefulness of reported crime statistics is old and broadly discussed in scientific field as in Wellford and Wiatrowksi (1975), Sellin et al. (1964), and Kitsuse and Cicourel (1963). In the book The Measurement of Delinquency, Wellford and Wiatrowksi (1975) furthered the understanding of the qualitative elements in criminal behavior, establishing a theory and research model with a measure of offense seriousness. That stimulated many researchers to follow theirs steps for the development of a science of behavior based on reported crime statistics.

Prediction models of crimes are also old, since Lombroso (2013) in 1876 already tried to construct a model based on the prison population, the new factor nowadays is the technological capability, artificial intelligence, ML and the system integration between big data, police database, and communication technologies. Which could reproduce and amplify same biases, resulting in ineffective predictive models, and discriminatory policing, as the Lombroso model already did in the past, in other words:

> If police focus attention on certain ethnic groups and certain neighborhoods, it is likely that police records will systematically over-represent those groups and neighborhoods. That is,

crimes that occur in locations frequented by police are more likely to appear in the database simply because that is where the police are patrolling (Lum & Isaac, 2016, p. 15).

To address that problem, the algorithm should have some transparency, allowing for some external auditing. Mohler and Brantingham (2018) attempt to make predictive policing source code open, providing a framework for deploying predictive crime models based upon crowd-sourced information, with a high level of algorithmic transparency.

4.1.8 Summary

To summarize, the CPS data collection and processing can be speeded up through cloud computing with the parallel processing and execution of tasks and queries. Caching at the edge, distributing the processing and caching execution tasks, using cloudlets whenever possible, is another strategy for a better workflows processing. Figure 21 summarizes the topics addressed in that section, showing a panorama of Cyber-Physical Systems for PPDR purposes in a Smart Community.

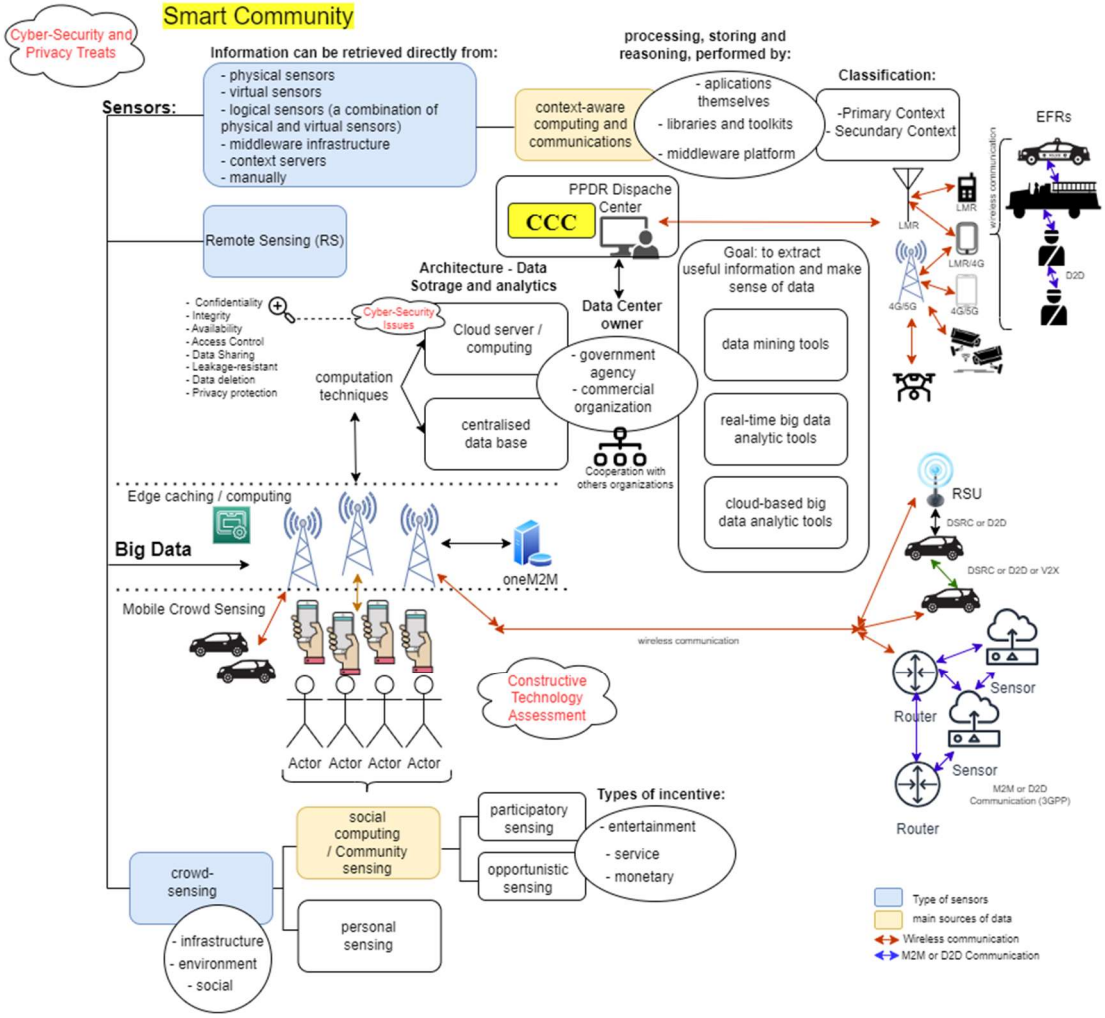


Figure 21 - Panorama of Cyber-Physical Systems for PPDR purposes (Author).

Transforming the data in manageable sizes in an efficient way can help to deal with big data. Also, methods of big data analytics are used to accelerate the processing and optimizing the information extraction from big data. At the CPS devices side, the use of M2M and D2D communication can help to deal with the enormous communications made by the devices to the network, reducing latency and accelerate data delivery.

Security and privacy issues are the biggest concerns in cloud computing, fog computing, M2M communications and at user side, with the possibility of private information leakage. Predictive policing is another concern, since the software are designed to learn from big data analysis and reproduce patterns, if biased data is used to train the predictive models, the result is discriminatory policing.

Despite all the solutions found in the literature, according to Wu et al. (2020), most of available IoT protocols cannot achieve the low latency required by MCC and two emerging IoT standards, IEEE1451 and IEEE P2668 can contribute to achieve those requirements, also, the 5G, especially URLLC, mMTC and eMBB presents as an alternative for MCC applications.

4.2 Smart Safety for Smart Cities

Smart cities emerge as a result of technological evolution, directly related to the growing of computational capacity of new technologies. This allows the integration of ICTs in the planning and management actions of cities, providing social innovation, related to sustainable urban development models, based on real and current data from urban spaces, and the people who use these spaces. For example, traffic management according to current data, garbage collection management, among others. In addition, the term Smart Cities is also related to the logic of an innovative and inclusive city, through citizen participation in urban management.

Despite all definitions about Smart City, there is still confusion about what a Smart City is, as shown in Guo et al. (2019), that pointed out several similar terms that have being used as intelligent city, digital city, cyber city, global city, e-city. The paper also provides a bibliometric analysis on smart cities research, that could assist researchers about the characteristics of smart cities researches, the paper also diagnosis that the label Smart City is a diffuse concept and not always used consistently, according to Guo et al. (2019, p. 2):

> Those complex definitions of a smart city could be categorized into two mainstream approaches: 1) technology domains such as the Internet of Things (IoT) and big data which has matured enough to make smart cities efficient and responsive and allowed smart cities to emerge. The technologies enabled buildings, energy grids, natural resources, water management, waste management, mobility, and logistics worldwide to become 'smart'; 2) people-oriented approach including soft factors such as participation, education, culture, policy innovations, social inclusion, government, safety, and cultural heritage.

In Guo et al. (2019) the terms "Safe City", "Safe Cities", and "City Safety" were not used at the systematic review as a synonym for Smart City. Despite not appearing at the Guo et al. (2019) bibliometric analysis, the terms appear on websites of software and hardware equipment manufacturers for CCC (HEXAGON, 2022; AxxonSoft, 2022; AEL Sistemas, 2022), and government websites (The Punjab Safe Cities Authority, 2022), referring to technologies used by PPDR agencies for Smart City scenarios, as cameras, and police surveillance tools based on big data and artificial intelligence (Tréguer, 2019). In Marseille, France, the term used is "Observatoire de la tranquillité publique", Observatory of public tranquility.

The term "Smart Safety for Smart Cities" is used in Marabissi et al. (2019), which describes the 5G field trial environment that was launched in Italy at the end of 2017, in the city of L'Aquila. The term refers to 5G use case to PS services as information system for police, and alert and management systems for disaster. According to the authors, through the use of equipment as smart glasses connected to the 5G network, and remote-controlled drones with cameras by the EFRs, the goal of "Smart Safety for Smart Cities" is:

> to ensure a greater level of safety for citizens by using innovative technologies that allow security forces to immediately determine the emergency status of an event and to simplify/optimize coordination and intervention activities. (...) in order to offer the best support for effective decision-making in the management of citizens' safety, in emergency and danger situations as well as in daily operations (Marabissi et al., 2019, p. 10).

The term "Smart City Public Safety Emergency Management" (Wang & Li, 2021, p. 169) was also found in the literature review, referring to cities that make full use of Internet, IoT, Cloud Computing and system integration in a Smart City scenario, allowing the emergency management system to play a positive role in urban safety governance. As shown in Wang and Li (2021), comparing the number of criminal cases in China from 2006 to 2012, before the implementation of a Smart City pilot, with data from 2013 to 2019, the criminality after the implementation showed a decreasing trend.

It can be inferred from the SLR that Smart City Public Safety Emergency Management refers to systems used for both applications: emergencies such as disasters, and Public Security, which is also referred simply as Smart City. Whereas "Safe City" is a term used for systems that aim only at Public Security, it is commonly used in manufacturer webpages, but not in scientific studies. This research uses the definition of ITU (2015) for Smart City:

> A smart sustainable city is an innovative city that uses information and communication technologies (ICTs) and other means to improve quality of life, efficiency of urban operation and services, and competitiveness, while ensuring that it meets the needs of present and future generations with respect to economic, social, environmental as well as cultural aspects.

This research is interested in the use of the Smart Cities concept in relation to the performance of PPDR agencies, and the impact of this on society, turning attention to social innovation, "understood as an innovative practice with the objective of creating a positive impact for society as wide as possible" (Bencadirno & Greco, 2014, p. 39).

About Safe City, according to The Punjab Safe Cities Authority (PSCA, 2022), "the Safe City is a concept for returning security and quality of life to today's complex cities through the use of technology, infrastructure, personnel and processes". According to Tréguer (2019), the Safe City is supported by technological innovations that make possible gathering and analyzing different sets of data, such as police files, personal information — mainly on social networks — etc., to produce statistics and help in decision-making according to the logic of preventive police. In the literature is possible to also find the nomenclature safety systems, referring to surveillance systems as a city management big data application (Atat et al., 2018).

The Punjab safe cities developed an integrated command, control and communication system for PS, with the installation of more than 10,000 cameras for surveillance, providing images for incident and event management, and connected to the analytics systems. The system will be integrated for traffic, being possible to collect traffic offense notices. The traffic police officers using portable terminals can receive that information and act.

In Marseille, France, through a tool developed by the company Engie Ineo, co-financed by France and the European Union (EU), the supervision center collects all available public data, from: municipal police, surveillance camera recordings, information registered by firefighters, etc. This information is analyzed and cross-referenced with other data, such as public transport, Public Health Assistance, meteorology, and major trends in social networks for security purposes. The goal is to better anticipate risks, a "Big Data of public tranquility." It is expected that with ML, the algorithm will learn progressively and bring more relevant analysis, according to the accumulated experience. The Observatory of public tranquility also includes an application for Marseille citizens to report any problems (Legros, 2017).

In many cities the PPDR agencies are already providing LTE UEs to the officers, such as, UEs integrated with crime analysis tools, providing real-time access to intelligence information, thus enabling data-driven patrols, with a significant reduction in response times and violence rates. For example, in Chicago City, which resulted in the 12th District, which faced the main crime challenges, the reduction of 37% in firearms incidents, 64% in murders, 35% in car theft, and 20% in property theft from March to October 2018 (Mayor's Press Office, City of Chicago, 2018). In addition, fewer crimes mean lower cost of crime.[17]

[17] Costs of crime are values of expenditures added to criminality, which can be calculated using different methodologies, such as the accounting methodology, which considers government spending on citizen security; average victims' losses and the probability of victimization; probability of punishment; average length of sentences; and opportunity costs associated with incarceration (IDB. 2017).

Songdo, Republic of Korea, is an example of safe city, where through the connection and integration with various agencies, information about emergencies is collected in real time, such as earthquakes and tsunamis. Information is also collected from emergency rooms in public and private buildings, and from Songdo's U-Crime and U-Disaster Prevention systems. If emergencies are confirmed and it is necessary, for example, to inform citizens for an evacuation, the information is transmitted to people through images, internet, applications and sound warnings. For crime prevention, various devices are used, such as CCTV, warning lights, emergency alarms, loudspeakers, fixed cameras and sound detectors at various points installed in the city, such as schools and shopping centers, all connected to the CCC (Lee et al., 2016).

For actions against crime, there are cameras installed at the main intersections of Songdo, loaded with Automatic Number Plate Recognition (ANPR), capable of collecting the license plates of the cars and pass by in real time. This information is used to find vehicles classified as wanted, as for being a stolen, and that information is sent to the responsible agencies, such as police, to have a quick response to the situation. Sound detectors scattered around the city also monitor abnormal situations, such as screams in an emergency, where the CCTV cameras immediately change angle to show images of the place to the CCC. With this information the CCC triggers the police officers to act, also making available on their UE the location images in real time (Lee et al., 2016).

Lopez-de-Teruel et al. (2019, p. 1) present the 5G-CAGE, "a project aimed to deploy a city safety solution that enables monitoring and analytics of video streams collected from distributed sources of a Smart City". The solution make use of 5G's low latency; high throughput; and VFN, as the proposed solution called City Object Detection (CODet), allowing the recognition of objects in safety related situations, as vehicles´ license plates, and human faces recognition. The collection of data can be made from distributed visual sensing, as fixed and moving cameras. The solution can process multiple streams in a virtualized ecosystem, combining image processing and computer vision algorithms.

Yang et al. (2022) presents a systematic mapping study which allows categorizing PS as a Smart City scenario for using 5G, among five other scenarios, namely: transportation, healthcare, city tourism, entertainment, and education. According to the authors, in that context, "public safety refers to safety and security to a city (including the citizens living in the city). Examples are security threat from theft, vandalism, looting, and riots, security for events, and anomalies such as smoke and fire". According to Okumura et al. (2018), PS includes services for addressing premeditated crimes, disasters, crowding, suspicious individuals, dangerous articles, and runaway vehicles, using 5G to capture information in real time from high-resolution cameras, then using AI-based face-recognition and image-recognition technologies.

For Rao and Prasad (2018), Smart Cities should address problems such as increasing crime and social unrest. To address those topics, it is necessary to monitor the city, identify locations with problems, and take preventive and corrective actions. This could be facilitated

by the use of video surveillance in streets and public places, followed by intelligent analysis to detect criminal activities and individuals. The authors highlight the need for integrating this data with data received from other sources for comparison and taking quick action. With system integration, crime tracking and detection should enable faster response from PS agencies. This could also be applied to disaster management and emergency response systems, which should be integrated with hospital, ambulance and disaster relief agencies. The authors also point out that the city governance should implement systems to enable residents' active participation and should enable transparency and ease of use in all services — which also include the systems for PPDR purposes.

In Grasic et al. (2018, p. 3) the PS system architecture for Smart Cities in Slovenia, beyond the sensors already explored in previous sections, includes the 112 calls inputs, which is a Public-Safety Answering Point (PSAP), where "the telephone information is considered as information generated by a human sensor". The goal of the paper is to define a classifier for forecasting the number of incoming calls to the 112 system in Ljubljana, capital of Slovenia, using open IoT data for the city for the years 2013 till 2016, intending to construct a prediction module to the system. In the USA, the 911 system also feeds the emergency system.

4.2.1 Human Activity Recognition in Safety System

About Safety System, computer system using deep learning techniques can be used for Human Activity Recognition (HAR) to automatically detect intrusion or violence. There are two types of HAR research, video-based models and sensor-based models (Wang et al., 2019). In Li et al. (2020), the authors proposed techniques to track and recognize human behaviors using an ultrawideband radar. In Yang et al. (2019), the authors proposed an open-set human activity recognition based on micro-Doppler signatures, both are sensor-based model studies. In Chih-YaoMa et al. (2019), the authors explore recognizing human actions in videos.

HAR has relied on visual data for decades and develops rapidly with the help of computer vision. Because of some interference caused by, for example, weather, light condition, walls, and so on, optical sensors are unsuitable for recording activities in the severe environment, for that, radars are suitable, since it is capable to detect objects through the wall and could operate long-distance detection.

> Human activity recognition using radar data aims at automatically recognizing human motions from radar spectrograms. When radar echoes are modulated by human activities, there will be micro-Doppler signatures motivated by micro-movements. Micro-Doppler frequency varies with the velocity of a moving target so that each movement has its unique micro-Doppler signatures, which can be used for activity recognition (Yang et al., 2019, p. 60)

Combining those techniques with deep learning, as present in Du et al. (2020), has achieved significant success in the field of object detection and image classification, which has

been attracted great attention recently, with several papers about the topic. Wang et al. (2019) present a survey in the recent advance of deep learning-based sensor-based activity recognition. Because of the fast development and advancement in that area, and the possible benefits of HAR application in the field of security monitoring, that is a promising use for PS.

4.2.2 Big data in Safety System

For disaster response, the use of big data can improve the accuracy and scientificity of the commanders' emergency decision-making. Some sensors can be triggered into performing actions, such as initiating water spray and firefighting measures when the smoke concentration exceeds a threshold, and the CCC can better allocate the emergency resources according to on-site data reading from sensing techniques, such as, context-aware physical sensors and social sensing. Figure 22 shows an algorithm that demonstrated an emergency management process using big data and IoT.

Also, the application of big data and IoT can help in an incident's recovery phase and in the post investigation of an event's causes, helping the accurate assessment of losses, which leads to the recovery planning and a better understanding of the event for future development trends. Also, it can help the PPDR agencies evaluate the actions taken during the events, checking which measures were good or bad and, based on the acquired knowledge, plan countermeasures for future possible events.

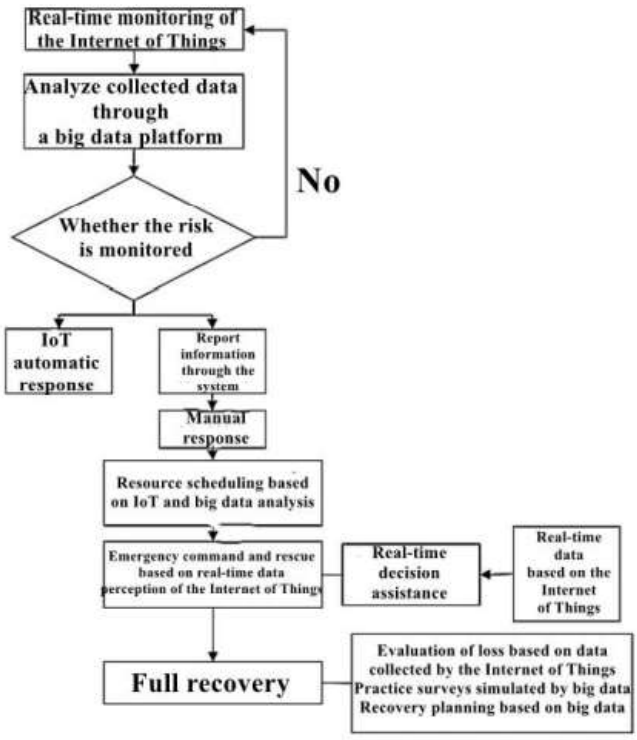


Figure 22 - Emergency Management Process of Big Data and IoT (Wu & Yu, 2020).

4.2.3 Smart resilience for smart cities

The term "smart resilience" is used by ESCAP (2019) to describe technological innovations for disaster resilience, which can help in all phases of disaster management, using four types of analytics: descriptive, predictive, prescriptive and discursive, as shown in Figure 23. According to ESCAP, the most important data sources for descriptive analytics are images from satellites and UAVs/drones, followed by social media, IoT and crowdsourcing. Khan et al. (2022) presents a survey about the use of UAV for disaster detection, mitigation, response, and preparedness. Mohan and Mittal (2020) present a survey about the use of ICT in disaster management.

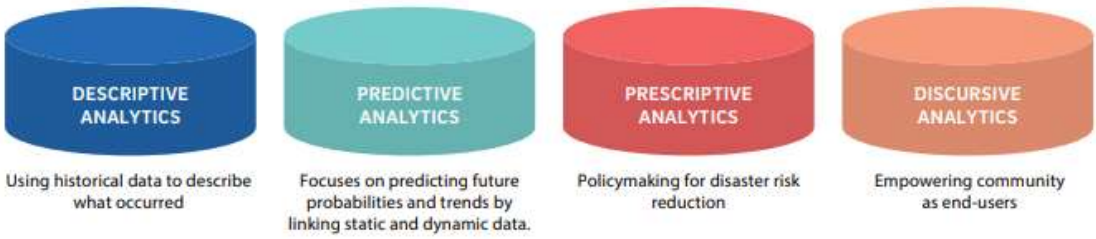


Figure 23 - Big data: four types of analytics for smart resilience (ESCAP, 2019)

Some use cases are: the post-disaster action in Sulawesi earthquake and tsunami, where the World Bank using the Global Rapid Post-disaster Damage Estimation methodology, including satellite and remote sensing imagery from a variety of sources, made a rapid assessment of the damage-affected areas. Within 10–14 days of the event was possible to access loss estimates, and the spatial distribution of damage. The economic losses were estimated at U$500 million, the World Bank used this approach to program its support for reconstruction through the funding of up to U$1 billion. Another use case is the cyclone Gita between 10 and 13 February 2018, that hit several countries in the Pacific. Big data allowed to predict the cyclone well in advance, allowing the Governments to prepare countermeasures. Post-disaster also made use of drones to capture images from the affected areas (ESCAP, 2019).

The use of ICT integrated with Smart Cities can improve the preparedness and responsiveness to disaster events, helping in the smart resilience for Smart Cities, as used by the Japan meteorological agency. This agency uses quantitative precipitation estimation, and quantitative precipitation forecast, as warning criteria to identify risk of flood inundations and landslides. Based on that information, the Public Weather Service can emit warnings to the population. The tools need to be smart to collect information and translate the various data in usable information, also, is imperative the coordination among multiple stakeholders with integrated information systems, and public awareness and consent of the population, ensuring privacy and engaging communities in data collection (ESCAP, 2019).

Figure 24 shows an example of the use of different resources of the city to gather information intending to help in smart city management, as suggested by Qadir et al. (2021),

where all the smart city key components are connected and monitored to address disasters. The proposed holistic system can help the cities in preparedness and mitigating effects, by enhancing the smart city governance in all disaster phases. An example is the use of 5G providing information on surviving UE locations unable to communicate because of the lack of wireless service, but still transmitting signal searching for available G-NodeBs, being able to provide awareness of victim location, as proposed by Alsaeedy and Chong (2020), using UAVs as mobile gNBs (UA-gNBs).

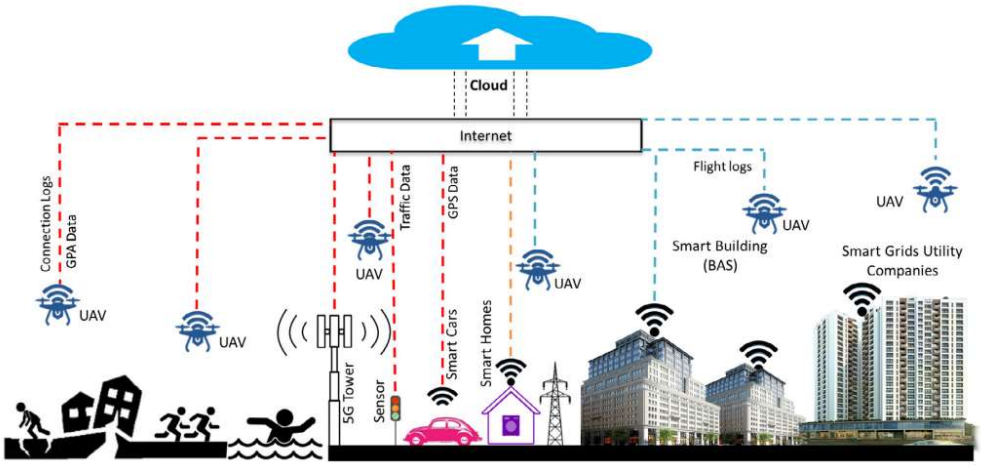


Figure 24 - IoT powered UAV based Smart City management framework (Qadir et al., 2021, p. 17).

4.3 Mission-Critical Communication

Radiocommunication objectives and requirements for PPDR were defined in several papers and technical reports as Carreras-Coch et al. (2022), which presents a summary of Emergency Communications Systems (ECS) requirements description. Jarwan et al. (2019), which present a summary of types of services that should be supported by PS networks. ITU-R (2003), which defined objectives and requirements as interoperability, reliability, functionality, security in operation and fast call set-up and already considered that "the radiocommunication needs of PPDR agencies and organizations are growing, future advanced solutions used by PPDR will require higher data rates, along with video and multimedia capability" (ITU-R, 2003, p. 2). The ITU-R (2003) report already envisioned that the PPDR organizations will operate their communications in a complex environment, requiring the recognition of same factors, as

> The involvement of a number of interests (such as governments, service providers, manufacturers); the changing regulatory framework for those involved in supplying systems supporting PPDR; that PPDR applications may be narrowband, wideband or broadband, or a mixture of these; the need for interoperability and interworking between networks; the need for high levels of security; the needs of developing countries; the needs of countries, particularly for developing countries, for low-cost communications equipment for public protection and

disaster relief agencies and organizations; that in some countries, national regulations and/or legislation may affect the ability of PPDR organizations to use commercial wireless systems or networks; that in some countries, commercial wireless systems currently offer and will probably continue to support PPDR applications.

The MCC in LMR presents several limitations that were mapped by the ETSI through the User Requirement Specification TETRA, intending to improve TETRA services driven by the provision of user driven services. The overall points to improve, according to a market questionnaire answered in 2001, where the two major topics to be address for furthers TETRA releases were: high speed data and; interworking[18] and roaming.[19] Then, in 2007, during the TETRA World Congress 2007, another questionnaires were applied to have a better understanding about the user requirements and address the topics in future releases, detailed in the TETRA Release 2.1 part 1 until 12 (ETSI, 2011).

Since 2001 some improvements were made in LMR networks until 2012, when the TCCA and the National Public Safety Telecommunications Council (NPSTC) signed a memorandum of agreement expressing the need to develop MCC standards for LTE-based technology. From there the technology that are increasing improve to reach the MCC user requirements is the LTE, while the LMR users continue with the same problems that were mapped in 2001 and 2007, and according to recent researches as Freire and Cândido (2020), Freire (2019), and Fonseca (2022), the two majors topics that now we can refer as problems, since there is no more releases in LMR technologies intending to solve those issues, continue to be high speed data and interworking.

In EUA, with the nationwide LTE-based (FirstNet), and in Europe, where LTE is increasingly considered by the PPDR community as a broadband technology to be integrated with TETRA, the LTE is the technology intending to achieve the PS requirements. Although, the adoption of LTE for PS requires the LTE to achieve the services specifications present in the current LMR communication, which are not usually defined for commercial purposes.

Comparison of services can be found in the literature as in Ulema (2019), Jarwan et al. (2019), Baldini et al. (2014), Freire and Cândido (2020), comparing TETRA and LTE, and suggests that LTE may continue to be the choice for MCC wireless voice and data communication. That is also the recommendation of the TCCA, pointing LTE as the evolution of the LMR communication. Intending to achieve those MCC requirements the 3GPP started to provide in the releases of 4G and 5G the technical specifications to reach the MCC requirements.

---

[18] When using a system such as TETRA, the users from one system can communicate with mobile users from the other system, as long as they operate within their home network. Interworking is used to provide communication between different technologies (ETSI, 2011).

[19] Roaming can be defined as "utilization of a mobile terminal in a network other than the one where the mobile is subscribed but on which the mobile can still be located and operated by agreement between the respective network operators" (ETSI, 2011, p. 7).

In the literature can also be found requirements for PPDR networks in 5G, as Volk and Sterle (2021) which studies 5G network for PPDR purposes, and present a dedicated 5G PPDR experimentation facility, the authors also presented a review of 5G and cloud-native technology enablers for PPDR purposes, and an overview of possible 5G PPDR architectures and deployment options. In Mezzavilla et al. (2018), the use of frequencies above 6 GHz in 5G for PS purposes is explored.

4.3.1 Frequency Spectrum

The spectrum used for LMR networks is harmonized across the world, for example, on the American and European continents the range of 380 to 400 MHz are predominant, is also observed 460Mhz and higher frequencies as 700MHz (BroadMap, 2017; Freire, 2019). When it comes to broadband services the spectrum allocation for broadband communication in PS were also broadly discussed along these years in technical reports as Das et al. (2020), BroadMap (2017), ITU-R (2003), ETSI (2014) and Electronic Communications Committee (ECC, 2013), which aimed at calculating the required amount of spectrum based on the assumption that the LTE will be applied throughout Europe for PPDR broadband network. The basis for the calculation were PPDR scenarios prepared by PPDR agencies and the EU Council's Law Enforcement Working Party (LEWP).

The report concludes that in Europe a dedicated spectrum of 2 x 10 MHz would be required for the PPDR broadband network, which were also aligned with the spectrum allocated in 2011 in the USA (the D-Block) for PPDR broadband in 700 MHz. The conclusion was also that only two bands remained as candidates for that use, the 400Mhz and the 700Mhz (694 MHz - 790 MHz) band. In 2013 the EU Radio Spectrum Committee (RSC) started to develop harmonized technical conditions for the 694-790 MHz band in EU for the provision of wireless broadband in support of EU spectrum policy objectives (ETSI, 2014). In 2016 the European Commission Decision 2016/687 has established the harmonization of the 700 MHz band for mobile services, the PPDR broadband network were specified to be allocated in 700MHz band in Europe, meanwhile, the way of implementation in the member states has been left open (European Union, 2016).

In each country the spectrum allocation is needed to define the frequency band for the PPDR broadband, as discussed for the EU in EU4Digital (2019), pointing out that the most common scenario among the EU countries is the channel arrangement: PPDR UL: 698-703 MHz and 733-736 MHz; PPDR DL: 753-758 MHz and 788-791 MHz. The countries governments should be aligned with the technological developments; PPDR strategies to achieve the general objectives of the communication technology considering also the social economic objectives of the technology, and their effects into society. Also, be aligned with cross-borders strategies in case of a broader solution as the Pan-European solution designed by the BroadWay project.

After the spectrum harmonization and allocation through national and international laws, the government and PPDR agencies should analyze the technological solutions which could attend the demands of each applied case. The solution should attend the requirements of the actual technology and offers advantages of new technologies as broadband and system integration, which were the two major problems identified by technical reports and papers, as shown before. Instead, the voice communication will remain as a critical component of PPDR operations, new services provided by broadband network with data integration, and intelligent analysis, will play a key role in PPDR operations.

Some decisions about frequency were made in France, which has allocated a 700 MHz band frequency for the broadband PPDR network; UK has opted to use the broadband network of the MNO Everything Everywhere (EE) mostly in 1,8GHz and 800MHz; Dubai allocated 2x10 MHz in band 28 and 2x5 MHz in the 700 MHz guard band in band 68; Finland has opted to use broadband network of the MNOs, including 700 MHz (BroadMap, 2017). In Republic of Korea the same 700 MHz frequency band is allocated to the LTE-based public safety (PS-LTE) network, the LTE-based high-speed railway (LTE-R) network, and the LTE-Maritime (LTE-M) network (Ahmad & Chang, 2020). EUA and Canada allocated 2x10 MHz of spectrum in the band 14; South Korea allocate 20 MHz in 700 MHz in the band class 28; Australia there is no dedicated spectrum, sharing spectrum with MNOs as in UK (Jarwan et al., 2019).

In Europe, BroadMap (2017, p. 27) indicated that "a harmonized dedicated European spectrum plan for PPDR broadband seems unachievable and a European solution must therefore to some extent include commercial mobile radio networks". In that sense, since the spectrum situation varies, an integrated solution, as proposed by BroadMap, would include different radio plans, and mix of dedicated networks and networks shared with commercial users. For that, national and international strategies, and spectrum plans should also consider heterogeneous networks.

4.3.2 MCC characteristics, requirements and user requirements

There are several papers and technical documentations about MCC characteristics, requirements and user requirements of the actual network as ITU-R (2003), ECC (2013), ETSI (2011; 2012), Baldini et al. (2014), Freire (2019), and Project HELP Consortium (2011). Below there is some of the most important characteristics and requirements of MCC communication.

According to Baldini et al. (2014), the basic services for MCC are: 1) Voice with specific level of quality to ensure that the requests and responses among the EFR are clearly understood, even in crisis situations, where background noise can be present, the voice should be also shared in Group Calls, where a pre-defined group of users can participate, and the groups are managed by a dispatch center. 2) Data connectivity, as query to remote data servers and video streaming, all services with specific QoS requirements. 3) Short Message broadcast

and multicast. 4) Push-to-Talk, allowing half-duplex communication, pressing a button to switch from voice reception to transmit mode. 5) Security services as authentication since sensitive information could be transmitted among EFRs. 6) Location service to determine where the EFRs are in the field. The authors also identified the main applications and the required data rate of current and future use for PS, as shown in Figure 25, that applications are also referred in technical reports as ETSI (2010).

Application	Description	Required data rate (Wide-band or Broad-band)
Verification of biometric data	PS officers may check the biometric data of potential criminals (e.g., fingerprints) during their patrolling duty by transmitting it to the headquarters or a center with the biometric archives	Wideband
Wireless video surveillance and remote monitoring	A fixed or mobile sensor can record and distribute data in video-streaming format, which is then collected and distributed to PS responders and Command and Control centers.	Broadband
Automatic number plate recognition	A camera captures license plates and transmits the image to headquarters to verify that the vehicles have not been stolen or the owner is a crime offender.	Wideband
Documents scan	In patrolling or border security operations, PS officers can verify the validity of a document.	Wideband
Database checks	This application area includes all the activities where PS officers must retrieve data from the headquarters to support their work.	Wideband/ Broadband
Location or Tracking for Automatic Vehicle or Officer Location. Situation Awareness	The PS officers have a GNSS (e.g., GPS) position localizer on the terminals. The positions are sent periodically to the headquarters to support decision management..	Wideband
Transmission of Building/Floor plans	In case of an emergency crisis or a natural disaster, PS responders may access the layout of the buildings where people are trapped.	Broadband
Monitoring of PS officer	Vital signs of PS officers could be monitored in real-time to verify their condition. This is particularly important for fire-fighters and officers involved in search and rescue operations.	Wideband
Remote emergency medical service	Through transmission of video and data, medical personnel may intervene or support the team in the field for an emergency patient.	Broadband
Sensor networks	Sensors networks could be deployed in a specific area and transmit images or data to the PS responders operating in the area or to the command centre. This application does not include video-surveillance, which is described above.	Wideband

Figure 25 - List of current and future PS applications beyond the basic services (Baldini et al., 2014).

Even with a fragmented target users and use cases, a set of requirements were identified in the earlier studies (2006) of the SAFECOM program (Cybersecurity and Infrastructure Security Agency [CISA], 2022). That were Made by the US Department of Homeland Security, focusing on interoperability, defining the operational requirements: "Support to Command and Control hierarchy; support to interactive and non-interactive voice and data communication; inter-agency interoperability; security; support to a new data applications, which go beyond

simple voice communication" and technical requirements: "Speech transmission performance; video transmission performance; QoS (packet loss, jitter, latency); timeliness in the delivering messages; radio coverage; call prioritization; robustness of PS equipment; energy consumption; security and resilience/availability of the networks" (Baldini et al., 2014, p. 624).

The term interoperable communications mean:

> The ability of emergency response providers and relevant Federal, State, and local government agencies to communicate with each other as necessary, through a dedicated public safety network utilizing information technology systems and radio communications systems, and to exchange voice, data, and video with one another on demand, in real time, as necessary (United States, 2010, p. 194).

About user requirements, some of that are: the EFRs needs to have full or part control of their communications with centralized dispatch; talk group configuration from the dispatch; priority levels among other users; robust equipment to the EFRs with unique accessories adapted to the user demand as long battery life, special microphones for discrete operation and hostile environments as on the helmet and throat microphone (which pick up the vibrations from the throat to activate the microphone), and so on.

According to ITU-R (2003) MCC are vital to the achievement of the maintenance of law and order; response to emergency and disaster relief situations, protection of life and property. The systems for PPDR aim to achieve the technical objectives of supporting the integration of voice, data, and image; providing additional levels of security associated with the type of information carried over the communication channels; supporting equipment that operates in extreme and diverse operational conditions; accommodating the use of repeaters for covering long distances between terminals and BSs in rural and remote areas, and also for on-scene localized areas; providing fast call set-up, one touch broadcasting and group call features.

According to ITU-R (2003), security should include end-to-end encryption and terminal/network authentication. The communications should have management controlled by PPDR agencies such as set-up talk groups, guaranteed access including priority and preemption calls, spectrum resource availability for multiple PPDR agencies, etc. The network should have the capability to operate in Direct Mode Operation (DMO), simplex radio and push-to-talk. Should be possible to have customized and reliable coverage allowing cell size or capacity extension during emergency and disaster situations as in rural and remote areas; to provide full-service continuity even with partial loss of infrastructure; to provide high quality of service including instant call set-up, resilience under extreme load and high call set-up success rate. The network also must consider various PPDR applications and use cases.

4.3.3 MCC scenarios

Radio operating environments for PPDR are important to the scenario's definitions from the radio perspective. According to ITU-R (2003), there are three scenarios, the day-to-day operations; large emergency and/or public events operations; and disasters operations. The day-to-day operations are routine operations that PPDR agencies conduct in their jurisdiction, generally the most network design is determined using this scenario with extra coverage capacity for unexpected events.

In large emergency and/or public events operation, the PPDR agencies are still required to perform their routine operations, but the size and nature of the event may require additional forces to join, as international organizations. In public events as Olympic Games, there is time to plan with advance and organize the operation. In large emergency situations, the PPDR agencies should have some planes in place in advance, even without knowing if and when the situation will occur. The radiocommunication equipment for those scenarios is generally brought to the target area and may or may not be linked to the existing network (ITU-R, 2003).

Disasters operation can be caused by natural or human activity as floods, earthquake, and terrorist attack. In that situations generally both networks are used, the one used in routine operations and the one that are brought to the area, when that is possible. In disasters situation the MCC will be an important asset since the terrestrial infrastructures may have been damaged by the disaster, or there is increasing traffic demands inside the zone. The report suggests the use of Mobile Satellite Services (MSS) in the situations where the infrastructures were damaged and highlight the problem of the cross-border circulation of terminals, being imperative that neighboring countries can offer the initial essential communications (ITU-R, 2003).

Considering those scenarios is important to bring some reflections to nowadays world, the most part of the day-to-day operations occur inside cities, where the LMRs networks and MNOs have good coverage. Since the LMR networks doesn't have data capacity, and the EFRs needs that resources to perform their duties, as sending and receiving images, the EFRs continue to use the LMR for voice communication, and the MNOs for data applications, such as WhatsApp, and using most times their personal devices, which could result in great vulnerability of information.

This is demonstrated in Fonseca (2022), where 884 agents of the Federal Police of Brazil were interviewed. Even with 85% of those responders considering MCC important and/or very important to their work, they are using MNOs to communicate because of the lack of data capacity and UE suitability (43.7% reported that the LMR UE is not suitable for the work). Also, 48.35% of the agents no longer uses the LMR network, which is TETRAPOL technology and has been in use for 16 years, and currently are facing problems of maintenance and frequency spectrum regulation to continue to operate in the 450MHz band. 64% of respondents uses cell phones instead of LMR radios in day-to-day scenarios (with no guarantee of QoS, priority or

preemption), not because they do not consider MCC as important or wanted to replace the MCC system for a regular commercial system (just 19% of the responders suggested replacing the LMR for regular commercial solutions), but because of the limitations of the LMR systems.

That is also a reality in Europe, according to BroadMap (2017), the European PPDR organizations uses the LMR networks and, despite the lack of guarantee QoS, priority and preemption, the European PPDR organizations continue to use applications through MNOs services, as video transmission, remote controlled cameras, and database queries.

In large emergency and/or public events operation remains the necessity of priority and a network with full-service continuity, even with partial loss of infrastructure. As an example, at the closing ceremony of the 2016 Olympic Games in Rio de Janeiro, where several heads of state were present, a storm hit the city of Rio de Janeiro with winds above 120km/h, which caused tree falls, accidents and various unforeseen events. The MCC network of the Federal Police of Brazil lost part of its connectivity due to the rupture of some optical fibers from the BSs to the control node. However, the BS covering the Itamaraty building continued operating locally, even without access to the control node, enabling communication between the police officers, who carried out the security of the dignitaries, during the way from Itamaraty to the Maracanã Stadium and in the event. Unaffected by the lack of connectivity and high traffic on MNOs. Also, a backup network had previously been set up using tactical repeaters, which could be used in case the main network failed. In addition, the DMO could have been used as a last resource. This was possible due to the technology, prior preparation of the telecommunications team, prior training of police officers, local coordination and coordination through the CCC.

In that situation the Federal Police were using only the LMR, but in case of the use of LMR and MNO, or only MNO, the MNO can have PS priority for traffic in an LTE network through preemption, and sharing of LTE networks can accommodate the MCC users because of the presence of multiple MNO infrastructures with multiple coverages. The Self Organized Network (SON), a concept existing in 4G and 5G networks, related to the concepts of self-awareness, self-configuration, self-optimization, and self-healing, can help with the dynamic networks, managing the network capacity, QoS, and coverage with self-capability to optimize and configure parameters, improving users' mobility and user experience. The problem remains if the e-Node-B completely loses the connectivity with the EPC, as happened in Rio in 2016, the commercial E-nodeBs do not operate without connectivity to the EPC, in that case, an MCIOPS should replace temporarily the e-nodeB. About direct communication, the latest 3GPP release already provides this functionality, although, according to the interview responses shows at chapter 6, that remains without working properly.

In all those scenarios using only LMR networks, the major limitations of PS systems remain. According to ETSI (2010), they are: 1) Lack of network capacity in emergency scenarios, since emergency scenarios usually lead to exceptionally high traffic loads, which a single MCC system may not be able to support. The situation can worsen considering the limited radio

coverage in some areas, and when some parts of the infrastructure are damaged. 2) Lack of broadband connectivity, which could enable real-time access to critical data. 3) Lack of interoperability between agencies using dedicated networks within their respective coverage areas, which affects cooperation between agencies, especially in operations where cooperation is a major requirement, as cross-border situations or large emergency situation.

4.3.4 Interoperability

Interoperability is a key aspect to consider in MCC, that is not only technical dependent but also, legal and working processes dependent. Software Defined Radio (SDR) technology can mitigate interoperability barriers, as demonstrated by the European Commission (EC) Seventh Framework Programme (FP7), known as EULER (EUropean software defined radio for WireLEss in joint secuRity operations (European Commission, 2015). This project took placed between 2009 and 2013 and were created intending to mitigate the lack of interoperability in Europe, adopting SDR providing interfaces with different RANs based on the Radio Access Technologies (RAT). Cognitive Radio is another solution, which has the following capabilities:

> To obtain the knowledge of radio operational environment and established policies and to monitor usage patterns and users' needs; to dynamically and autonomously adjust its operational parameters and protocols according to this knowledge in order to achieve predefined objectives, e.g., more efficient utilization of spectrum; and to learn from the results of its actions in order to further improve its performance (ETSI, 2010, p. 8).

Some solutions with system interoperability were implemented, using technical development and work processes implementation. The first implemented cross-border Inter System Interface (ISI) in the world were between Norway and Sweden, using the scheme ISITEP (Inter System Interoperability for TETRA and TETRAPOL Networks), having as partners Motorola and Airbus, responsible for the technology development, the cross-border was established in 2016 (Swedish Civil Contingencies Agency, 2014; Motorola Solutions, 2017). In 2017 a similar integration between Finland and Norway was announced, an EU-funded ISITEP initiative (Motorola Solutions, 2017). In 2020 another integration was announced, a three-country cross-border collaboration between Finland, Norway and Sweden, following the methods in the Norway/Sweden, Finland/Sweden and Norway/Finland bilateral ISI-services (MSB, 2020).

According to BroadMap (2017), there are other types of cross-border operation in use as: the DMO between Serbia and Croatia; the TMO between Sweden and Denmark, between Sweden and Finland, between Romania and Moldova; a TMO gateway between The Republic of Ireland and Northern Ireland; a solution based on TMO and DMO between Belgium and Netherlands. Those different models of interoperability also can be observed inside countries with different LMR systems, and are a majority requirement in large events, as happened in the 2014 soccer World Cup in Brazil, and in the Olympic Games in Rio 2016. In these events,

protocols were created by the telecommunications working group, with the solution through a TMO gateway between LMR networks. The CCC had working processes designating how to act in situations where communications between agencies need to be interoperable.

In 3GPP networks there is no issue about interoperability between the standard interfaces since the technologies are all 3GPP compliant. However, there is a need for bilateral agreements between the service providers. In the case of MNOs providing the services, that are made by roaming agreements. In the case of different models of broadband PPDR networks, legal agreements and working processes would be needed in different levels.

4.3.5 Some European Commission Programme in that area

The FP7 has funded various projects intending to improve the communication capabilities of EFRs, some of them were the Enhanced Communications in Emergencies by Creating and Exploiting Synergies in Composite Radio Systems, known as HELP (2011-2012), the proposed solution was based on the adoption of LTE for PS (Project HELP Consortium, 2011). The Digital and Innovative Technologies for Security and Efficiency of First Responders operation, known as DITSEF (2010-2013) aimed to enhance the efficiency of information gathering and sharing between EFRs and CCC, supporting EFRs through a network of sensors, localization and communication systems, particularly in the event of large fires. These technologies were integrated into wearable systems for the EFRs (European Commission, 2017).

The project ABSOLUTE is one of the applications of MCIOPS, was a project raised by the European Commission intending to raise in the sky a balloon with Attached 4G eNodeB (AeNB), to rapidly deployable mobile network to provide broadband services based on a flexible, scalable, resilient and secure network design with: "i) LTE-A BS embedded in Low Altitude Platform enabling a large coverage for broadband services ii) Portable land mobiles interoperable with conventional public safety networks, iii) Advanced multiservice professional terminals for first responders" European Commission (2019).

With broadband technologies, since is based on common protocols specified by 3GPP, the technology itself is an integrator, and since the requirements for narrowband MCC are well-known, as demonstrated before, the next step was collected PPDR interoperable broadband communication requirements. In that sense, the BroadMap project (European Commission, 2022) took place between 2016 and 2017, intend to map interoperable EU PPDR broadband communication applications, and technology, including nuances of societal differences, different cultures, processes, geography, and legal frameworks, with participation of 15 countries in Europe. The main intention was to define a transition roadmap to a Pan European PPDR mobile broadband network.

According to the final report of BroadMap (2017), the Pan European PPDR interoperable and harmonized solution consists in three layers, namely: harmonization; interoperability and

governance; networks and users. On the harmonization layer, each country needs to provide PPDR services using their own organization. The harmonization will be obtained by using standardized technology, as 3GPP technologies, and harmonized frequency bands. The interoperability and governance layer defines a common PPDR Pan European cross-border interoperability solution, the Standardized PPDR Interoperable Communication for Europe (SpiceNet). On the networks / user layer, the SpiceNet provides common services that can be used in all participating countries and can be extended for interested countries via agreements.

At the radio network level, the BroadMap report proposes a solution based on the 3GPP Release 15 mission-critical standards in three different migration ways, starting from the legacy narrowband networks, highlighting the importance to integrate it with the target solution to mitigate risks. According to the report, the key functionalities are: security, interoperability, priority and preemption, location-based MC features, spectrum, applications for PPDR, Pre-Commercial Procurement (PCP) setup recommendations. Also, a Technical Validation Committee (TVC) should describe the technical architecture of the requirements not yet developed at standardization institutes level, evaluating the PCP prototypes and pilot systems.

The main purpose of the BroadMap project was establishing the foundation for a European Interoperable PPDR Broadband communication solution, targeting also "to align the PPDR vision with the European roadmap for 5G deployment, priorities and early trials" (BroadMap, 2017, p. 26). Proposing an architecture model, focused on Interoperability, intending to be the basis of the SpiceNet services. The BroadMap efforts result in the BroadWay project. Actually, the EU is working on the BroadWay project, a pan-European broadband system for PPDR, which is in its third and final phase. BroadWay Pre-Commercial Procurement started on October 8th, 2021, initiated by the signature of awarded contracts to the two first ranked consortia of the Phase 3 call-off competition, following their successful completion of the Phase 2, or Prototype Phase (BroadWay, 2022; Public Safety Communication Europe, 2020).

The 5G-EPICENTRE Project is an EU-funded innovation under the Horizon 2020 research framework, aiming to deliver an open, federated 5G end-to-end experimentation platform, design to attend the needs of PPDR software solutions. As PS constitutes a niche market regarding ICT stakeholders, the intention of the 5G-EPICENTRE platform is to allow developers and small and medium-sized enterprises to build up and experiment their solutions in a low-cost way, intending to lower the entry barrier to the PPDR market.

The platform is based on open service-oriented architecture, accommodating open access to 5G networks' resources, providing eMBB, mMTC and URLLC, as an open-source repository for PPDR 5G Network Applications, called, the NetApps. There are 4 test beds in the 5G-EPICENTRE federation, the 5G-VINNI experimental in Aveiro, Portugal; the 5GENESIS in Málaga, Spain; 5G Berlin, in Berlin, Germany; and the 5G CTTC end-to-end experimental platform, in Barcelona, Spain. Some of Netapps expected as result is shown in Figure 26. In

2023 the platform is expected to become open to third-parties external to the project consortium (5G-EPICENTRE Project, 2023; Apostolakis et al., 2021).

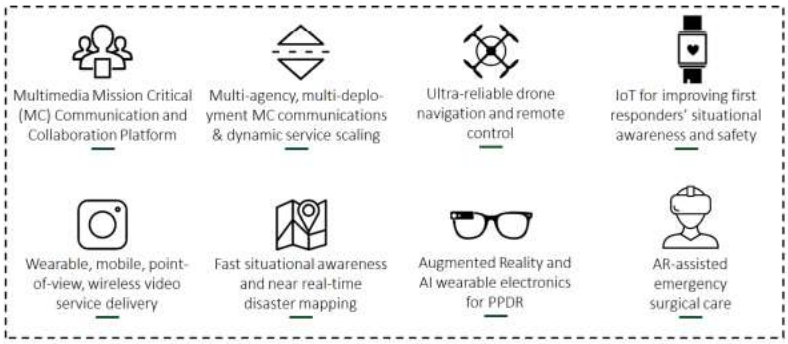


Figure 26 - 5G-EPICENTRE Project, experimenter apps, adapted from Apostolakis et al. (2021, p. 2).

The Faster Project is a Horizon 2020 funded project that involves a consortium of research, social and technical partners, and EFRs organizations. The goal of Faster project is facilitated the first responders' visual perception in disaster, and dangerous areas, by developing a set of tools towards enhancing the operational capacity of EFRs. The solution includes: AR technologies; mobile and wearable technologies; body and gesture based user interfaces; lightweight and camera-equipped UAVs combined with AR see-through devices, and advanced 3D scene analysis, delivering information in real time; a platform of autonomous vehicles, namely drones and robots; multi-modal data from the field, utilizing an IoT network, and social media content, to extract meaningful information, providing situation aware content data for the EFRs through portable control centers. Faster will support inter-agency communication, allowing real-time reporting (FASTER, 2023).

4.3.6 Governance

About PPDR networks ownership and operation, BroadMap (2017) classified them as GOGO (government owned, government operated), GOCO (government owned, contractor operated), and COCO (contractor owned, contractor operated). In Europe, most networks are Government Owned (GO), and the operation is splitting in government (GO) and contractor (CO) operation. As observed in the interviews from Chapter 6 and in Freire (2019), in Latin America is also the same of Europe, government owned (GO) and operation split into GO and CO. The possible reasons to the use of GOGO are security, users' anonymity and user data protection, also, when MNOs doesn't reach the Service-Level Agreement (SLA), the results are mostly loss of revenue, while, in PPDR communications the result could be life losses.

The existing P-25, TETRA and TETRAPOL networks are using dedicated spectrum and dedicated infrastructures to guarantee network availability and integrity. When moving to 3GPP networks, there are different usage models to choose from: dedicated, hybrid, and commercial networks. In most countries in Europe PPDR users use normal data subscriptions

over MNOs, the exceptions are Astrid in Belgium, where an MVNO solution has been used; and in VIRVE, Finland, where a secure MVNO solution has been used (BroadMap, 2017).

For broadband solutions, according to BroadMap (2017), government control is essential, but the form of this control may vary based on the adopted solution and organization model. If commercial actors are part of the solution, agreements, regulations and audits should be considered, also, security specifications and management of the system must be well-defined.

In the case of a common system between countries, as the Pan European network proposed by BroadMap, the report suggested the needs of creation of a dedicated PPDR communications entity, under the legal form of a Grouping of Territorial Cooperation (GTC), to establish a broadband-based authority. With procurement and operational roles (e.g., coordinate the system), and submitted to the national law where it has its registered office (since the operation would involve more than one country), where the member and associated countries should have defined missions in its constitutive agreement.

4.3.7 Overview of some MCC networks in use

Most PPDR agencies are still using LMR technologies, although, the European PS networks were mapped in 2017 by TETRA Critical Communications Today (2017), as shown in Figure 27, it can be observed that some countries are already in transition to broadband networks.

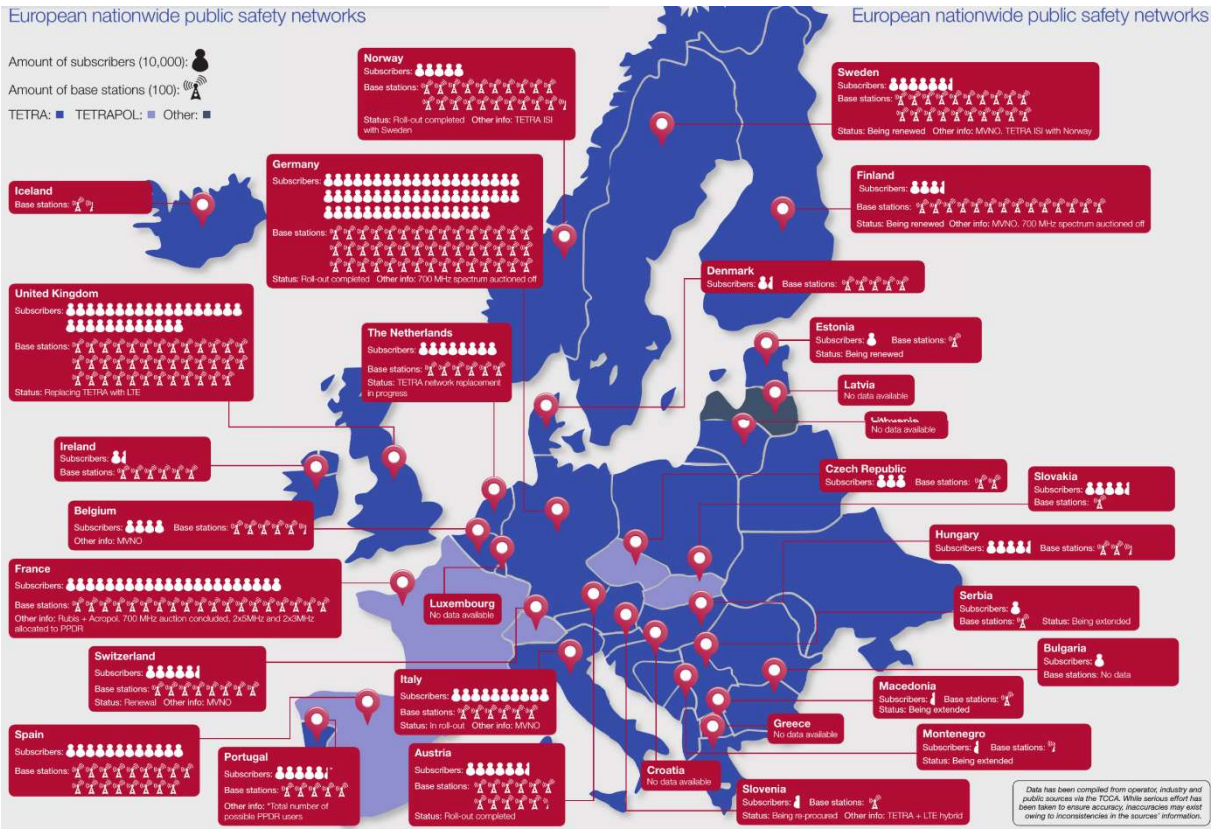


Figure 27 - European nationwide PS networks (TETRA Critical Communications Today, 2017, p. 27).

4.3.8 Major requirements in the transition from MCC narrowband to broadband

The MCC have some specific characteristics, as the need to be full available even in locations without network coverage, for this, the users should communicate using D2D communication, without the need of any infrastructure. With 4G and 5G it is possible to deliver a fast network through UAVs, as a flying ad-hoc network, which can provide communication support in scenarios as disaster, acting as communication gateways between EFRs. That could be done, for example, through D2D communication, which "addresses the energy efficiency and battery lifetime of UEs, but it requires special devices to be deployed that have high transmission power, long battery lifetime, and the ability to control radio resources" (Alsaeedy & Chong, 2020, p. 2065), although, such devices are not widely used by the end-users, being a critical requirement for ad-hoc networks.

Also, the PPDR agencies should have the possibility of delivery an autonomous network in a short period, this can be done through tactical equipment named by 3GPP as MCIOPS, a tactical BS that could be in service isolated or integrated to the network through internet or satellites. This functionality was already available in LMR networks, in 4G and 5G networks the tactical eNodeB/gNodeB has more processing capacity and could have a transportable solution that includes RAN and mobile core, creating a dedicated network that can run with or without external connections, as shown in Athonet (2022). Tactical solution in 5G were also tested and demonstrated in Heikkilä et al. (2022) with the use of a 5G Stand-Alone equipment.

The CCC should be able to analyze different data sources, from the communication network, and other sources as big data, cameras, information from other PPDR agencies, from its own databases matching with big data information as real-time information from cameras reading license plates, and so on. And then, sending relevant information, even real-time information to the EFRs in the field though broadband networks. For this, the network should have data capacity and meet some requirements of MCC networks, allowing the data collection from the IoT devices and the information sharing between EFRs.

According to Zhou et al. (2021) an important dimension of IoT 2.0 is the MCC based systems. IoT 2.0 is an evolution of IoT, including seven major fields, namely: ML intelligence, MCC, scalability, energy harvesting-based energy sustainability, interoperability, user-friendly IoT, and security. As MCC systems has requirements as URLLC and system availability, 5G networks and IoT 2.0 could reach MCC requirements, providing better services than 4G.

Another aspect that should be observed is coverage, for legacy PPDR and broadband networks. For broadband networks should also be observed the downlink and uplink data throughput and sustain data capacity. The coverage calculations could be based on geographical and population coverage, and it is presented as outdoor coverage, without considering the penetration losses, and indoor coverage. MNOs deploys the networks

attending the minimum coverage regulation in a way to maximize profits, they are in generally capacity driven instead of coverage driven.

For MCC networks the biggest concern is about availability, which are related to coverage and capacity. That differentiation is one of the reasons why PPDR agencies cannot completely rely on MNOs to provide the broadband network. The implementation of priority mechanisms in commercial networks can solve in part the capacity problem, although, some laws, as the EU net neutrality regulation (EU) 2015/2120 (European Union, 2015), regulate that each user should be treated equally, meanwhile, an MNO without priority for PPDR purposes could never reach mission-critical goals (BroadMap, 2017).

When analyzing LMR coverage is important highlighting that in some countries there is a network infrastructure dedicated to vehicular radios and handhelds. And there is a network infrastructure dedicated for Air-to-Ground (ATG) services to support Air-Ground-Air (AGA) operation, as communication between radio users operating from aircraft and helicopters, and ground-based operatives including UEs and dispatch centers. According to BroadMap (2017), in Europe, only five countries have implemented AGA coverage.

The security is another important aspect, in LMR networks there are several levels of security and LMR system uses specific encryption strategy. in TETRAPOL, for example, there is a Terminal Master Key (TMK) used in UEs and inserted locally in each UE through the Terminal Programming Station (TPS) server, with a time to expire. These keys are generated in the Control Node of each regional network in the Key Load Unit (KLU) application. The national network has a Key Management Center (KMC) where the network cryptographic keys are generated. Altogether there are 13 keys of 128 bits. TETRAPOL provides End-to-End Encryption (E2EE), and the organizations can use and manage their own encryption keys. E2EE, device authentication, and air interface encryption can be used in LMR networks, also, lost or stolen devices can be blocked from the dispatch center.

3GPP networks doesn't provide that level of security, although, it is possible to improve the security, as shown in 4.1.5, and according to BroadMap (2017, p. 19), using "mobile device management, sandboxing (separation of applications), secure VPN, split tunneling (a dedicated VPN for certain applications), encryption of sensitive data and security keys, installation of applications in a secure container, and many more functions". Interoperability is another key aspect, which are technical and working processes dependent, needing legal agreements; methods for collaboration; training for the methods, and guidelines. In LMR there is a lack of technology compliant, which turns the interoperability hard to reach. In 3GPP networks there is no technical issue about it between the standardized interfaces, and with the O-RAN initiative more interfaces are becoming open.

About applications, the local necessities should be observed to develop or choose applications to be used by PPDR agencies in MCC broadband networks. In that sense, even with some standard applications that is already available in the market, some other application

should be integrated intending to solve local problems. The MCC broadband network will bring connectivity, but the applications will bring intelligence to the operations. In that sense, the applications should be well-defined based on user requirements, and solution driven towards the local demands, based on common standards e.g., 3GPP. Allowing system integration, further development, and an application ecosystem supporting sharing of applications, for example, an PPDR store for applications, with control access of the users.

Figure 28 and Figure 29 show some 3GPP compliance applications already available in the market that allow MCC through 3GPP networks, and integration with legacy LMR networks. Enabling features such as group communication over an IP network, MCPTT, geolocation, digitalization and automation of business processes, text messages, video transmission, etc. The Airbus solution is in use in México, the Motorola solution is in use in EUA and UK. Tactilon Agnet is the Airbus solution, an application developed in partnership with Streamwide (which also has an application called Team on Mission already in use in France). Streamwide are also part of the consortium led by AIRBUS in the BroadWay project (Streamwide, 2022).

Another important step is to evaluate the legislations. Loopholes or incompleteness of existing legislation should be identified before the technology adoption, avoiding the risk of investing in a solution that could not be implemented, or just be partial implemented due legal issues. The project should identify those loopholes and point out ways to be taken at legislative level to allow the deployment of the new broadband MCC network, and the new ecosystems of actors, services and applications to support the network and the MCC community.

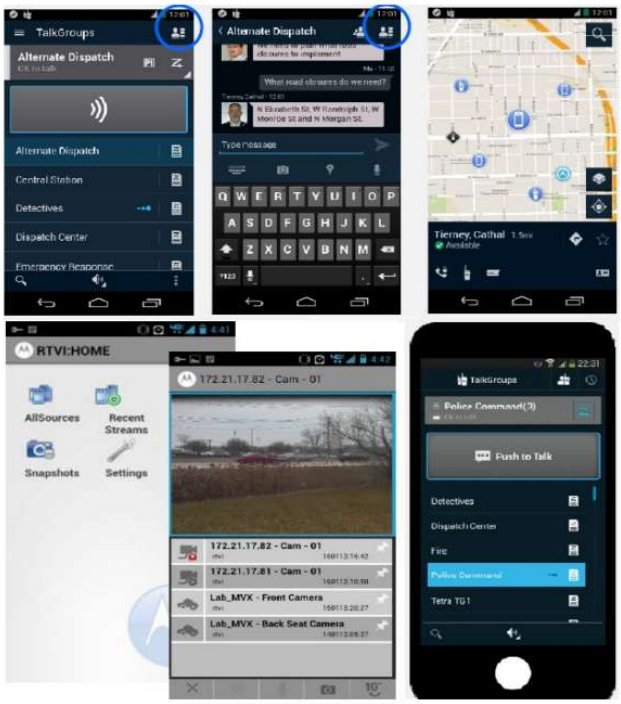


Figure 28 - MCC Application, Motorola Solution, adapted from Motorola Solutions (2017).

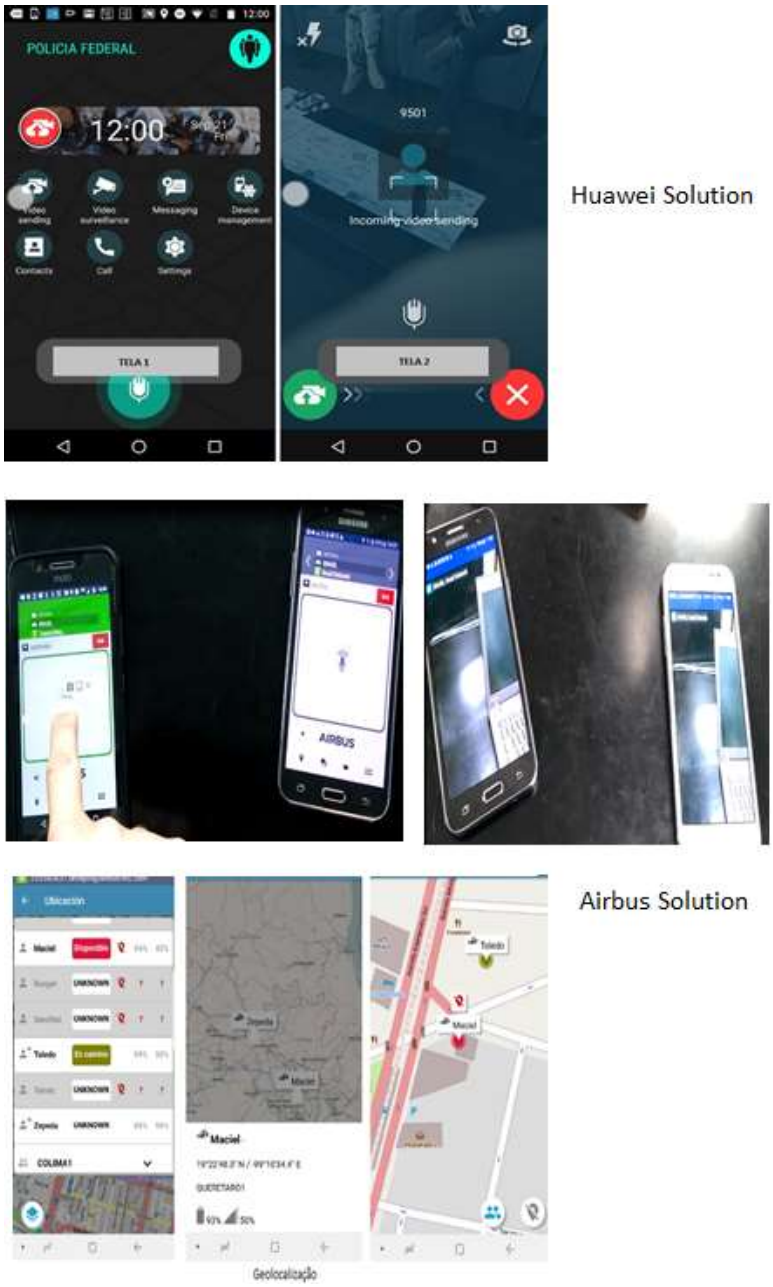


Figure 29 - MCC Application, Huawei and Airbus Solution (Author).

Some aspects must be inherent in MCC, with strict specifications, which should continue to be inherent in broadband MCC, according to Jarwan et al. (2019) they are: coverage; reconfigurability; capacity; availability; service continuity; security; management of priority, interconnection; and interoperability. With broadband networks also the cell and user throughput, user data volume, and latency should be observed, according to the end user specifications, and type of services requested. In resume, the major requirements to be observed in the transition from MCC narrowband to broadband are described below:

> The solution must cover network, interoperability, devices and applications and meet the actual requirements for European end users. (...) The solution also needs to be flexible to account for

> revised end user specifications, changing technologies and security requirements due to changing threats or geopolitical situations. PPDR-specific requirements for availability, robustness, resilience and priority mechanisms are of high importance, especially when commercial or hybrid models are included in the solution. The commercial parts of the solution must be audited to ensure that these requirements are fulfilled (BroadMap, 2017, p. 26).

The BroadMap highlighting when introducing the broadband MCC, interoperability with the legacy narrowband networks must be ensured, at least for voice. Also, the existing legislation loopholes or incompleteness should be observed. Local and global agreements is another need to ensure governance above national legislations and in conformity with the current global regulations. Keeping in mind that the final goal of the technological solution is to improve the quality of life of the citizens, as described by BroadMap (2017, p. 52), "the solutions provided must contain all innovative ways to create Mission-Critical PPDR broadband interoperability solutions (for networks, devices and applications) to help prevent crime, to save lives and to minimize personnel and economic costs".

4.3.9 MCC broadband devices

Despite the technology, the end-user devices can be categorized as mobile radios, installed in a vehicle; portable radios or handheld, carried by the users; and consoles, used to monitor and control the communication groups, providing emergency control (Ulema, 2019). Although, for the use of broadband technology the portable radios are the UEs, equal the ones used for commercial purpose as a smartphone, also with ruggedized and secure models.

About UEs, dual mode devices P25/LTE, TETRA/LTE and TETRAPOL/LTE, as the Motorola radio P25 APX NEXT, and TETRA MXP7000, are already available in the market and in use for some PPDR agencies. Being used in different models as GO of LMR network and LTE through commercial MNOs, MVNOs, and private networks. Other management models are possible which enable a soft transition to broadband networks maintaining the legacy network.

There are smartphones as the Bittium (Bittium, 2023) with a high level of security against information leaks, and models with physical PTT button, allowing to just press the button to talk, as a LMR radio. Motorola and Huawei also developed smartphones for MCC, as the Motorola L10, robust, resistant to falls and submersible up to 1 m of water for 30 minutes (ruggedized UE); dedicated tactical PTT button, and it also offers hardware encryption.

Cellular-enabled wearables devices used by EFRs are explored by Saaf et al. (2020), specifically a MCPTT application using LTE Cat-M2-enabled smartwatches and real-time video using body-worn cameras, gas exposure measurement based on smart helmets, EFR healthcare and vital sign monitoring. The communication can be made by wearable smartwatches, which also allows to the EFRs the hands free to perform their tasks with responsive. The authors

analyzed the MCPTT access time performance for different smartwatches combinations of device capability and D2D-related parameters.

In Saaf et al. (2021), the wearable devices are explored, and a performance evaluation of wearable-based mission-critical applications is conducted, where latency and reliability performance in MCPTT LTE smartwatches are tested and compared. Some use cases of wearables are real-time video sharing using body-worn cameras; smart glasses for remote assistance; smart-bands with measurements of exposure to toxic substances and monitoring vital signs; exoskeletons for supporting manual tasks; smartwatches for location tracking, communication, monitor alerts. "Therefore, wearable technology can deliver reliable in-field communications, enhanced situational awareness, and improved first-responder safety" (Saaf et al., 2021, p. 07). For this, the options of UE and accessories should be observed.

According to Alsamhi et al. (2019), drones play a vital role for PS purposes, delivering timely wireless communication services in target areas, as the ones affected by disasters, or even in specific situation as a pursuit of a criminal, the search for a missing person, or guiding search and rescue teams. For PS, the collaboration between drones and wearables is capable to support PS requirements, as real-time monitoring and real-time analytics, improving the decision-making-process in smart cities by helping the PPDR agencies in management crises.

The authors explore the collaborating between smart wearable devices and drones, intending to improve the level of PS in smart cities. The wearable devices allow EFRs to connect with each other and share information with the CCC. However, the wearables have limited transmission power, being disabled for long distance transmissions. In that situation, drones can connect with each other, and with the wearables, allowing data collection by various devices connected to drones, then the authorities can have real-time data received from drones, and real-time analytics to take decisions.

4.3.10 Some use cases of Mission-Critical Communication through broadband networks

FirstNet, in the USA, and the Emergency Services Mobile Communications Program (ESMCP), in the UK, adopted a mix of LMR and LTE networks as a solution. LMR offers narrowband voice capacity for MCC, with restricted data rates but with wide area coverage, in addition to LMR D2D communication; FirstNet and ESMCP provide MCC broadband (ESMCP, 2022; FirstNet Authority, 2022). The FirstNet network consist in:

> The FirstNet network supports mission-critical applications like, incident management, GIS, weather, traffic, video streaming, real-time resource tracking, mission-critical push-to-talk (MCPTT) operation, security management, email, office tools, records management, database access, reporting, medical references, strong user and device authentication, VPN, mobile gateway security, mobile device management (MDM) and end-to-end encryption. Though its

primary users are first responders like, police, fire, medical services, it also extends its support to utility organizations, NGOs, and volunteer organizations active in disaster situations. As the network is based on commercial cellular technologies like LTE, LTE-Adv, and emerging 5G, it addresses interoperability issues between various actors involved in disaster management (Zahid et al., 2019, p. 620).

Firstnet has allocated 2x10 MHz of spectrum in 700MHz, until 2017 more than US$7 billion had been invested. There is dedicated spectrum but also different implementation modes in parts of the country, a consortium led by the MNO AT&T was nominated as prime contractor, and the PPDR users can be directed to the contractor's frequency bands, intending to increase the PPDR services performance (BroadMap, 2017).

1. USA: FirstNet, national LTE network for PS, integrated by AT&T; 911 call center also feeds data to FirstNet (FirstNet Authority, 2022). AT&T was contracted in 2017 to manage the FirstNet for the next 25 years (Jarwan et al., 2019). "The network is a single, nationwide network architecture consisting of a secure, redundant evolved packet core network (EPC), transport backhaul, and radio access networks (RANs) in the fifty states, five territories, and the District of Columbia" (U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, 2020, p. 55).
2. UK: Emergency Services Network (ESN), hybrid solution through the network of the MNO EE + Extended Area Service (EAS) + Air to Ground (A2G) network for emergency service (ESMCP, 2022).
3. Qatar (Gulf Times, 2017), Dubai (Hill, 2019), South Korea (Byung-Yeul, 2020): Private LTE network for PS. Republic of Korea has private LTE PS networks, where the same 700 MHz frequency band is allocated to the LTE-based PS network, the LTE-based high-speed railway (LTE-R) network, and the LTE-maritime (LTE-M) network (Ahmad & Chang, 2020). Also, the dedicated network is used by eight disaster response agencies, enabling an integrated response to disaster, is conceived primarily by private networks and utilizes a part of commercial networks, and uses 20 MHz in the band 28. The communications service infrastructure is provided by fixed BSs, commercial networks, mobile BSs, and LTE-R / LTE-M network (Lee et al., 2021).
4. Mexico: S-MVNO, Airbus provides broadband for PS through the "Red Compartida", which has 90 MHz bandwidth, in 700 MHz. ALTAN is a Mobile Virtual Network Enabler (MVNE) and provides broadband for Airbus, which performs the interoperability between TETRAPOL IP and ALTAN network as MVNO (Freire, 2019). Australia tested a shared-network Public Safety Mobile Broadband, an S-MVNO deployment model, using two MNOs (TPGT Telecom and Optus), where the PPDR agencies have control of the core, Nokia provided a 5G-

ready core network for the PPDR agencies, MCPTT and an interworking gateway with the legacy LMR system (P-25) (Critical Comms, 2022).

5. Australia: Telstra Emergency, MCC with prioritized access, preferential data treatment and self-dimensioning bandwidth on commercial LTE (Telstra, 2022).
6. Sendai: Private LTE network, with drones for alert and rescue assistance in case of tsunamis (Nokia, 2020).
7. Astrid in Belgium: MVNO, Proximus, a commercial operator provides the MVNO with the possibility of roaming for all Belgian MNO providers to increase availability. The Proximus network supported priority and preemption for the PPDR users (BroadMap, 2017).
8. VIRVE in Finland: S-MVNO for PPDR broadband. The government owned an LTE core, which provides control of the broadband subscriptions, and a common subscriber management for the TETRA network, providing secure MVNO broadband services to the PPDR users. The RAN are from 2 MNOs contracted by VIRVE to provide the broadband RAN, the UEs are mostly vehicular multi-access routers that access the RAN from the MNOs and are routed to the dedicated LTE core via a secure backbone. The goal is to provide critical level mobile broadband over the Finnish territory, and the dedicated LTE core solution is part of the roadmap solution (BroadMap, 2017).
9. Rivas Vaciamadrid: Dedicated LTE PPDR network working in the 2,6 GHz band and operated by a non-governmental organization (BroadMap, 2017).
10. The EU is working on a pan-European broadband mobile system for PPDR, the BroadWay Project (BroadWay, 2022; Public Safety Communication Europe, 2020).

4.3.11 Paths for the MCC Emergency Management System

Command and Control Centers (CCC) "include a number of systems, applications, tools, policies, and people responsible for maintaining, administering, operating, and managing the whole critical communications network in a reliable, secure way" (Ulema, 2019, p. 158). The CCC could be by agency, region, and nationwide, depending on the country. Ideally these CCCs should be connected, allowing an integrated coordination and action. Other systems should be integrated to these centers as the emergency response system, incident management system, and the public warning system. The preparedness of the operations people is an important issue, especially with inter-agency operations, with no proper training even the most technological advanced system in use, the results of the technology will be limited.

Emergency response system, as 911 in the USA, provides the link between people in emergency situations and PPDR agencies. Through the phone service, the emergency response should be able to recognize the calling number, gathering information as location, and forward

the call to the nearest Public Safety Answering Point (PSAP), the dispatch consoles are typically located in the points to manage the MCC groups and communication. The dispatchers, working for the PSAP, as 911, should be trained and equipped with tools to proper alert the agencies quickly, and to gather information about the caller as location. Then, that information should feed an incident management system where all PPDR agencies have access with its own CCC, but capable to integrate a unified incident control center with proper coordination and sharing of resources in case of a situation that needs integrated action (Ulema, 2019).

The incident management system should allow a nationwide interagency planning, coordination and action, with appropriate systems allowing integration of PPDR agencies and stakeholders. The center should have a set of procedures consistently describing the role of each agency when an incident takes place, including how the MCC system would be shared among EFRs from different agencies in the incident area. A National Incident Management System (NIMS) with a Unified Incident Command and Decision Support (UICDS), as projected by the Department of Homeland Security (DHS) in the USA, intending to share and manage incident information across states and PPDR agencies. NIMS and Incident Command System (ICS) have standardized procedures and policies to manage incidents, providing a common hierarchy from multiple organizations, with proper trainings, as the ones provided by Federal Emergency Management Agency, through the Emergency Management Institute (2023).

Public Warning System (PWS) are systems used to inform the population about emergency situations and provide lifesaving instructions as safe routs and procedures. In the USA there is integrated nationwide system for these purposes, the Integrated Public Alert and Warning System (IPAWS), managed by the Federal Emergency Management Agency (FEMA), and using standardized protocol named the Common Alerting Protocol (CAP). The system provides a single interface with other PWSs, as the Wireless Emergency Alerts (WEA), with messages broadcasted directly to cell phones in a certain region; the Emergency Alert System (EAS); and the National Oceanic and Atmospheric Administration (NOAA) Weather Radio (Ulema, 2019). These management systems are referred in Figure 30.

4.3.12 Paths for MCC in Smart City scenarios

Based on the models presented on the literature review, SLR and the use cases, Figure 30 was constructed considering some variations, presenting five paths for MCC in Smart City scenarios. It also shows the devices used by PPDR agencies in broadband networks. In this Figure, the smart wearable devices used by EFRs are referred as IoFRTs, and the IoPST are IoT devices used specifically for PPDR purposes. In case of private networks, the core belongs to the PS network. The core network sharing options are detailed in Figure 32.

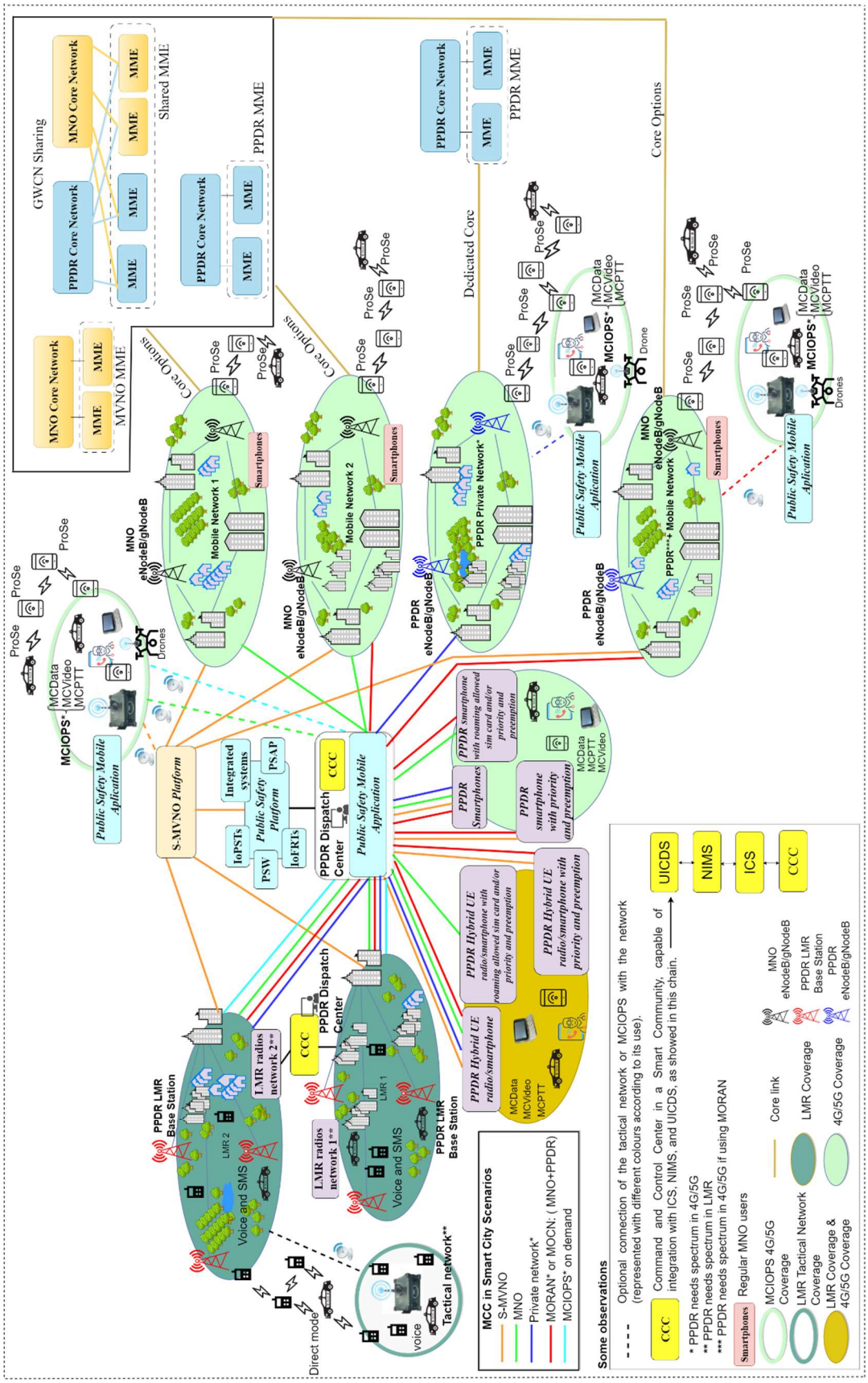


Figure 30 - Paths for MCC in Smart City scenarios (Author).

4.3.12.1 S-MVNO

It is possible to use coverage from multiple MNOs. In Figure 30, the coverage comes from MNO 1 and MNO 2, both connected to the S-MVNO platform, which has its own SIM card. If the PPDR network has spectrum in 4G or 5G, MCIOPS can be used connected to the S-MVNO, to improve coverage in a certain area. For example, a place where occurred a disaster and has no MNO coverage, that tactical network 4G or 5G can solve temporally the coverage problem, being possible acting isolated or connected to the network. As the S-MVNO has SIM cards, the UEs can change MNOs coverage due to roaming agreement. It is also possible to connect to MNOs with shared resources with PPDR, as shown in the picture as PPDR+MNO using MORAN or MOCN. It is also possible to connecting to legacy LMR networks through the S-MVNO Platform and a Public Safety Mobile Application (PSMA) installed in the 4G/5G UEs. Interworking of MCPTT and LMR is based on the 3GPP Interworking Function (IWF) standard.

The Public Safety Platform (PSP) in Figure 30 represents PS information sources as police databases, connected to the S-MVNO, receiving and sending information to IoPSTs, IoFRTs, integrated systems and the CCC. The PSP is also connected to the PSMA, which has a console to manage the communication groups as a dispatch center, and the application in the UEs. When using an MNO, the UEs from PPDR will share resources with the regular MNO users, represented in Figure 30 as the box "smartphones".

Since there are roaming agreements, the roaming allows the UE to user another network when the user is in an area not explored by the designated MNO. Meaning, the roaming is possible when the user changes the concession area, as moving to another country. If in the same region the MNO 1 and MNO 2 have the concession to operate the mobile service, an user can change from one MNO to another, because one of them has a bad coverage in the area, since the country regulations allows that changing. Allowing UEs to use the best coverage, changing MNOs according to the best signal, not according to the concession zone. That could be possible in an MVNO for PS, allowing the EFRs to always uses the MNO with the best coverage, through a multi-operator coverage. That is also a solution proposed by Lyfo (2023) through the Lyfo.NET, a software for switching between any mobile 4G/5G network, and the Lyfo.SIM, a sim card with access to all mobile networks.

The UEs could be hybrid devices radio/smartphone, meaning that the EFR can choose the network to use, for example, some places could have no MNO coverage, or the MNO could be in congestion due to a special event as a concert or soccer game, in those cases, the EFR could use the LMR network. The UEs could be PPDR smartphone without priority and preemption, meaning they are sharing equally the MNO resources with regular users, what is not recommended for PPDR purposes due to the risk of not having enough resource for MCC. Although, if the country legislation allowed differentiation, the PPDR smartphone should have priority and preemption, in that way, a MCC from PPDR smartphones will have priority usage

of the network to take precedence over a regular user and preemption allowing to take over resources assigned to lower priority users.

4.3.12.2 MNO and licensed shared access

Licensed Shared Access (LSA) is a concept-based spectrum sharing between PS and MNOs. At least locally, PS network remain most of the time available, not using the entire spectrum, being temporally and spatially available, which could be used for other purposes when unused, and get back to the PPDR uses when needed. The other way is also interesting, when PPDR needs supplementary resources for their network, and could get spectrum from MNO by managing spectrum sharing resources. Mercy et al. (2018) list possibilities for LSA cooperation, namely:

- Sharing resources as an LSA, where "the available spectrum of incumbent can be used by the LSA licensees with certain sharing rules included in the rights of use of spectrum granted to the licensees, thereby allowing all the licensees to provide a certain level of QoS" (Mercy et al., 2018, p. 1), this is suitable mainly when the EFRs needs the resources for non-critical applications.
- With the MNOs being obligated to give spectrum to the PPDR network in areas that are not covered by them.
- With the MNOs being obligated to give spectrum to the PPDR network during critical operations, in that situation, the MNO can design its network using wide spectrum and release spectrum when the EFRs need it.

Höyhtyä et al. (2018, p. 73573) also explored the LSA functionality. According to the authors, "on some occasions spectrum sharing technologies are crucial in finding suitable radio resources for communications e.g., when the current infrastructure has been damaged or lost". The paper demonstrated the LTE rapidly deployable network use case using LSA and sensing to find spectrum information for the available frequencies of the trial network. The MCC users can be the primary user in LSA, allowing MNOs to use their spectrum in some situations. Also, the MCC users can be the secondary user in LSA, accessing commercial bands in some conditions, the spectrum management can be made by the LSA functionality offering spectrum information for the rapidly deployed LTE network. The collaboration between MNOs and PPDR networks can be enabled by a political decision which can bring benefits for both parties.

That solutions can be also used for transportable and rapidly deployable network, as the applied cased in Finland in Hallio et al. (2019, p. 3), where the authors conclude "the possibility to combine TETRA networks and terminals and LTE smart devices with Airbus PTT application gives flexibility to arrange PPDR services in a cost-efficient way". The LSA evolution spectrum manager was used in the 2300 MHz band to control and dynamically manage the priorities of the transmissions, as shown in Figure 31.

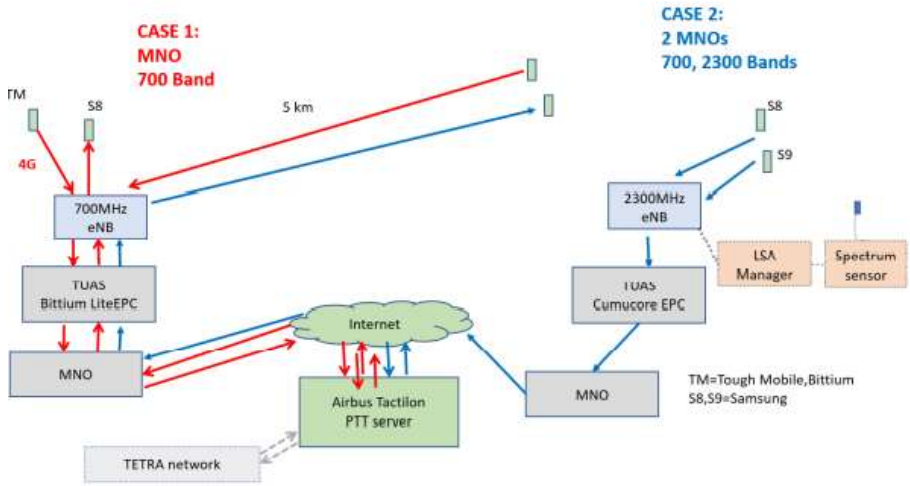


Figure 31 - Rapidly Deployable Network using MNOs and TETRA (Hallio et al., 2019, p. 3).

Regarding the use of MNOs, in Finland, Virve 2.0 project defined requirements for MNOs to provide a 3GPP standard based MCC broadband service for the Finnish PPDR community. According to Hallio et al. (2019, p. 1), "commercial mobile radio networks are a cost-effective option for critical communications due to a large ecosystem and a wide selection of affordable user equipment". The MNOs can be used without the need of an S-MVNO, as shown in Figure 30. In that case, the PSMA will manage the resources between users that could be from different MNOs, LMR legacy networks, or a MCIOPS.

Although, if the user changed area between MNOs, or the designated MNO has poor coverage compared with other MNO, the UE may not be able to do automatic roaming, depending on the country regulation for roaming. Meanwhile, it is possible to have UEs with roaming allowed sim card, as the one proposed by Lyfo, 2023, which is regulation dependent in some countries. The MNOs can also activate priority and preemption for the PPDR users, which is also regulation dependent.

4.3.12.3 Private network

In this case, the infrastructure is owned by the PPDR agency, having an LTE-based network and/or a 5G-based network to provide broadband services for MCC. Since one of the requirements of MCC networks are availability, guarantee by a broad coverage area. In that sense, should be needed many dedicated eNBs and gNBs, demanding a lot of time, and high values for Capital expenditure (Capex) and Operational expenditure (Opex). Although, this solution is perfectly suitable for PPDR purposes, being an ideal solution when it can be deployed achieving the PPDR agencies´ requirements (Jarwan et al., 2019).

4.3.12.4 Hybrid solutions

Hybrid solutions are the combination between MNOs and private networks uses for MCC purposes by sharing infrastructure and resources. According to Abdallah Jarwan et al., 2019, there are two ways for infrastructure sharing: passive, where radio equipment as base stations and towers can be shared; and active, where radio antennas and spectrum resources can be shared, as the use of MOCN, MORAN and the Gateway Core Network sharing (GWCN).

> In MOCN, the radio spectrum is shared, or pooled, between the PS operator and the commercial network operator. However, in MORAN, each operator uses its own dedicated radio frequencies. In GWCN, a part of LTE RAN and several MMEs are shared between the two operators. The radio spectrum in GWCN can be dedicated (as in MORAN) or shared (as in MOCN) between the operators. (Jarwan et al., 2019, p. 7)

However, the GWCN is a risk implementation for PS, since the MMEs are responsible for UEs authentication and authorization, being preferable that the Public Safety Network (PSN) has his own MME. Figure 32 shows types of sharing infrastructure, where the government can choose between: 1) The GWCH sharing, having its own core network, sharing the MMEs with MNOs and having the RAN using MOCN, or MORAN. 2) having its own core network, controlling the MMEs and using MOCN or MORAN for the RAN. 3) using the core network and MMEs from an MNO and using MOCN or MORAN for the RAN. In all the 3 cases the PSN can use dedicated spectrum, combined or not with the shared spectrum use, for example, a regular use by MOCN and an emergency use for MCIOPS with dedicated spectrum. Sharing the infrastructure enables faster deployment with low costs.

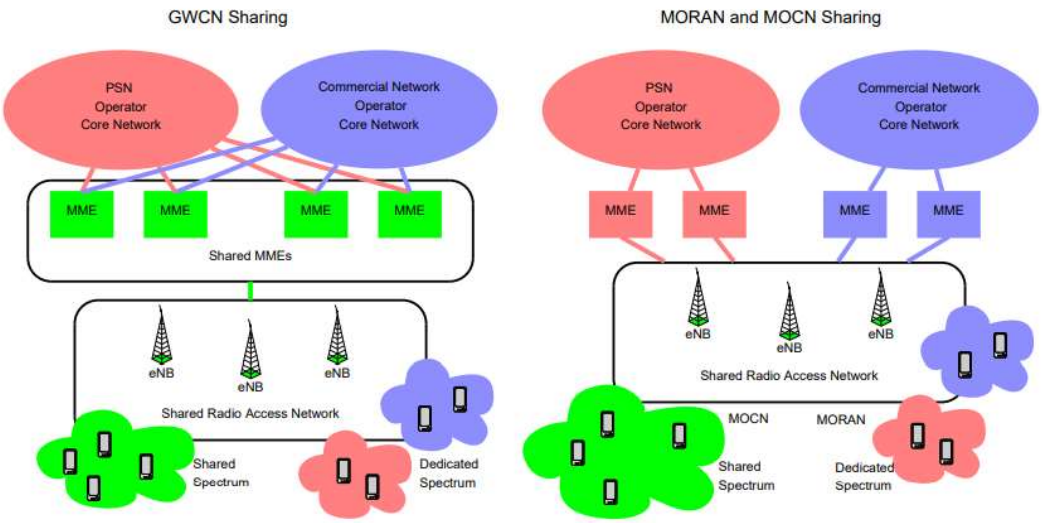


Figure 32 - LTE infrastructure sharing (Jarwan et al., 2019, p. 7).

Jarwan et al. (2019) suggest an evolutionary approach for broadband MCC: first, the services being delivered without mission critical requisites by MNOs or MVNOs. Second step

is GWCN, through RAN and MMEs sharing with MNOs. Third, PSNs sharing part of the RAN with MNOs. Last step is the separation of resources, having a dedicated MCC LTE-based network fully supporting PS requirements, although, that ideal solution demands a very high investment. That suggestion shows four levels of network dependency on MNO resources, not necessarily the network must follow these steps and "evolve" to the last step. For this, each applied case must be analyzed, adapting to local needs and resource availability.

4.3.12.5 Following the paths of MCC in Smart City scenarios

Intending to construct the new MCC broadband network, first thing that the government and the PPDR agencies needs to check is if their country has designated spectrum to build the new MCC broadband network, and if the bandwidth is enough to deliver the broadband services. Having that as a primary assumption, the rollout options could be checked.

The first rollout option is using the existing MNOs. The issues in that use are that the PPDR agencies has no control of the subscriber management, and the PPDR agencies must use the SIM Cards from the MNOs. The PPDR agencies have no control of the coverage and have no traffic separation from regular users. The benefits are that the PPDR agencies will have the availability of a broadband network in a very fast time, depending only on a contract between the agencies and the MNO, without the need of build up any infrastructure.

That use could lead to some issues, for example, when the PPDR agency need to act in remote areas, such as Amazonia rainforest in Brazil, maybe in the location there is no MNO coverage, although, there is LMR coverage from the legacy network, in that sense, an integration between networks could be done, allowing the EFRs to use the MNO when there is coverage and the LMR when there is no MNO coverage, acting in this way the EFRs will have limited resources, mostly voice, but will not be without communicate with the dispatch center. That could be possible using hybrid devices with LTE sim cards and also act as an LMR radio.

For that happen it is necessary integrate the LTE and LMR system, which could be done by a donor radio providing voice integration through a VoIP gateway as JPS (JPS, 2023). Integrating a communication group from a radio to another system, as the Federal Police of Brazil did on the crash of the Air France flight 447, in route from Rio de Janeiro to Paris. That happened in 2009 and the Federal Police had in that time a TETRAPOL network installed in Fernando de Noronha island, but not integrated with the trunked national network (Lyra, 2009). Meanwhile, the forensic experts in the cities of Brasilia and Recife needed to receiver the information in a secure way, with strong cryptography in place due to the sensitive information about the victim's identification. In that sense, the JPS was taking in place, connecting a donor radio in Fernando de Noronha Island (the closest place near by the accident location) to a JPS gateway, connecting it to a satellite communication and receiving that in Recife, where other JPS were connect to the internet, receiving the encrypted communication, and feeding other TETRAPOL radio connected with a national group communication in the trunked system.

In that case the connection was with the same system, in Fernando de Noronha island there was a tactical network, and in Recife there was a trunked system connect with nationwide TETRAPOL network. That integration could be done to another network as an LTE network, but in that case, the TETRAPOL cryptography would be lost and the security on the LTE side would be done by the LTE network. Another alternative is to use gateways as the Motorola motobridge (Motorola Solutions, 2023), which allows to integrate voice in different networks.

Motobridge was the solution used during the FIFA world cup in Brazil in some CCC, as the one in Pernambuco state. In that sense, if any emergency happened and it was needed to integrate the communication between agencies using different LMR networks as P25 and TETRAPOL, that could be done by the gateway. There are different solutions for integrate LMR with LTE, but the LMR´s side is not standardized and vendor dependent, meanwhile, the 3GPP´s side is standardized, and that could be done by the IWF. The Public Safety applications also have a software to operate as the dispatch center, executing similar LMR networks functions such as managing the communication groups and the users, as shown in Figure 33.

Figure 33 - Streamwide solution executing functions of dispatch center (Author).

In Figure 30, that is represented by the Mobile Network 1, using the MNO core network option, connected with the Public Safety Mobile Application, that is in fact installed in the PPDR smartphones or PPDR hybrid UEs (LMR+LTE) with no priority and preemption and no roaming allowed SIM card. The resources of that application are managed by the Public Safety Platform, which is an IWF platform that could integrate data resources from other systems. At that point, a connection with the LMR system could be made, allowing integration with the LMR legacy system, represented in Figure 30 as LMR1 and LMR2 — which refers to different LMR networks in different agencies, e.g., the Federal Police using TETRAPOL and the fire brigades using P25.

Following the green line in Figure 30, it is possible to use more the one MNO network if the country legislation allows the national roaming for PPDR purpose. In that sense, the UE can change the coverage between the Mobile Network 1 and the Mobile Network 2, the SIM Card will manage that change. The purpose of that is increase the availability, changing MNOs according to the coverage. Another option to increase availability, that is also regulation dependent, is allow priority and preemption for the PPDR devices, which will give priority in the use of commercial MNOs. In Australia the Telstra, and in USA the AT&T, are MNOs making using of priority and preemption to the EFRs, although, the PPDR broadband networks works

in different models, as are explained below. Also, the shared network model already has been adopted in the US (FirstNet), the UK (ESN) and Finland (Virve2) but using only one MNO.

If the PPDR agencies have designated frequency in broadband, they can operate a MCIOPS in isolated areas with no MNO coverage, as a tactical bubble to provide a temporary coverage in an emergency. The MCIOPS can works isolated from the network, and the UEs can communicate using the Public Safety application. Meanwhile, it is also possible to integrated that with the network through Internet Protocol (IP) connection, and the dispatch center can manage the communication groups between the EFRs in MNO and MCIOPS coverage.

Intending to reduce the security risks when using the MNOs, PPDR agencies can use the RAN from MNOs, and implement a private core. In that way, the PPDR agencies can have control of the subscriber's database. An intermediate solution is to have partial control of the subscriber's database, the shared MME. Both solutions are shown in Figure 30 on the right top.

About the S-MVNO, represented by the orange line, through the S-MVNO platform it is possible to use the coverage from different MNOs, represented in Figure 30 as Mobile Network 1 and Mobile Network 2. In that case, the EFR will use the SIM cards from the S-MVNO, as it happens in Mexico, and through roaming agreements it is possible to change between different MNOs coverage, with no need for a SIM card with allowed national roaming, since that could be managed by the S-MVNO.

The core option for that use is the S-MVNO having control of the subscribers, and not necessarily the core belongs to the PPDR agencies. In Mexico the core belongs to AIRBUS, which is an MVNO operator dedicated to Public Safety, attached to the MVNE of the Red Compartida, ALTRAN. In Mexico the EFRs smartphones uses the SIM Card from the AIRBUS S-MVNO, the Public Safety application in use is the Agnet, an application developed in partnership with Streamwide and used by AIRBUS. The Agnet has also an instance in laptops to works as a dispatch center, and the application has integration with the nationwide LMR network of the Mexican Federal Police, which is TETRAPOL and an AIRBUS solution. Since the S-MVNO operator and the LMR vendor are the same, there is no issue about the integration of the two systems. The connection with the MNOs could have priority and preemption to increase availability, also, making use of hybrid devices to make use of the LMR coverage in places where there is no MNO coverage. If the PPDR agency has designed spectrum for broadband, they can make use of MCIOPS integrated or not to the network.

The S-MVNO is connected to MNOs, it is possible to improve the RAN coverage through MORAN or MOCN solutions, is the case represented by the orange line connect to the bubble representing the PPDR + MNO solution. In that scenario, the PPDR agencies can improve the coverage developing some RANs, making use of the MNO coverage and coverage improvements as MORAN or MOCN. In the UK the PPDR agencies uses the coverage of the commercial MNO EE and installed some g-nodeBs, the PPDR agencies doesn't have dedicated frequency spectrum, making use of the EE spectrum. The PPDR can also develop their own

core, having full control of the subscriber database, with PPDR agencies developing their own S-MVNO, and not being operate by a commercial partner as happens in Mexico.

In Australia a proof-of-concept trial, which began in April 2021, tested a shared-network PS Mobile Broadband model, showcased the benefits of the government operating the core network and applications, while utilizing the RAN of two MNOs (TPGT Telecom and Optus) to enhance coverage, reliability and resilience. It is an initiative between Nokia, TPGT Telecom and Optus, that signed a contract with the New South Wales Telco Authority to deliver the POC. It is an MVNO deployment model, using two MNOs where the PPDR agencies have control of the core, in such scenario, the PPDR agencies can either possesses their own spectrum and the dedicated core can facilitate multi-carrier roaming, which is an area where commercial carriers can contribute. In that POC, Nokia provided a 5G-ready core network for the PPDR agencies, MCPTT and an interworking gateway with the legacy LMR system (P-25) (Critical Comms, 2022).

The hybrid solution is shown in Figure 30 with the red line. The USA developed a hybrid solution, the project was built in a public-private collaboration between the FirstNet Authority and the commercial MNO AT&T. FirstNet is "an independent authority within the U.S. Department of Commerce, tasked with ensuring the establishment of a nationwide interoperable public safety broadband network. FirstNet is the single, nationwide licensee of the 700 MHz public safety broadband spectrum" (Federal Communication Commission, 2018). The mission of the FirstNet Authority is to ensure the deployment and operation of the nationwide public safety broadband network. The Spectrum Act allocated about US$7 billion to start the construction of the new infrastructure. Nevertheless, the major portion of funding is contributed by AT&T. It is estimated that over the course of the 25 years consortium, AT&T will invest over US$40 billion in the construction and operation of Band 14 (Locke, 2022).

AT&T built a dedicated core for PPDR purposes, where the PPDR agencies have complete control of the subscriber's database. The PPDR agencies also have a dedicated spectrum frequency in 700MHz (2x10 MHz), which is nationwide allocated, and the FirstNet Authority allows commercial users in this dedicated band, being a shared band in normal situations. When an emergency happens and the PPDR agencies needs dedicated spectrum, the system has mechanisms to diver the commercial traffic to other bands, or even drop the traffic, releasing the PPDR dedicated spectrum to work in a dedicated mode for PPDR purposes.

Being clear that "The FirstNet network, powered by AT&T, does not exclusively operate on Band 14. And Band 14 is not exclusive to FirstNet", AT&T give access to FirstNet users in all bands that they operate, with priority and preemption over non-FirstNet users, in exchange, in normal situations AT&T can run commercial traffic on band 14, however, if an emergency occurs, AT&T will give priority and preemption to the FirstNet users and release the band 14 to be used exclusively for the EFRs, allowing EFRs, city services and critical infrastructure to continue operate, even during an emergency (Locke, 2022). With that model of sharing

spectrum, the FirstNet Authority can, in a certain way, monetize the use of the dedicated spectrum when that doesn't need to be dedicated, which could help to pay the system.

The USA use case is a hybrid solution where the FirstNet Authority has control of the dedicated 4G core, with QoS, priority and preemption, offering services as: end-to-end encryption; security monitoring 24 hours/7 days by a dedicated team at the Security Operations Center (SOC); superior reliability and availability due to have core network elements geographically distributed across multiple locations; local control with customization of priority levels, empowering local responders to take charge, by doing so, incident commanders and eligible EFRs can prioritize their responses according to specific situational needs; mission-critical functions, supporting a range of next-generation PS capabilities based on open standards, such as, MCPTT and enhanced location-based services (Bratcher, 2018).

The dedicated core connects a variety of elements, such as the RAN, which allows access to a variety of devices, including phones and IoT devices, also allowing to evolve for 5G, which will have more decentralized architecture, breaking the core into smaller pieces and locate them all over the network, increasing resilience, security, availability, and latency by putting the users closer to the network processing computing, allowing video intelligence solutions, real-time situation awareness and augmented reality services (The FirstNet Authority, 2023). FirstNet also implement their own dedicated RAN in band 14 across the nation, complementing the AT&T RAN coverage (Hardesty, 2022). Band 14 offers another advantage, as it has permission to the use of high-power user equipment within its frequency range. This feature allows signals to travel over greater distances from the UE due to the higher power in uplink.

In the MCC broadband network, the PPDR agencies makes use of applications (app)s designed to attend their needs, in the FirstNet example, the apps are available in the FirstNet application catalog, working as a store application for PPDR purposes with certified apps that passed in stringent security assessment (The FirstNet Authority, 2023). In a hybrid solution, if PPDR agencies have designed spectrum, they can make use of MCIOPS integrated on not to the network. In the USA the FirstNet has PPDR MME, although, another country can develop a solution improving the RAN coverage through MORAN or MOCN and not having PPDR MME, or having a shared MME, as shown in Figure 30.

About the UEs, in the case of the PPDR agencies having their own core, that is designed intending to have full control of the subscriber´s data base, seaming that is not a desire situation having EFRs controlled by another core, in that way, makes sense to not having devices with roaming allowed SIM Cards. Instead, have UEs in use by the EFRs, such as, regular smartphones, smartphones with priority and preemption, hybrid UEs, and hybrid UEs with priority and preemption, as shown in Figure 30. Meanwhile, if a country will not develop a PPDR MME in the PPDR + Mobile Network mode, they can make use of the roaming allowed SIM Card resource, which could enable the use of a prior MNO as the one that they increase the

coverage with MORAN or MOCN, also enabling the use of a secondary MNO, in case of better coverage, as shown in Figure 30 by the connection with the Mobile Network 2.

About the integration with the LMR legacy network, that can increase the resilience and availability of the entire system due having another mature technology that could be used as complementary service or backup, also allowing a smooth transition between the narrowband and broadband system. That is the recommendation of U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency (2020).

About the private network, represented by the blue line in Figure 30, dedicated RAN is built up using specific band, with dedicated core and dedicated RAN having only EFRs using the network. That is represented in Figure 30 by the bubble indicated by PPDR Private Network, that could also have MCIOPS working isolated or integrated to the network. About the UEs, since the PPDR agencies have full control of RAN and core, there is no need of priority and preemption considering that only EFRs made use of the RANs, not disputing the resources with regular users. The intention of having its own core is to have full control of subscriber's database, seaming that the roaming allowed SIM Card will not play a role in that scenario. About the integration with the LMR legacy network, as the hybrid scenario presented before, that can increase the resilience and availability of the entire system.

The MCIOPS on demand scenario, shown in Figure 30 as the light blue line, is an option to continue using the LMR network, and makes use of a tactical broadband network just in situations where it is needed, which can work isolated or integrated with the LMR network, by the Public Safety Platform. For that, the PPDR agency need to have designated spectrum in 4G and/or 5G. That use just for an emergency scenario that demands broadband services as videos, was what happened in the rescue of the children in a cave in Thailand in 2018. It was possible to communicate via voice and video with the children inside the cave, helping with the rescue, and enabling communication between the children and their families. For that, the PPDR agencies made use of a tactical equipment in LTE, named eLTE Rapid Deployment Broadband Trunking System, a portable LTE equipment design for emergency response, which integrates the functions of core, base station, and dispatching system (Huawei, 2018; 2023).

The MCIOPS can be deployed by drones in emergency scenarios, as described in previous sections about solutions to be used in disasters, that is described in Figure 30 using drones with transmitters instead the use of the black box with transmitters, or even complementing the black box transmitters coverage. The black box represents a tactical 4G/5G solution intending to create the MCIOPS 4G/5G coverage. In all 4G/5G scenarios, the ProSe should allow the direct mode communication, meanwhile, since the frequency ranger is higher than the ones used in LMR (some countries have LMR networks in 400MHz and others in 700MHz, and the regular 4G spectrum starts in 800MHz going up, in the case of 5G, that also starts in 800MHz, the most common is nearby 3.5GHz, which could go up to millimeters waves), the range of coverage in the same conditions will be low, also, the LMR radios have higher power in uplink,

which also helps to increase the direct mode reach compared with 4G and 5G, even in the bands that are allowed to have higher power UEs, as the case of band 14 in the USA. Another issue is about the direct mode operation for 4G and 5G, even with all efforts made by 3GPP, that still faces problems to become a regular function in 4G networks, as pointed out by the MCC expert during interviews, which is presented in the chapter 6.

4.3.13 4G and 5G, main issues in the use for MCC broadband services

One of the biggest concerns when integrating MCC services into 4G and 5G networks are security and privacy aspects. Sicari et al. (2020) gives an overview of the security and privacy issues in 5G, investigating data integrity, confidentiality, authentication, access control, non-repudiation, trust, privacy, identity management, key management, policy enforcement, and intrusion detection. The paper pointed out the importance of fog computing and blockchain paradigms, questioning the level of reliability to 5G-IoT systems about data protection. According to the authors, the encryption mechanisms play a central role, where the ciphering techniques should ensure the data protection and not compromise 5G efficiency.

The security requirements of PS network include the needs for strong security mechanisms as: mutual authentication schemes; end-to-end security through data encryption; secure access to databases with restrict access to avoid data leakage; data authentication and acknowledgment of communications; intrusion detection; strong firewall, among others. Also, the physical layer should be protected against jamming attacks[20] and eavesdropping[21].

With respect to access control and authentication, according to Sicari et al. (2020), traditional public key infrastructure-based authentication schemes provide networks with identity authentication, and conditional privacy protection, which are not enough to ensure the reliability of information. The authors highlighted that a distribute architecture from the combination of 5G and fog computing can give a good efficiency in granting access tokens to authorized parties and the fog computing platform can distribute trust authority to authorize access. That approach is needed because of the dimension of future 5G-IoT networks, being necessary to distribute the tasks to perform. Also, 5G requires a sort of chain trust, considering all the entities involved. The end devices are vulnerable to physical attacks as they are far from the main network, they should also be protected against hardware tampering and interception. With distributed architecture the remote management became the usual, which increase the risks of attacks, being important to analyze how to improve the trust and rogue node detection.

[20] Cyberattack in which an attacker transfers interfering signals on a wireless network intentionally to disrupt the communication.

[21] Cyberattack in which an attacker intercepts, deletes, or modify data that is transmitted between devices.

Considering hybrid architecture, where broadband MCC will connect through MNOs, Suomalainen et al. (2021) survey security architecture and enablers for MCC in 5G, identifying security threats, vulnerabilities, threat actors, and risk levels. The resilience and availability of the networks are other concerns when integrate MCC services into 4G and 5G networks. The network should be scalable and reconfigurable, and also, be available where it is needs. For a disaster situation, according to Debnath et al. (2022), the functional operational area of disaster communication is: emergency crisis in urban area; natural disaster in a rural area; cross-border law enforcement; major event; and indoor scenario. Also, in disaster situations leads to congestion in the network and the 4G/5G network should have some strategy to assure the network service for the disaster affected users and EFRs users, in case of a shared network.

According to Chamola et al. (2020), ML algorithms are very effective to tackle the congestion issue, handling multidimensional and vast volumes of data generated in the network, also, the algorithms utilizing data from users are useful for finding victims and evacuation route for the victims, improving the information quality and accuracy to the EFRs.

About availability, Ahmad and Chang (2019) propose an efficient user priority–based random-access scheme for coexisting LTE MC networks. In the paper there are LTE-based PS and LTE-based marine networks, as happened in Republic of Korea where the same 700 MHz band is allocated to more than one network. Since the PS users has higher priority, the access is granted by allocating RACH resources in the contention-based random-access (RA) procedure. The authors propose a scheme to assign RA preambles for PS users intending to avoid preamble collisions in multiple access situation between the PS and marine users.

Ahmad and Chang (2020) address the same issue about coexisting LTE MC networks, intending to mitigate the co-channel interference and guarantee the QoS prioritization and MC user requirements, through employing user priority-based resource allocation schemes based on Coordinated Scheduling (CS), Coordinated MultiPoint (CoMP), and Intercell Interference Cancellation (ICIC) in RAN-sharing environment. The proposed solution was implemented in three LTE PS networks, sharing the same 700MHz band in Republic of Korea. The simulation results shows that when CS CoMP are implemented by muting the neighboring interfering BSs, it is observed an improvement in cell-edge-user performance and throughput for coexisting networks. When ICIC with CS CoMP are implemented, the networks achieve higher performance and provides fewer outages than RAN sharing with CS CoMP only.

Debnath et al. (2022) pointed out the D2D communication available in 5G, which can be used for effective disaster recovery as an 4G/5G underlay network for nearby PPDR users in 4G/5G dedicated and commercial network. The paper presented several researches in the last years, providing an overview of the existing technologies and recent development in the field of emergency communication, some of them with integration of 4G and 5G technologies.

The idea of ProSe via D2D communication is "to form an ad-hoc network where certain nodes of the network (which may still have access to an operational cellular infrastructure in a

post-disaster situation) can act as gateways to extend network coverage to isolated nodes" (Hayajneh et al., 2018, p. 26216). In Zhou et al. (2020) a drone operates in emergency communication as a supplementary network, broadcasting emergency messages to ground devices and users in PS scenarios using D2D communication. An emergency alert message is broadcasted by the drone and then the users which successful received the message become the active transmitters and multicasted by the D2D users using D2D links. According to the authors, under practical setups, the cell edge user located 2 km from the ground projection of the drone reach the link coverage probability around 90% with a drone height as low as 200 m, providing on-demand communication for EFRs and victims in a disaster, even in the case that the existing terrestrial infrastructures were partially or completely damaged.

Drones can be used to provide coverage after disaster, Drone-based Small Cellular Networks (DSCN)s can be rapidly deployed to fill coverage in case of damages in the terrestrial infrastructures, although, due to capacity and back-hauling limitations on Drone Small Cells (DSC)s, to have a coverage in an area is necessary a multitude of DSCs. As in a post disaster scenario users tend to cluster in one location, Hayajneh et al. (2018) propose a clustered deployment of DSCs and studied the coverage probability and energy efficiency for that use. According to the authors, both, D2D and DSCNs will complement the LMR networks.

The coverage performance for drone wireless networks is also analyzed by Liu et al. (2018) considering three path-loss models and comparing the Line-of-Sight (LoS) probability functions for the different path loss model. The research considers practical values for drone heights around 50~100 meters. Selim and Kamal (2018) proposed a 4G/5G drone-based communication to provide cellular coverage in places affected by disasters where the terrestrial infrastructure is totally damaged. The proposed solution intending to minimize the drones' energy consumption, guaranteeing a minimum rate for the users, and determining the better placement of these drones.

Even with the deployment of UAVs networks in a post-disaster scenario, congestions can still occur, which can increase the latency of delivering messages. Intending to relieve the backhaul and minimize the post-disaster congestion in the deployed UAV network, Wang et al. (2020) proposes that imperative contents, as evacuation routes, can be cached by the EFR devices and quickly provided to victims by D2D transmissions, without the use of UAVs' backhaul. That is a case of using both, D2D and DSCNs at the same time in disaster scenarios, intending to achieve better results.

Another strategy is the use of satellites because it does not depend on the existing terrestrial infrastructure network. In Zhou et al. (2021) an integrated satellite-ground post-disaster emergency communication network is proposed, where the nodes of the network including Mesh access point nodes, and satellite portable stations with rapid deployment in a shorter time, achieving higher data transmission bandwidth and small transmission delay. Satellite solutions can be deployed in hybridization with LTE, providing LTE services with the

reliability of satellite communication for PPDR purposes, with a suitable architectural solution able to meet MC requirements (Debnath et al., 2022; Casoni et al., 2015). With 5G the Non-Terrestrial Network (NTN) is expected to provide high-speed broadband coverage to isolated areas and can be also used for disaster situation, allowing satellites to be used as BSs.

Also, when IoPST, as fire alarms and gas leak detectors, are connected through an MNO, if the MNO is disrupted by a disaster, these devices may become useless. New protocols, as the one suggested by Park et al. (2022) with a new self-organized low-power multihop failover protocol, intending to solve this problem. If the MNO is paralyzed by a failure, the proposed protocol recovers the communication by forming a detour route using a secondary network with a failover process without centralized control, performed autonomously by self-organization and collaboration of distributed nodes, routing to areas where the MNO normally operates. In the paper a 447 MHz narrowband wireless network is used as secondary network, which is activated only at the moment when network failover is necessary, being a low-power relay. The nodes are equipped with a communication module in the same frequency designated for PS systems in the Republic of Korea.

IoT's critical communication can also be done by D2D communication and UE-to-Network Relay standards defined by 3GPP, where devices that cannot connect to a BS communicate with adjacent devices connected by D2D communication. Also, the deploying of temporary BSs in disaster areas through balloons, vehicles and UAVs, as cited before, are solutions intending to solve the communication problems during a disaster.

Despite all the use cases found about the use of LTE for MCC, according to Sanchoyerto et al. (2019), despite the 3GPP effort of standardizing the MCPTT service, intending to leverage 4G and 5G broadband networks to get closer to the performance of LMR voice, the MCPTT service deployed over an LTE network still has some issues to reach the KPIs defined by 3GPP under any circumstances. This affirmation is based on testbed experimental results. Although, the authors pointed out that the KPIs can be reached through 5G with the offer of low latency services for MCC, also, MEC, SDN and NFV can be used intending to reach those KPIs.

During normal scenarios 4G can meet PS requirements, although, during emergency and disaster scenarios, the 5G functionalities are essential for improving the network, but even with the improvement, according to Othman and Nayan (2021, p. 11), based on a review of existing solutions to meet PS requirements "substantial research efforts are necessary to improve these functionalities to meet the rigid requirements of public safety use cases in terms of network slice reliability, resilience, and security, especially during the emergency and disaster scenarios".

The 5G can reach the PS requirements in normal scenarios, as in Chochliouros et al. (2021), testing with success the use of MCPTT in the context of the 5G ESSENCE project, which promotes a cloud-enabled small cell infrastructure with a fully distributed orchestration architecture, sharing the 5G infrastructure in an emergency scenario between EFRs and civilians. Although, that is not yet guarantee for rush scenarios as disaster.

Also, other techniques, such as network slicing and Licensed Shared Access (LSA) can improve the support of MC applications in any environment, as demonstrated by Höyhtyä et al. (2018) in a real network, enabling priority communications over an MNO and the rapidly deployable networks through spectrum sharing (LSA) for PPDR purposes. Also, softwarization and virtualization of the network resources can improve dynamicity. The authors demonstrate that the MCC users can receive a high-quality service in an MNO.

Other concern is that the system should provide efficient support for group-based communications services, since PS users normally work in groups and these services must be available in all scenarios. For this, 3GPP introduces Group Communication System Enabler (GCSE), and the evolved Multimedia Broadcast and Multicast Services (eMBMS). The GCSE is "a logical interface that facilitates the creation, management, and deletion of group communications, either through a centralized approach by a core network and an application server or a distributed approach by a BS" (Othman & Nayan, 2021, p. 5).

The eMBMS is designed to provide efficient delivery of broadcast and multicast services, allowing a single or more BSs to transmit the same radio signal to multiple users. That functionalities together with MCPTT should allow efficient group communication, reaching the KPIs described in 3GPP (2016) for MCPTT in a group communication.

High reliability is another concern, since the MCC services are related to real-time services, the VNF provided by 5G networks at the edge with latency constraints is essential to reach the QoS requirements related with real-time services. In the literature is possible to find several papers considering delay-sensitive utilization of fog resources, meaning that the researches about the topic are increasing and solutions for the use of 5G resources to reach MC communication and services. Also, the self-organized network (SON), which is described by 3GPP as a self-configuration, self-optimization and self-healing of the network, is applicable for post-disaster situations, improving the reliability.

The scientific papers demonstrate that even with certain limitations in some conditions, the 4G network is ready to improve MCC, and the 5G network will be even better to reach the PPDR communication requirements. For this, the network functionalities should be well-defined and explored according to the user needs.

4.3.14 Paving the way

The strategic high level architecture design by BroadMap in Figure 34 resumes the steps and needs for the transition from legacy PPDR narrowband systems to MCC broadband system. This picture refers to the transition expected in Europe, while the EU Member States and associated countries have the individual transition roadmap, dependent on the status of national decisions. Then, the SpiceNet reference architecture model describes a proposal to provide a foundation for the Pan European PPDR MCC broadband services.

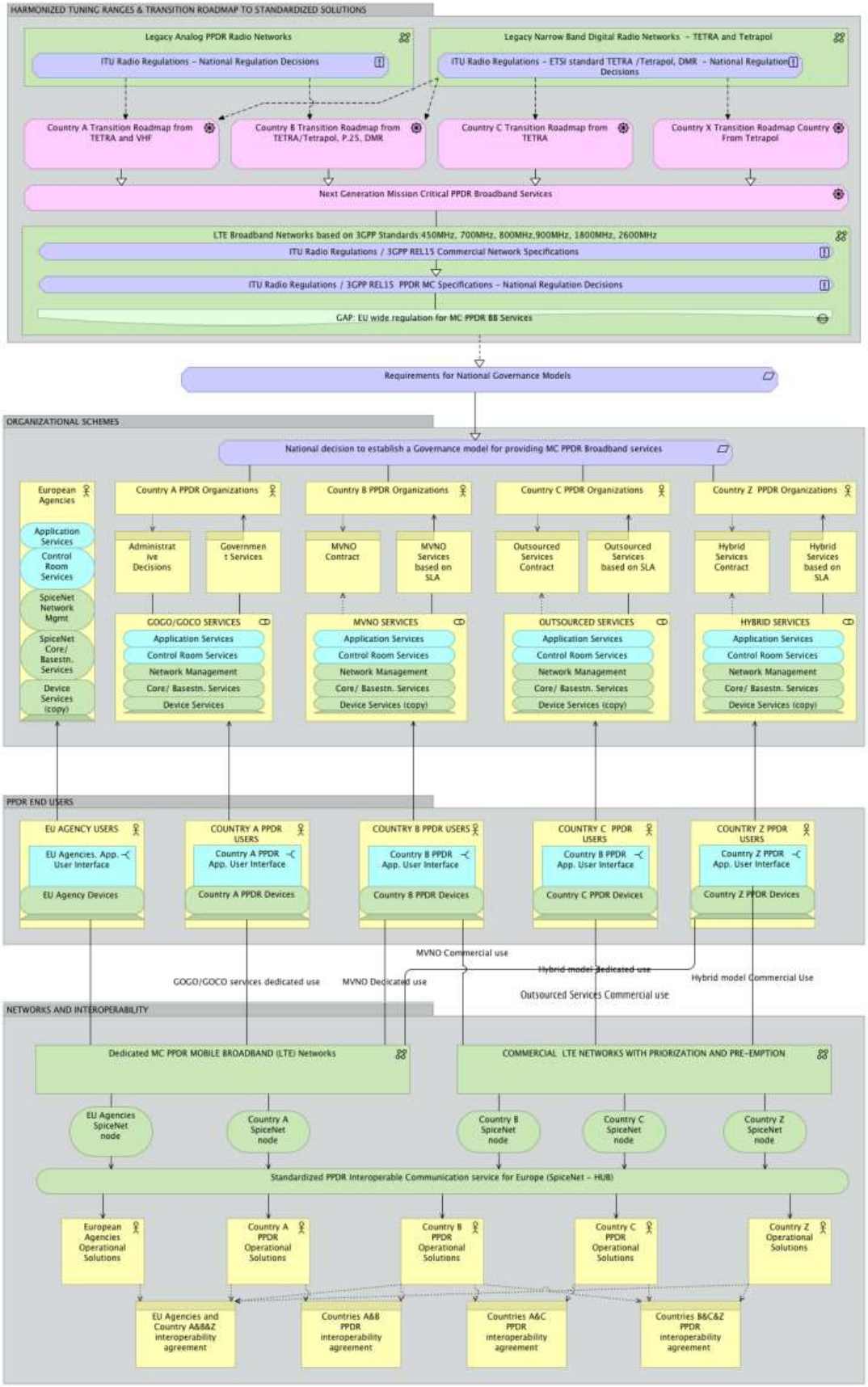


Figure 34 -SpiceNet strategic high-level architecture (BroadMap, 2017, D5.2 Annex 1, p. 3).

The high-level architecture model of the SpiceNet has four layers, namely: harmonization, referring to the transition to standardized solutions. Organizational schemes, referring to national decisions to establish a governance model for providing MCC broadband services. PPDR end users, referring to the services provided to the PPDR devices and EU devices. Networks and interoperability, referring to the networks models as dedicated LTE network, and commercial LTE network, used by the countries for PPDR purposes, and the standardized PPDR interoperable communication service, which makes possible the interoperability between countries and different agencies.

Figure 34 listed different countries, as the case of a PAN European network, and shows different ways for the transition, including a range of services models as MVNO and outsourced. Also, include different models of networks and reinforce the final goal to have a standardized PPDR interoperable MCC broadband service. Which is a good overview of technological options and steps that should be taken to reach the final goal. In a country with different types of networks used by different agencies, a national decision should be made to establish a governance model, but first, the regulations should be observed to make possible the development / implementation of the MCC broadband network.

The major requirements to be observed in the transition are listed in section 4.3.8, and the section 4.3.11 resumes the possible paths of MCC in Smart City scenarios. Figure 30 gives an overview of those paths. According to the literature review and SLR, the LTE technology-based should be the goal for the transition of MCC from narrowband to broadband, and a roadmap should be created toward this objective, considering different phases of activities.

According to Ulema (2019, p. 50),

> The alternatives that include more than one technology may be preferred for various reasons. For example, there may be existing deployment based on a technology that may not satisfy the established criteria and requirements. In this case, while deploying a new system based on another technology, the existing system may continue to serve alongside the other technology for the foreseeable future. Another reason for the dual technology consideration could be that one technology may not satisfy all the requirements. Therefore, the two technologies jointly provide full coverage of all the requirements.

Although, the author highlights that LTE technology-based should be the long-term goal. That is also the recommendation of U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency (2020, p. 36) to the statewide governance bodies and emergency communications leaders in USA:

> Emergency communications are accomplished through many technologies, each with varying capabilities, standards, and features. As the public safety community adopts new technologies, LMR will remain an important tool for mission-critical voice communications for emergency responders in the field for many years to come. Successful future planning requires a multi-path

approach in maintaining LMR systems' operability and interoperability while planning and deploying new emergency communications technologies. As such, grant recipients should invest in sustaining LMR capabilities while also planning for new technologies. As LMR and IP-based technologies continue to become integrated with one another, interoperability and cybersecurity become increasingly important.

However, for the long-term goal to be achieved is necessary clear understanding of what needs to be done and defining priorities. For the U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency (2020), the priorities are: priority 1: governance and leadership; priority 2: planning and procedures; priority 3: training, exercises, and evaluation; priority 4: activities that enhance communications coordination; priority 5: standards-based technology and infrastructure; priority 6: cybersecurity.

4.4 Metrics

This section presents some metrics for the Smart Emergency Management System.

4.4.1 Technology metrics

The International Telecommunication Union (ITU) specified the minimum requirements of technical performance for 4G and 5G in radio interface, described in ITU (2017) and shown in Figure 14. The requirements for 5G are summarized in Figure 35. The target values for 4G can be compared with the ones shown in Figure 14.

KPI No.	Description	Value	Key Use Case
K1	Density (devices/km^2)	$\geq$10,000	mMTC
K2	Mobility (km/h)	up to 500	eMBB
K3	Peak data rate	DL:20 Gbps, UL:10 Gbps	eMBB
K4	User Data Rate (Mbps)	DL:100, UL:50	eMBB
K5	User plane Latency (ms)	4 (eMBB), 1 (URLL)	eMBB, URLL
K6	Control plane Latency (ms)	20	eMBB, URLL
K7	Reliability	frame error rate $<10^{-5}$	URLL
K8	Availability (%)	>99	URLL

Figure 35 - KPIs to assess 5G performance in field trials (Marabissi et al., 2019, p. 8).

According to Marabissi et al. (2019), the use case of 5G in Smart Safety for Smart Cities can be classified as an eMBBB use case, measured using KPIs K3, K4 and K8 from Figure 35. Since the broadband MCCs are using 4G/5G networks, those KPIs should be analyzed to check the network performance. For MCPTT, the metrics could be the ones used by the 5G-ESSENCE project (Chochliouros et al., 2021) from 3GPP (2016). The lists of KPIs for MCPTT service and the target values suggested by 3GPP are detailed in Figure 36.

- MCPTT access time — defined as the time between the moment an MCPTT user requests to speak pressing the MCPTT button, and the moment this user gets a signal to start speaking, not including the confirmation time from receiving users.
- End-to-end MCPTT access time — defined as the time between the moment an MCPTT user requests to speak pressing the MCPTT button, and the moment this user gets a signal to start speaking, including the confirmation time from first receiving users (not applicable if no acknowledgement is requested during the MCPTT group transmission).
- Mouth-to-ear latency — defined as the time between an utterance by the transmitting user and the playback of the utterance at the receiving user's speaker.
- Late call entry time — defined as the time to join an ongoing MCPTT group call, from the moment an user decides to monitor an MCPTT group call to the moment the MCPTT UE's speaker starts playing audio.
- System response time — defined as the time required to deliver a chat message to all group members.
- Number of delivery failure — the number of messages that were not delivered during the period, since, after the delivery deadline, the time expires, and the messages are discarded.

KPI	Metrics	MCPTT Service	MCPTT Emergency Group Calls and Imminent Peril Calls
K1	MCPTT Access time	< 300 ms for 95% of all MCPTT Request	< 300 ms for 99% of all MCPTT Request
K2	End-to-end MCPTT Access time	< 1000 ms	
K3	Mouth-to-ear latency	< 300 ms for 95% of all all voice bursts	
KPI 4[a]	Late call entry time for calls without application layer encryption	< 150 ms for 95% of all Late call entry requests	
KPI 4[b]	Late call entry time for application layer encrypted calls	< 350 ms for 95% of all Late call entry requests	

Figure 36 - KPIs for MCPTT service (3GPP, 2016).

Lee et al. (2021) proposed a performance test call model of Mobility Management Equipment (MME), and System Architecture Evolution Gateway (SAE-GW) among core equipment for MCPTT. The existing performance test method for LTE defines a call model that includes Voice over LTE (VoLTE), and data service, being necessary defining a new call model with MCPTT, which is a representative service of MCC LTE, the Public Safety-LTE (PS-LTE).

Since the requirements for the MCPTT system capacity in Korea are 480,000 Busy Hour Register Attempts (BHRA) for registering, and 82.4 million Busy Hour Call Attempts (BHCA), the paper proposed the load conditions of the simulator for MCPTT system testing based on those requirements. The proposed call model and test methods are designed to be tested in commercial PS-LTE, which encompasses most use cases (in shared mode with PPDR resources), making that paper a reference for testing the PPDR network in broadband in the most used case model, and providing call model for performance testing, field test methods for MCPTT and eMBMS, and measurement of wireless coverage and quality.

The measures suggested by Lee et al., (2021) are described in Figure 37. Also, the mobile BSs should be tested for data communication, voice and video PTT functions in terms of interoperability, call quality, and coverage. The test content and criteria for this are described in Figure 38.

Measures of a call model with MCPTT services
Time related to the process of MCPTT registration in BHRA and MCPTT service in BHCA.
Time and number of transactions related to the process of call connection/disconnection and voice/video call and general traffic to each subsystem of the MME core.
Time, number of transactions and throughput per subscriber intending to evaluate the capacity and performance of SAE-GW.
KPIs to measure MCPTT voice channel of the terminal for a group call.
Packet analysis of MBMS service.
Coverage measurement test with the measurement of RSRP value in certain areas throught RF scanners installed in vehicles (drive test).
Quality measurement of call voice, individual call text, individual call video voice group call, text group call, and video group call, with measurement of time for each call.
Data measurement by repetedly downloading and uploading files.
Individual and group voice calls should be measured as recommended by standarts associations as ITU, ETSI and 3GPP, using indicators as connection success rate; dropped call rate; voice quality and call success rate.

Figure 37 - Measures of a call model with MCPTT suggested by Lee et al., (2021) (Author).

Category	Test Content	Test Criteria
Convenience	The ability to move the mobile base station quickly and provide immediate service in the field	- Availability of self-organization network feature - Subscriber registration and group creation - Required time for service provision - Convenience of antenna installation and appropriateness of antenna type for each wireless environment - Expansion of call capacity - MCPTT function based on 3GPP Rel13
Coverage	Coverage by wireless environment	Effective coverage measurement (downtown area, empty site, and mountainous areas)
Interoperability	Handover testing (RAN sharing, etc.) - Mobile station (normal type) ↔ Fixed station (PS-LTE) - Mobile station (general type) ↔ other communication networks (commercial networks/LTE-R/LTE-M)	- Availability of S1/X2 handover - Availability of intra/inter-RAT handover - Availability of idle mode mobility - Parameter applicability for RAN sharing (neighbor list, PLMN, etc.)
Call quality	- Individual call quality (voice/video) - Group call quality (voice/video)	Call service based on quality verification indicators

Figure 38 - Mobile base station test items (Lee et al., 2021, p. 17).

MCC requires a resilient and reliable network. In that sense, one of the essential KPIs is the level of resilience, a Quality of Resilience (QoR) metric as suggest by Deepak et al. (2019),

presenting three network scenarios, and the QoR analysis for those scenarios, as shown in Figure 39. The scenarios are congested network, partially connected network, and isolated network. As a suggestion for QoR metrics, a score could be calculated according to the techniques described in Figure 38, and it may or may not be used by the network in the three different scenarios.

Network scenarios	QoR improvement techniques to facilitate post-disaster communication
Congested network	• User traffic classification and prioritizing the user groups by analyzing received data • Advanced call and data buffering and queuing protocols to minimize connection loss • Machine learning based user grouping and association for efficient multicasting
Partially connected network	• Efficient switching protocol from the cellular to D2D communication mode and vice-versa • Multiple hop formation in a self-organized manner to the working base stations • Low signaling overhead and energy efficient distributed network protocols
Isolated network	• Fast deployment of new network, for example, MANET, UAVs, manually or enable Multi-hop D2D communication • Optimal trajectory and altitude for UAVs, energy efficient signaling protocols for MANETs • Multiple routing paths to reach to the working base stations and the backhaul network

Figure 39 - QoR improvement techniques for post-disaster scenarios (Deepak et al., 2019, p. 137).

When the network is on air, to consistently maintain and manage service quality on the PPDR network, it is necessary to establish indicators for a Service Level Agreement (SLA), and sensoring the traffic for the IoT devices involved. Meaning, after the establishment of the network, that should be tested to verify if the network reaches the PPDR requirements, continue quality and availability test should be applied, in order to maintain the quality in the process of operating PPDR networks integrated with an emergency management system of the city. For this, SLA should be defined and measured regularly over time.

4.4.2 Society metrics

Regarding society, Freire (2019) proposes measuring the cost of crime and comparing to the reduction of costs due to a broadband solution able to improve the PPDR response. In society, the cost of crime, violence and natural disasters can be measured by the lives lost, lives affected, and financial losses. In Brazil, for example, the cost of crime grew substantially between 1996 and 2015, with an average increase of 4.5% per year (Secretaria de Assuntos Estratégicos da Presidência da República do Brasil, 2018).

The cost of crime and violence in Brazil totaled US$75.894 billion in 2014, which represents 3.14% of the Gross Domestic Product (GDP), according to the Inter-American Development Bank (IDB) (Caprirolo et al., 2017), and 4.38% of the GDP in 2015, according to the Secretariat for Strategic Affairs of the Presidency of the Republic of Brazil (2018) (Secretaria de Assuntos Estratégicos da Presidência da República do Brasil, 2018).

According to Grous (2013), by using broadband MCC, "the UK police may be able to achieve productivity gains of 5-20% savings". Considering 5% as reference and using that value as saving in cost of crimes, a projection shows that if the adoption of technology could result in a 5% reduction in the costs of crime in Brazil, which would mean US$3.79 billion in annual savings, considering the IDB value for 2014; considering the projection of spending growth from the previous decade, current savings should be even higher. The economic costs alone – not forgetting there are also social costs and other impacts of crime on society – would be enough to justify the implementation of more effective technology, capable of promoting improvement either as an incremental or disruptive innovation.

People's well-being cannot be measured directly; however, using available data, it is possible to obtain an approximation of the well-being costs imposed by crime on the population. It is impossible to measure the effective value of the loss of a life: this calculation would have moral implications that are intangible. However, it is possible to measure the loss of productive capacity due to the reduction of the workforce. Meanwhile, there is no single methodology capable of incorporating all welfare losses, and different types of methodologies generate different estimates.

Authors such as Becker (1968), Stigler (1970) and Ehrlich (1973) calculate "the aggregate social welfare losses associated with crime as the difference between the total expected welfare of potential victims and criminals in the scenarios no crime versus with crime". Whereas the accounting methodology "quantifies costs incurred and losses experienced that would not have occurred in the absence of crime, and then uses these data to represent direct welfare losses for citizens" (IDB, 2017, p. 2).

Two other methodologies are contingent valuation and hedonic pricing, which estimate the total cost of crime. In IDB (2017) the accounting methodology is used to compare the costs of crime for 17 countries in Latino America and Caribbean, in the period 2010-2014. IDB focusing on three types of costs: government (Public) spending; household and business expenses; and costs for victims and criminals. Figure 40 shows the causal loop diagram for the cost of crime, considering the accounting methodology, the same adopted by the IDB (2017). R1, R2, R3, R4, R5, R6 and R7 are positive feedback loops. The variables for analysis are: Cost of crime (social costs of criminality); costs of victimization, related to the decrease in the quality of life of the general population and with the income not generated by the prison population; private security expenditures, related to corporate expenditures in private security and

household expenditures in private security; public expenditures, related to expenditures on the judiciary system, expenditures on the police, and expenditures on penitentiary administration.

The cost of crime is boosted by the cost of victimization, which in turn increases as the general population's loss of quality of life increases, forming a positive feedback loop R1. The cost of crime is boosted by the cost of victimization, which in turn increases as the income not generated by the prison population increases, forming a positive feedback loop R2. The cost of crime is boosted by private expenditure on security, which in turn increases as corporate expenditure on security increases, forming a positive feedback loop R3. The cost of crime is boosted by private expenditure on security, which in turn increases as household expenditure on private security increases, forming a positive feedback loop R4. The cost of crime is boosted by public spending, which in turn increases as spending on the judicial system increases, forming a positive feedback loop R5. The cost of crime is boosted by public spending, which in turn increases as police spending increases, forming a positive feedback loop R6. The cost of crime is boosted by public spending, which in turn increases as prison expenses increase, forming a positive feedback loop R7.

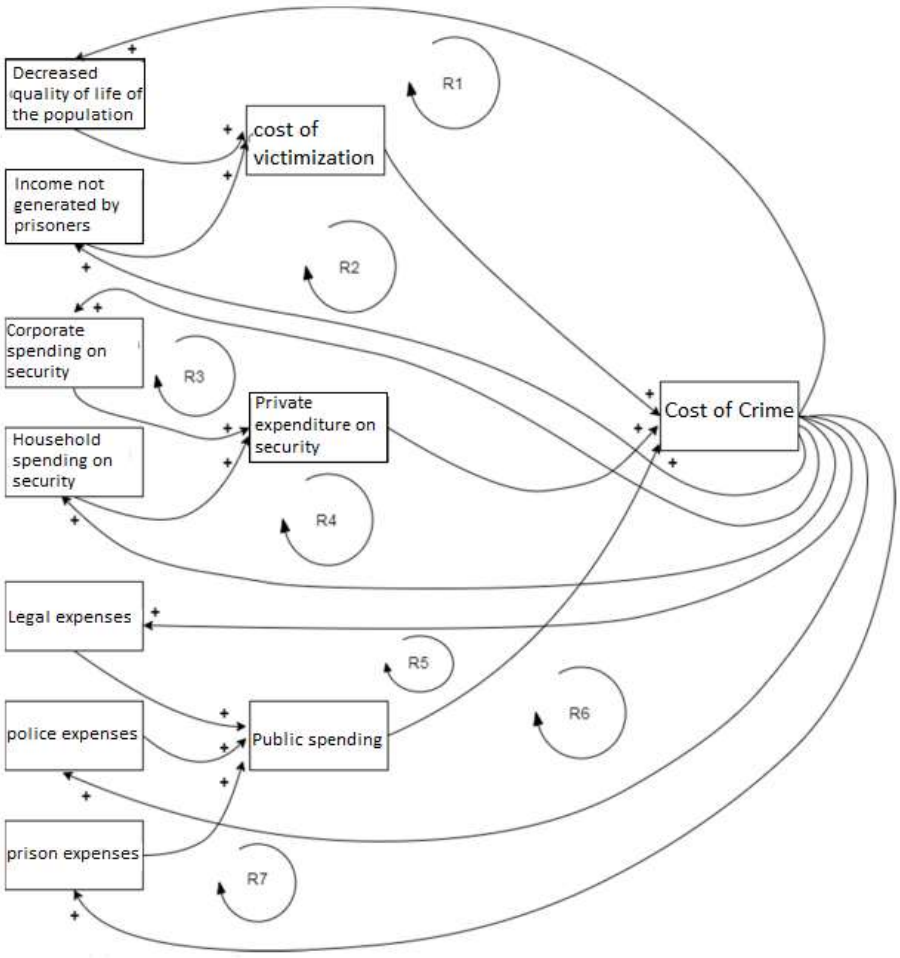


Figure 40 - Causal loop diagram of cost of crime according to the accounting methodology (Author).

Regarding costs of disaster, the ESCAP report in 2018 assumes that the total multi-hazard risk for the Asia-Pacific region would rise to US$193,525 million. Considering that the United Nations Economic Commission for Latin America and the Caribbean indicates that direct losses generally represent 30% to 40% of total losses, the total average annual loss, including indirect losses, would rise to US$270,936 million in the Asia-Pacific region, representing 1% of the region's GDP. In some countries that number is even higher, representing 15% of GDP in Vanuatu, 14% of GDP in Tonga — both part of Small Island Developing States (SIDS) —, 6% GDP in Myanmar, and 5% in the Philippines (ESCAP, 2019).

Other measures can be used, such as those related to agriculture. Some countries have a high portion of their GDP depending on agriculture, like India (17%), Pakistan (26%), Vietnam (17%), and China (9%), and disasters can directly affect that activity. Another measure could be the share of the population living in rural areas and working on low-productive agriculture; countries with those characteristics can also be more vulnerable and highly affected by disaster, like Nepal, Tajikistan, Lao People's Democratic Republic, and Afghanistan (ESCAP, 2019).

The abovementioned measures are related to economic losses. Although, in disaster cases, the life losses since 1970 in Asia and Pacific were two million people, 59% of the global death toll. In the world the average number of deaths per year was 28,730, in Asia and Pacific was 42,000. The main causes of natural disaster deaths in the world were drought and earthquakes; in Asia and Pacific, it was earthquakes, storms and floods. In Europe and the Americas, the fatalities from extreme temperature are increasing. Also, over the period from 1970 to 2018, the average number of people affected in the world annually was 38 million, while in Asia and the Pacific it was 142 million (ESCAP, 2019).

With climate changes added to the complexity of disasters, the complexity to predict disaster increases. Although it also increases the availability of technology and data from various sources as IoT, big data, remote sensing, etc., making it possible to predict disasters, helping in the preparedness, management, and disaster risk reduction, which can reduce the risk of lives losses, lives affected and economical losses in the area hit by a disaster. Also, technology can help in the post-disaster recovery. Below there is an example of how using big data can make a difference in disaster scenarios:

> In August 2006, super typhoon Saomeo hit Zhejiang province killing 483 people, displacing 1.8 million and causing losses of $2.5 billion. In contrast, in September 2018 super typhoon Mangkhut hit Guangdong Province killing just 16 people, displacing 1.5 million and causing direct losses of $2.1 billion. The substantial reductions in mortalities and economic losses were attributed to big data applications that, by 2018, had enabled impact-based forecasting and risk-informed early warning. (ESCAP, 2019, p. 108)

4.4.3 Metrics to define the best deployment from MCC narrowband to broadband

Peltola and Hämmäinen (2018) proposed a methodology based on socioeconomic value to define the best deployment alternatives for broadband PPDR networks between a dedicated network, a commercial network, or a hybrid of the two. The criteria are population density and service availability, both related to socioeconomic benefits achieved. The study focuses on the mobile access part of the solution. A causal loop analysis model is presented in Figure 41, intending to define the net socioeconomic value (NetBenefits) of the PPDR broadband network, showing: the causalities; how the services are linked with the social benefits; how the PPDR services are dependent on the mobile network services; and the applications dependent on the PPDR network. The NetBenefits is given by Equation 4.1, where p equals population density, and the threshold point is the value where the two deployment alternatives (considering the population densities) have equal NetBenefits values.

$$NetBenefits = Availability \times Socioeconomic\ Value(p) - Costs(p) \quad 4.1$$

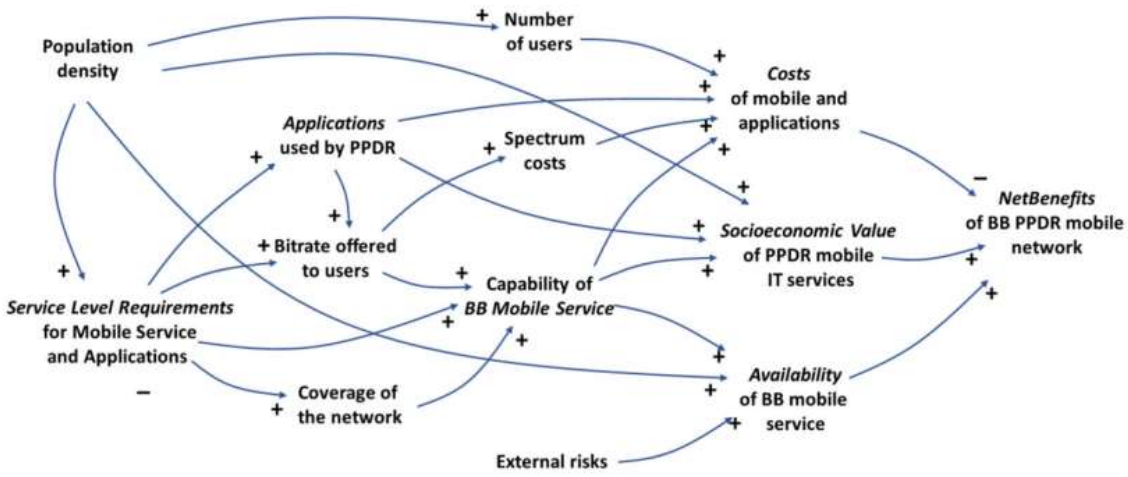


Figure 41 - Causal loop diagram of Broadband (BB) PPDR network valuation (Peltola & Hämmäinen, 2018, p. 11).

The population density is closely correlated to the use of PPDR services since it is creating value for society. Also, the network's cost is related with the population density since more users and buildings demand more BSs. The unavailability of the network service is divided in a local service interruption, wide area service break, and service break in all networks in the same area. The study made for the European Commission concluded that PPDR networks should be available at least 99.99% of the time (European Commission et al., 2014), meaning the MNO availability for PDDR coverage purposes should be evaluated to check the achievable and feasible service availability target that the MNOs. In the availability point of view, the services can be divided in fundamental, defined as services viewed by emergency organizations as their

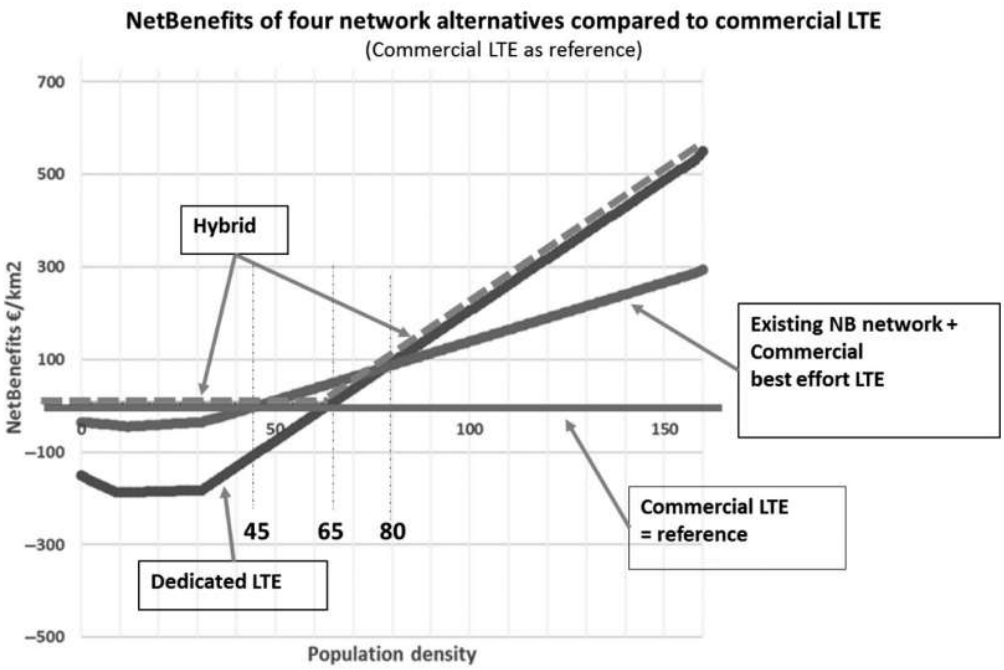
life assurance with very availability of 99.9% as PTT; crucial, defined as broadband services with high availability of 99.5% as download of maps; and beneficial, defined as broadband services with a more relaxed availability of 99% (Peltola & Hämmäinen, 2018).

The social economic value in Finland was estimated in three different ways: based on reference cases in €/citizen/year; estimation method to predict the savings due to better performance in PPDR operations when the agencies utilize broadband services; and key costs of the existing PPDR operations and estimation of cost reduction in PPDR operations through the implementation of a broadband network. In Finland, by the first method, the cost is between €41-€94/citizen/year; by the second metric, the calculation suggests that the savings would be €41/citizen/year; by the third method, the cost considers savings of 5% of all the existing costs, amounting to more than €350 million, since the annual cost is €7 billion, €65/citizen/year for a population of 5.4 million people (Peltola & Hämmäinen, 2018).

Other costs are also considered, as the annual costs of the existing services, being PPDR LMR network (~€22 million, €50 monthly per user for 37,500 users), plus monthly MNO user fee between €30-35/month/user (currently the PPDR agencies uses MNO services to complement their communication as a regular user), resulting in €85/month/user; subscriber fees of MNO services in all 5 regions; and annual investment and operating costs of an LTE dedicated networks in the 5 regions (since the regions have different characteristics, the network will be different, as the number of BSs required) (Peltola & Hämmäinen, 2018).

In the causal loop of Broadband (BB) PPDR network, the spectrum cost is mentioned. According to Ulema (2019, p. 51), in EU, an analysis made by the European economic center shows, when implementing BB PS networks, the socioeconomic benefits would reach €34 billion annually, contrasting with the opportunity cost of €3.7 billion, by selling the designated spectrum at an auction to obtain a one-off economic gain. "Naturally, the benefits are several times greater than the opportunity cost, suggesting that there should be no doubt in implementing broadband public safety networks".

The fourth technological network alternatives are: existing narrowband (NB) PPDR network + the commercial best-effort service combination; the commercial broadband network fulfilling QoS requirements; the dedicated broadband network; and the hybrid broadband network (dedicated or commercial network). The causal loop helps to compare which one created the highest socioeconomic value in the five different areas analyzed, and the result is shown in Figure 42. In the sequence, a Monte Carlo simulation is performed to compare the two most attractive alternatives, dedicated and commercial network (Peltola & Hämmäinen, 2018).



Network Type	Availability and Socioeconomic Value
Dedicated NB + best-effort commercial LTE	99.9%/253M€ + 99%/362M€
Commercial LTE network	99.5%/615M€
Dedicated LTE network	99.9%/615M€
Hybrid network	(Sparsely: 99.5%+Densely: 99.9%)/615M€

Figure 42 - PPDR network alternatives (Peltola & Hämmäinen, 2018, p. 11).

The paper reached two important conclusions about the use of the PPDR narrowband network in parallel with broadband network to improve availability in Finland: 1) "in a certain densely populated part of the country, maintaining the existing narrowband network services would, in fact, be feasible". 2) "based on the sample study, the commercial network is most preferable up to the point when the population density reaches 50-125 persons/km^2; after that point, the dedicated network is more appropriate due to the lower costs" (Peltola & Hämmäinen, 2018, p. 17). The same methodology can be used for other countries to help in the decision-making process of the digital transformation of MCC from narrowband to broadband, with a proper benchmark to compare alternatives, allowing the government to better choose and negotiate the solution.

5

RESEARCH CHARACTERIZATION, METHODOLOGIES AND METHODS

This research can be categorized as applied to its practical interest, aiming at results that can be used in the solution of real problems. It uses both quantitative and qualitative approaches with the collection of primary and secondary data. The pursuit of describing and understanding processes related to the research object characterizes the approach as qualitative, while the presentation of scenarios with numerical valuation metrics is characterized as quantitative. Therefore, it can be classified as qualitative-quantitative approach.

Secondary data were obtained through SLR and bibliographical review, while primary data were extracted from interviews and data treatment. For the primary data collection, interviews were carried out with 14 specialists from different countries, namely Argentina, Brazil, France, Netherlands, Portugal, and United Kingdom. These specialists occupy decision-making and/or technical lead positions in PPDR agencies (cited in the interview results as G and L), MCC equipment and mobile communication equipment manufacturers (cited as J and H), Smart City projects (cited as F), information security agencies (cited as I), commercial MNO (cited as N), telecommunications regulatory affairs agency (cited as O), and software development companies of public safety mobile applications (cited as B and E). In addition, there were interviews with recognized experts in MCC (cited as A and C), Smart Cities (cited as M), and data privacy legislation (cited as D).

This research's main contribution is to support PPDR agencies in finding a solution for the immediate problem of modernizing the MCC narrowband network (LMR) through 4G and 5G networks, and aggregating intelligence services in a Smart City context. This research involves technology analysis and system integration to solve problems faced in the real world, while making a scientific contribution based on the Design Science Research Method (Dresch et al., 2015). This method can be used as a form of knowledge production to achieve two purposes: generating scientific knowledge and helping PPDR organizations in the solution of

real problems. This study's scientific contributions include the models, analysis, literature review and methods developed to present the scenarios. The Technology Assessment (TA) methodology for MCC, developed by Freire (2019), was used. It considers technical aspects, economic factors, social context, costs and benefits of the solution, the context in which it will be applied, and it focuses on user requirements capture based on understanding the Activity System's context and user-related task analysis as a resource for improving MCC systems.

However, the methodology developed by Freire (2019) focuses only in MCC; its use in Smart City scenarios was part of the results, pointed out by the application of the methodology, but it was not further explored. In this research, the Smart City scenario is explored; with the need to expand the analysis horizons through multiple actors and interactions, other methods and methodologies were also used to answer the research questions.

That also meets the Design Science, which, besides being rigorous and scientifically valid, must also seek pragmatic validity, which means that the proposed solution to solve a research problem should work. Validity also seeks to determine the benefits of the solution, its effects in the environment where the solution will be applied, and the needs of those interested in the solution. This research is based on Design Science Methodology and Technology Assessment Methodology; these approaches guided the process of data collection and interpretation.

5.1 Methodology for building scenarios based on empirical data

The work developed by Freire (2019) analyzes the technologies currently used in LMR in Brazil and presents user cases in other countries elected as reference, namely Mexico, the UK, and the USA. A bibliographic review on the use of LTE for MCC was presented, and a method for Proof of Concept (POC) of LTE for MCC was proposed. It focuses on user and expert requirements, and capture based on understanding the activity system's context as a resource. The collected data were analyzed using Bunge's Systemism (Bunge, 2000), to propose a system with the logic of Composition-Environment-Structure-Mechanism (CESM).

A theoretical framework regarding resource information on Activity Theory was built to include the user's context in social, cultural and psychological aspects, as well as usability, to identify methods of data collection. Primary data were obtained from interviews and data treatment based on Mwanza's stages (Mwanza, 2001), and de Mello and das Neves's (2018) contributions. In addition, questions based on usability methods, such as Jordan's concepts (Jordan, 1998) and the System Usability Scale (SUS), were applied to 30 users and experts.

Investments in technology require prior impact analysis considering several factors. Freire (2019) aimed to support the development or improvement of MCC systems based on the results from the TA methodology. TA uses a variety of data sources to create a single information system, which aims to point out the best path of investments. The SLR disclosed several types of TA, but none were applicable to MCC systems. Therefore, it was necessary to

develop a new methodology, proposed as a series of steps to be followed — the "Six-step model" shown in Figure 43 adapted for this research, where only the first 4 steps were performed, since this research is interested in the construction of scenarios and conducting Proof of Concept (PoC) - step 5, and gathered summarized information including the PoC - step 6, are already part of applied case scenarios experimentation, which is not part of the scope of this research.

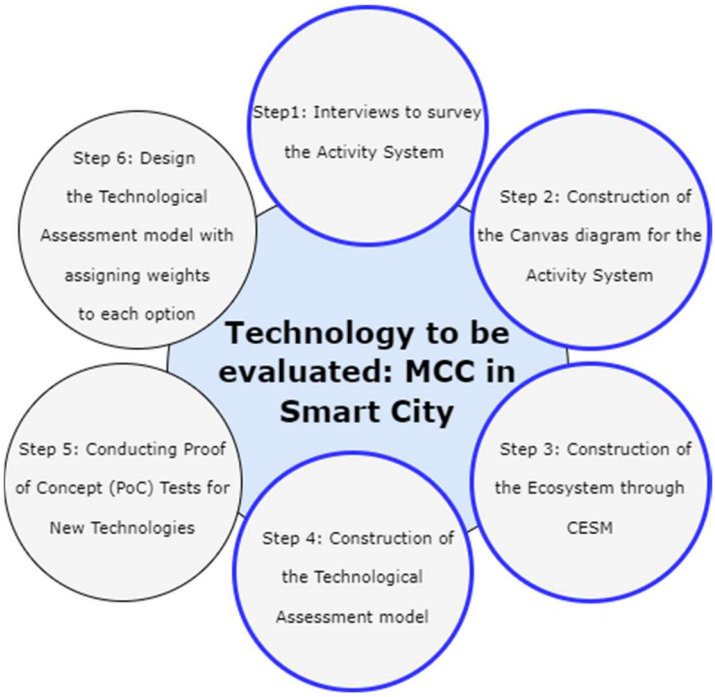


Figure 43 - Six-step model, adapted from Freire & Cândido (2019).

The construction of the Six-step model aimed to help managers in the decision-making process for choosing a technology for MCC, through the development or adoption of technology, thus providing a better service to the population with actions that have positive impacts on society — for example, reducing crime. The six steps are:

1. Having a better understanding of the Activity System — who are the subjects involved, what are the means used to carry out the activity, and what is the purpose of the activity;
2. Construction of the canvas diagram for the Activity System;
3. Construction of the Activity System innovation ecosystem;
4. Construction of the appropriate model for evaluating the Activity System;
5. Definition of PoC parameters for new technologies and, if possible, implementation of the PoC with costs and projections for the new technology, considering all information boxes, connections, and information flows.
6. Design of the TA model, which combines the summarized information gathered in the previous steps, assigning weights to how much a given technology meets

the needs of each information box, with the costs involved and the projections of return to society. The numbers presented should be normalized to facilitate comparison.

The collection data for the first step is based on Activity Theory, which constitutes a model that has the activity as its basic unit, addressing that context when analyzing human practices at their individual and social levels. This research is interested in the construction of scenarios. For that, steps 1, 2, 3 and 4 of the six-steps model were used.

5.1.1 Steps 1 and 2: Understanding the activity system and constructing the canvas

Among the methods that operationalize the application of Activity Theory for Human-Computer Interaction (HCI) contexts, Mwanza (2001) proposed a methodology that guides the process of collecting and interpreting data for requirements gathering, using the Activities System by Engeström (1987) as a heuristic model. The method enables the analysis of work practices and the understanding of the community's social and cultural context, considering mediation aspects through tools, rules, and division of labor. The operationalization process is applied in eight stages, of which the first six were used in Freire (2019). They are: activity modeling; activity system modeling; activity system decomposition; generation of research questions; conducting detailed investigation; and interpretation of findings.

Stage one refers to modeling the situation through the application of interviews with subjects of the activity, in a reserved environment, in sessions with audio recording under the participants' consent. The interview begins with an explanation of the experiment, followed by the application of previously selected questions. The questions were defined based on the guidelines by Mwanza (2001), which are shown in Figure 44 as questions 1 to 8. De Mello (2018) added a ninth question that was not in Mwanza's guidelines. Freire (2019) incorporated de Mello's (2018) suggestion to establish a bridge between the current reality and the desired situation, which is related to TA. Freire (2019) also proposed additional questions (10 to 14) to the model, intending to contemplate the difficulties in carrying out the activity and to help in the construction of scenarios. Figure 45 shows the questions applied to experts in Freire (2019), which were based on the question guidelines from Figure 44.

From the data collected in the interviews, it is possible to identify components and generate a Canvas Activity System. The conceptual view of the canvas is shown in Figure 46. The identification of subjects/actors, mediators and object is essential for the construction of the Data Collection Modular Model applied to survey scenarios. The application of the questions shown in Figure 45 enabled the construction of the LMR MCC Activity System, shown in Figure 47, based on the theoretical Canvas Activity System shown in Figure 46.

1. **Activity of interest:** What type of activity am I interested in?
2. **Object or objective of the activity:** Why does this activity occur?
3. **Subjects of the activity:** Who is involved in this activity?
4. **Activity mediation tools:** Through which means the subjects perform the activity?
5. **Activity mediation rules and regulations:** Are there cultural norms, rules or regulations that govern the performance of this activity?
6. **Activity mediation division of labor:** Who is responsible for what in carrying out this activity and how are the roles organized?
7. **Community in which the activity is conducted:** What is the environment in which this activity is carried out?
8. **Objective of the activity:** What is the desired outcome of performing this activity?
9. **Desiring movements:** If you could solve any aspect related to your activity, what would it be?
10. **Difficulties in carrying out the activity:** What are the main difficulties to realize the activity in **your country, considering the current scenario?**
11. **Opportunities for carrying out the activity:** What opportunities do you see in the advancement of technologies for the activity in your country and the possibility of partnerships with other countries?
12. **Governance for carrying out the activity:** What legal, economic and social implications do you consider relevant in this decision to implement new technologies for the activity?
13. **Transfer level and use of existing technology, identification of difficulties in implementing future technologies:** What is your opinion on the possibility of interoperability between the agencies involved in the activity, through current technologies and through new technologies?
14. **Desiring movements for governance:** In your opinion, what would be an ideal governance model for carrying out the activity in your country, considering current technologies and new technologies?

Figure 44 - Question guidelines based on Mwanza (2001), de Mello (2018) and Freire (2019).

Interview questions: 1. How would you describe CC activity? 2. What is the purpose of the CC? 3. Who is involved in the CC? 4. What are the resources or means used to carry out the CC? 5. What are the social norms, rules or regulations that influence or govern the performance of the CC? 6. What is the role of each individual in the CC and how do they organize? 7. What is the environment in which CC is performed? 8. What is the desired result when performing CC? (MWANZA, 2001). 9. If you could solve any aspect related to the activity, what would it be? (MELLO & NEVES, 2018). 10. What are the main difficulties you identify in the current Brazilian scenario for the CC? 11. What opportunities do you perceive in the advancement of technologies for CC in Brazil and the possibility of partnerships with other countries? 12. What legal, economic and social implications do you consider relevant in this decision to implement new technologies for CC? 13. What is your opinion on the possibility of interoperability between public safety agencies using current technologies and through LTE? 14. In your opinion, which would be an ideal model for CC in Brazil, considering the current technologies and new technologies?

Figure 45 - Questions applied to experts in Freire (2019).

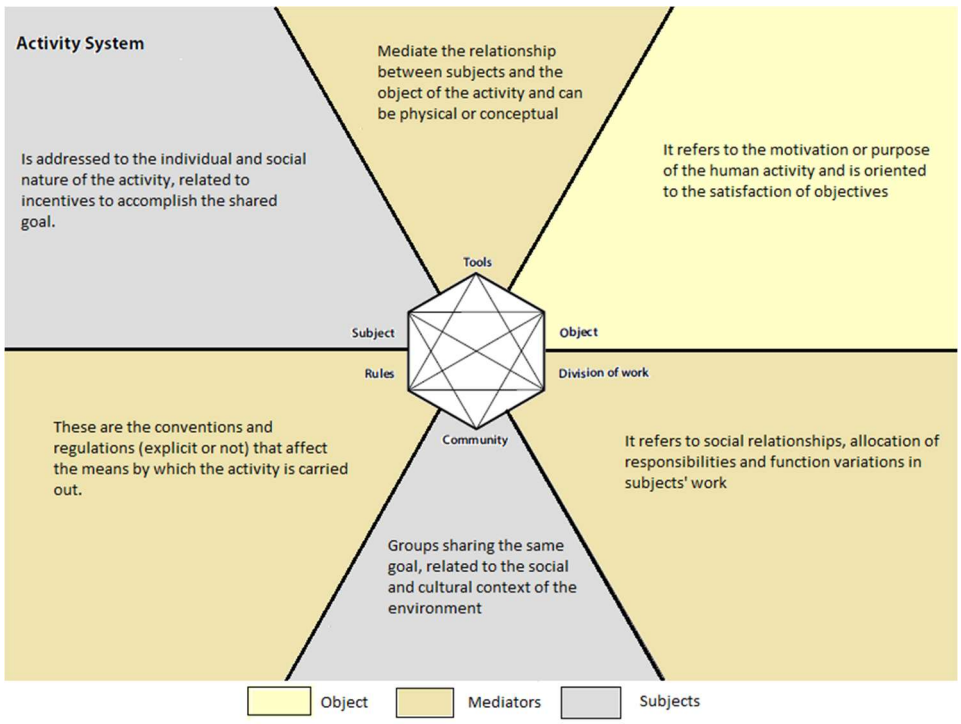


Figure 46 - Canvas Activity System, adapted from de Mello (2018) and Freire (2019).

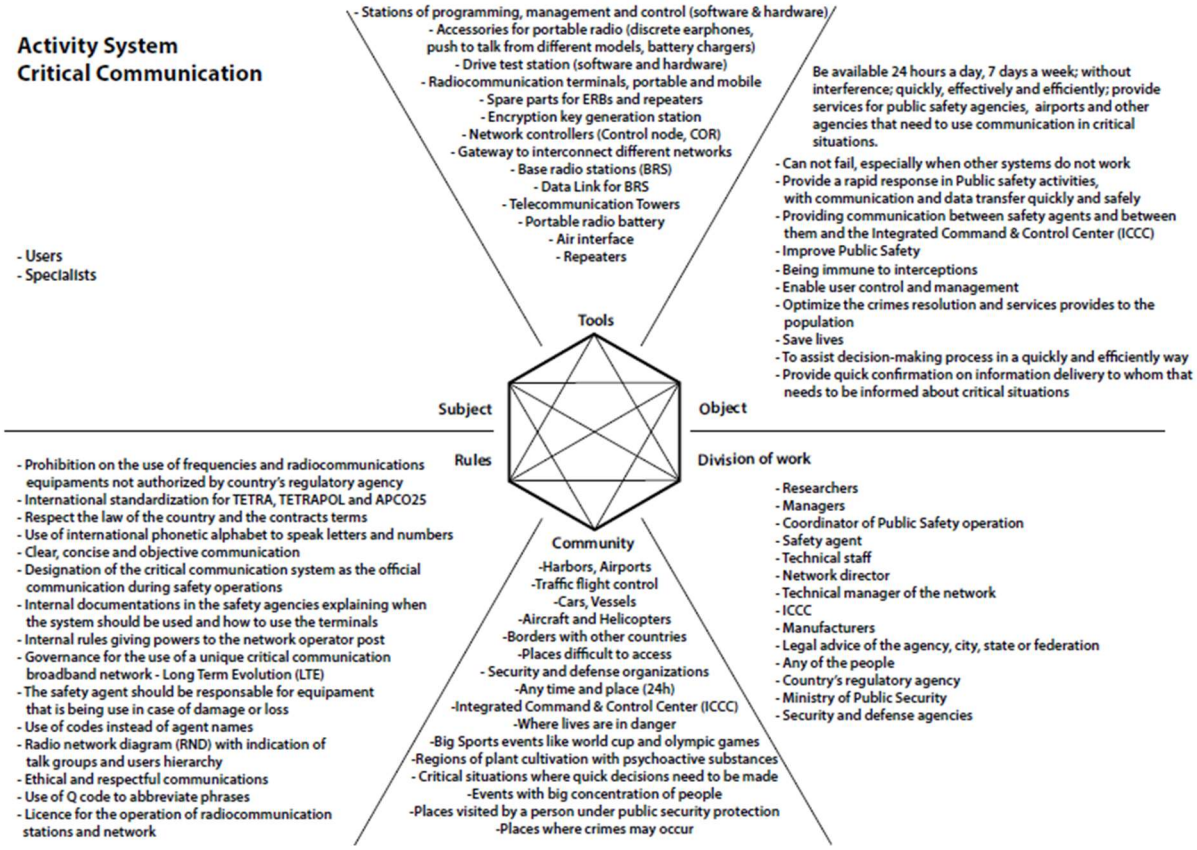


Figure 47 - LMR MCC Activity System (Freire & Cândido, 2019).

5.1.2 Step 3: Construction of the system through CESM

Considering the answers from the interviews and adapting them to Bunge's systemism (Bunge, 1980; 1985; 2000; 2003; 2005), combined with Activity Theory in the context of HCI, it was possible to map the elements and the relationship between them to build the ecosystem. Bunge's systemism is a reduction that describes a system by its Composition, Environment, Structure, and Mechanism (CESM). In Freire (2019), Bunge's systemism concept was used to construct the ecosystem from the Canvas Activity System, placing it in a broader context, dividing it into Composition, Environment and Structure, distinguishing system levels, and displaying the relationships between elements through Structures and Mechanisms.

In the model, the Composition is atomic — that is, each component is an atom of the system. The system's components will be the Subjects and Tools from the canvas; each Subject must be represented, and the Tools can be represented by a single element. The Environment are external items that act or suffer the action from some component; the Environment component will be the Division of Work items from the canvas. The Structure is the connections between components, and between them and the environment; they are represented by the lines that connect the boxes. Mechanisms, on the other hand, are the processes that act on

transformations, which can cause the system's growth or collapse (or some property of the system). The Structure is the link, and the Mechanism is the process related to this link.

The Mechanisms can be found in the fields Rules and Division of Work from the canvas. In this research it is proposed that the mechanism can also be represented by the possible metrics to evaluate the relationship between the elements and must be represented in the ecosystem to facilitate the visualization. In addition, the fields Object, Tools and Community subsidize a broader understanding of the Activity System, assisting in the identification and construction of the CESM. If the system is not working properly, all four possible fonts (C, E, S and M) should be examined and there should be an attempt to repair the system by changing some or all of them. The conceptual model for the ecosystem is shown in Figure 48. Figure 49 shows the LMR MCC ecosystem.

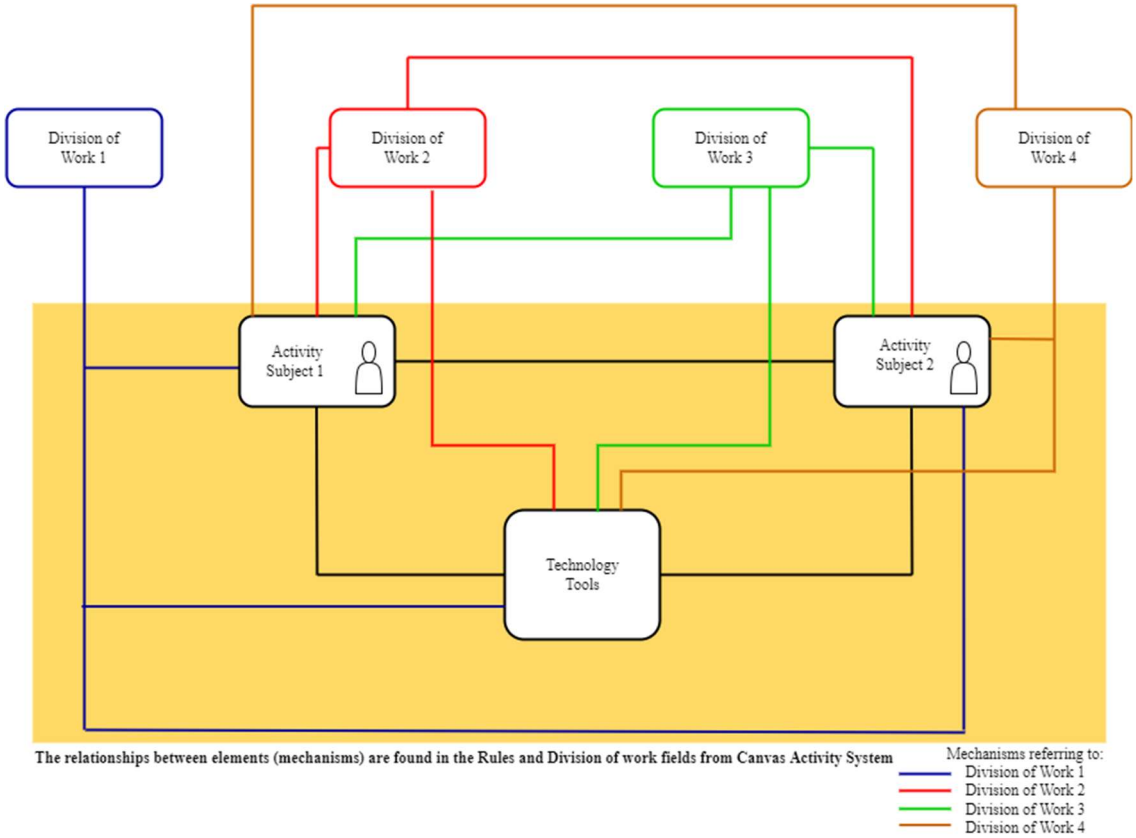


Figure 48 - Ecosystem from the Canvas Activity System, adapted from Freire (2019).

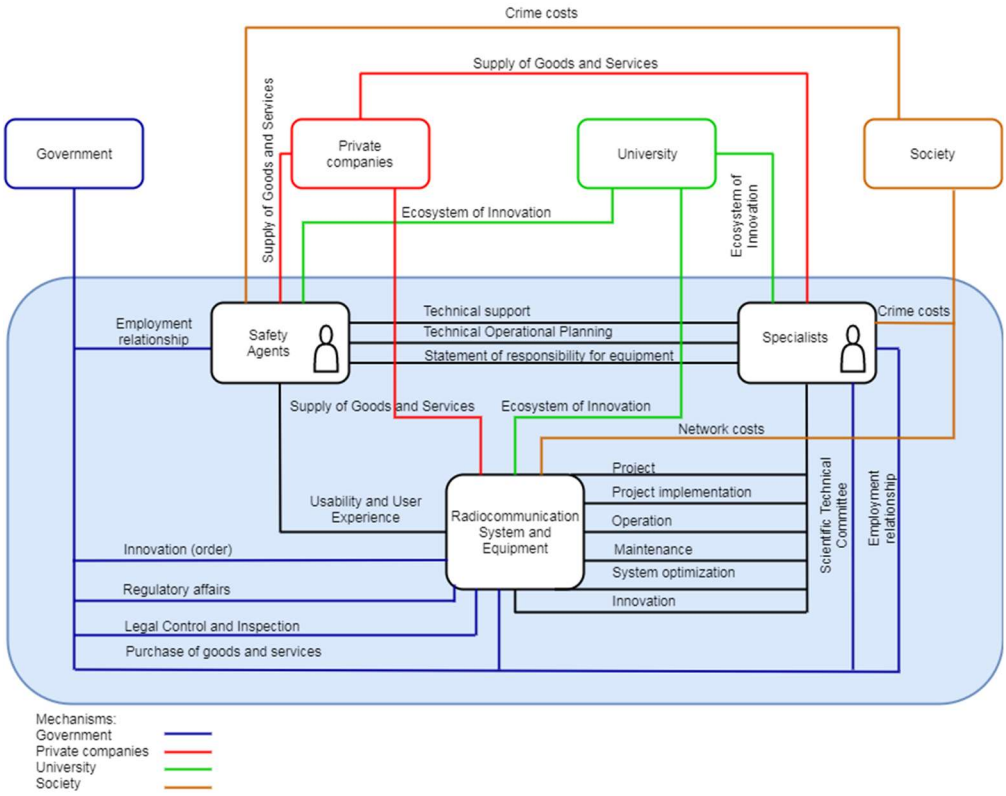


Figure 49 - LMR MCC Ecosystem (Freire & Cândido, 2019).

5.1.3 Step 4: Construction of the Technology Assessment model

In the model, the elements of the CESM system will be the dimensions of the TA model, which may include some or all of them. The links between the elements are the Mechanism, in this research is proposed that the mechanism must be represented by the field of studies, the relationship between the elements and the metrics, some or all of them should be analyzed in the informational flow, according to each applied case. The relationship between the field Tools and the system is the box represented by Technology in Figure 50; it must appear among the analyzed dimensions because it is the means through which the Activity System works. Due to its importance to the system, its output in the informational flow is from a macro view, considering the scenario's survey, considering the main technology tools and the activity purpose. In the Activity Theory, the human element is the main element. With that in consideration, dimensions representing the activity Subjects must exist. Figure 50 shows the conceptual representation of the TA model, and Figure 51 shows the LMR MCC TA model.

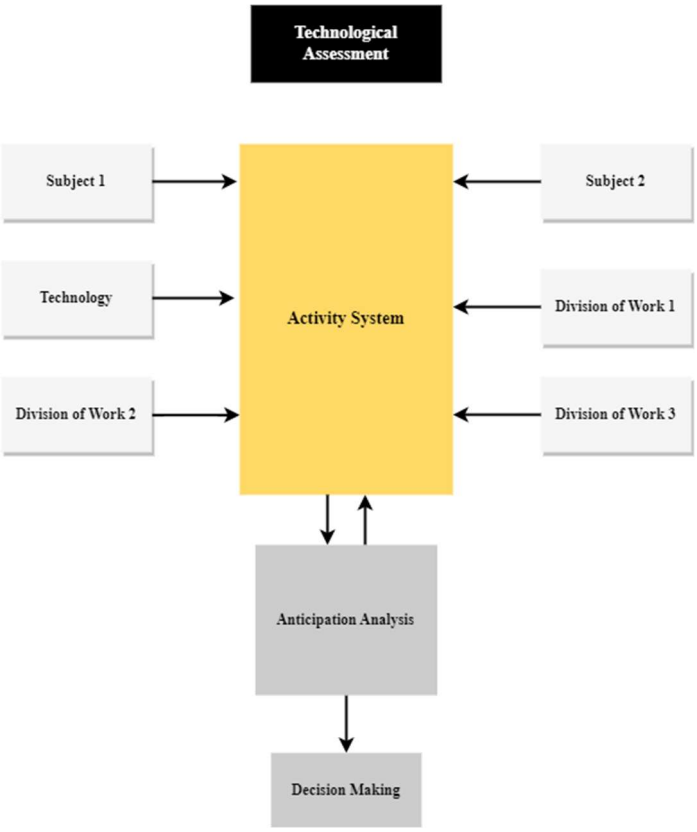


Figure 50 - Technology Assessment conceptual model, adapted from Freire (2019).

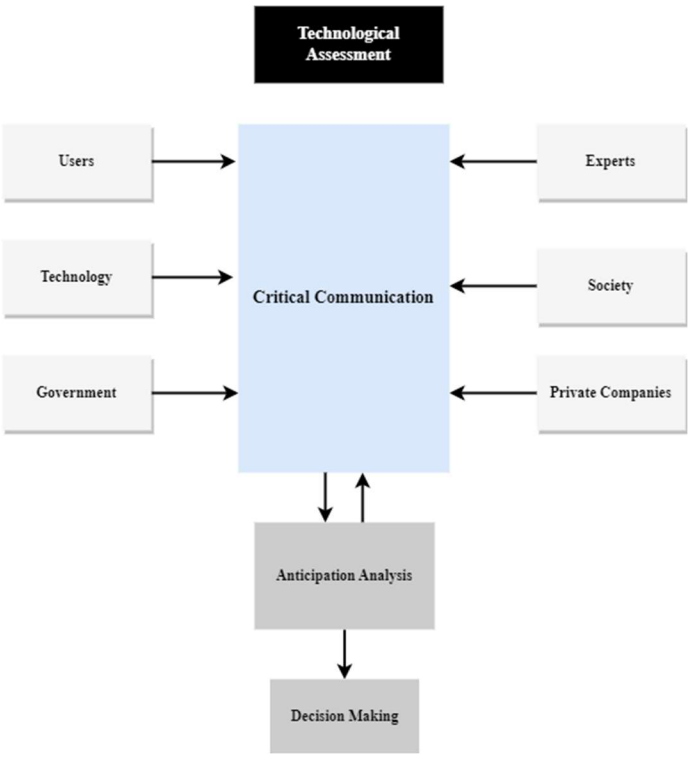


Figure 51 - LMR MCC Technology Assessment model, adapted from Freire & Cândido (2019).

5.1.3.1 Dimensions

The Society dimension is presented in the LMR MCC ecosystem (Figure 49), linked with the system by the network costs and cost of crime. The cost of crime intends to evaluate the impacts on society as an indirect measure; it was presented as a suggestion to the perception of technology impacts on society. In Freire (2019), the society was not a Subject of the TA for MCC in the MCC Ecosystem; the connection between the activity subjects and technology tools was through cost of crimes and network costs. The reason for that construction is that, in an LMR system, technology behaves as a closed system, where the information and communication are confined to the PPDR agencies and the CCC or Dispatch Center.

One of goals in this research is to apply a Constructive Technology Assessment (CTA) approach, where the society is also a subject of the Activity System. This new approach is possible due to technological developments on the ICT, which now allows an individual to feed the system through social computing or providing relevant information in a platform, as the one suggested by Shih et al. (2019). In that sense, society should be consulted about the scenarios presented as results, and it should be questioned on how to contribute to the Smart City Public Safety Emergency Management system. With that approach, the society could have two analyses: one as Subject of the activity, acting inside the system, and the other as presented in the LMR MCC Ecosystem (Figure 49), acting outside the system and indirectly measured by the social impacts, using cost of crime methodology and network costs.

The LMR MCC TA model (Figure 51) presents six dimensions, namely Users, Technology, Government, Experts, Society, and Private Companies. From that, the dimension used for the construction of the Data Collection Modular Model is the technology dimension. As this research is concerned with the construction of scenarios using the CTA approach, Society was also analyzed as a Subject of the activity through citizens being included as a subject of the activity, as demonstrated in the next chapter and in Figure 55, the MCC in Smart City TA model. For more detailed inputs from the society's point of view, it would be necessary to apply participatory methodologies, which are not in the scope of this research.

6

CONSTRUCTION OF SCENARIOS BASED ON EMPIRICAL DATA

The first stage was constructing the questions considering the guidelines detailed in section 5.1.1, adapted to the research objectives, then applying the interviews. The questions applied are:

1. How would you describe Mission Critical Communication (MCC) considering Smart City environment?
2. Why MCC should consider Smart City environment?
3. Who should be involved in MCC in Smart Cities?
4. Through which means the Emergency First Responders (EFRs) perform / should perform the MCC in Smart Cities?
5. Which are/could be main social norms, rules, or regulations that influence or govern the performance of the MCC in Smart Cities?
6. What are/should be the role of each agency in the MCC in Smart City environment and how do they organize?
7. What is the desired result when performing MCC in Smart City environment?
8. What were/are the main difficulties that you identify for the MCC in Smart City environment to happen?
9. If you could solve any aspect related to the activity (MCC in Smart City environment), what would it be?
10. Which considerations (legal, economic, and social) do you consider relevant in the decision to implement new Information and Communication Technologies (ICT) for MCC considering Smart City environment?
11. Do you think there could be any negative implications? How to avoid that?
12. In your opinion, what would be an ideal governance model for carrying out the MCC in Smart City environment? (if the question 6 were answered considering a

future and desired scenario, not an applied one, that question should not be applied since the answer will be redundant).

6.1 Interview results

The questions applied helped the construction of the Broadband MCC Activity System considering a Smart City environment, and the construction of the ecosystem for that — both presented in the following sections. The answers helped filling some gaps that were identified in the beginning of this research and represented in Figure 20, as detailed below.

6.1.1 MCC considering Smart City environment

According to the interview answers, most PPDR agencies nowadays have their own networks, where MCC is carried out through fragmented networks (agencies with different LMR solutions), using trunking-based technologies developed 20 years ago for a few vendors, and lacking integration protocols between different interfaces to enable diversification of suppliers; these are expensive solutions to build and maintain. The EFRs also make use of commercial broadband networks without dedicated resources to access data in a non-mission-critical manner. Public commercial networks, on the other hand, have evolved over the last 20 years, through the development of a standardized, interoperable technology with network open topologies and standardized interfaces, which allows equipment from different manufacturers in the same network. Through 3GPP, the various interfaces are being increasingly standardized, allowing a greater number of vendors and enabling a variety of new services, such as using a public network at the service of mission-critical instead of a closed network (N).

In a Smart City environment, PPDR agencies, citizens and other actors are feeding the system to have integrated action intending to achieve better results. This affects not only Public Safety events, but also other areas, such as energy, public transport, and healthcare, by providing better coordination for different players based on a variety of data with information management (E, M, O). There is an intense exchange of data between two different systems, MCC on one hand and Smart City on the other. The technology connects those two sides through a center (CCC) where data are received from various actors — not just PPDR agencies — treated and forwarded to intelligent action by agencies and EFRs (O). That technology must be planned with citizens and for citizens. In that sense, the technology is applied to cities and agencies to improve people's lives (M), being a tool to achieve goals, not the goal itself (M). In that new scenario, the systems are integrated making use of broadband networks, a variety of data and artificial intelligence to help in the decision-making process for city efficiency, aiming to benefit the citizens (J, O), and the communication aimed at the digital society, being always available, safe and resilient (G).

The MCC, in that sense, could be also consider as the LMR evolution, intending to access and process a variety of data sources due to the possibility of system integration, high process capability, and availability of broadband resources, in an open ecosystem with more stakeholders than the legacy system (L, N). That new view involves more actors and more input data — therefore, more risks (I). It is a real-time communication linked with urban events using IoT, Big Data, Machine Learning, and GIS, integrated with various agencies and local authorities, with the aim of anticipating crisis events and acting during and after those events: a data-based performance aiming to provide a better service for the citizens of a Smart City (F).

According to all the interviews, there is a clear need for interoperability between MCC and Smart Cities. Nevertheless, the collaboration between different regions, PPDR agencies and stakeholders to share intelligent resources (e.g. videos from drones to help the fire brigades, and real-time information to provide situation awareness) will only happen if there is a proper coordination to integrate the resources, with long-term plans to develop a nationwide strategy for the broadband network and the system integration between the different stakeholders, in compliance with local legislation on data policy, data treatment, and privacy.

6.1.2 Why MCC should consider Smart City Environment

MCC is about applications used by mission-critical organizations. Meanwhile, with LMR systems, the applications for voice and narrowband are limited. Nevertheless, data applications became more relevant to provide more effectiveness in an emergency scenario, such as knowing if there is a chemical risk in a fire, based on the database of dangerous goods from the fire brigade. With that in place, more effective plans can be developed, based on big data information and on data sharing between agencies, cities and private companies, respecting data protection and privacy, with the final goal of strengthening democracy (A).

Smart cities have a data generation structure for the CCC through several segments that predict or indicate more quickly phenomena that are relevant to the actors involved in the MCC. For example, a traffic sensor coupled to public transport can show there is an excessive delay on the route, which may indicate a problem on the road; this information can help the action of PPDR agencies. Smart cities could be a data input capable of improving the work of PPDR agencies. Better data improves the decision-making process, not just during events, but also in preventing or mitigating them (O).

MCC should consider Smart City environment because of the need for coordination of different city services, such as ambulance, police and firefighters. Those agencies have cultural and technological issues to overcome, so if one network that could be better integrated and interconnected is available, the city can have better services, providing more adequate solutions to the people living in a city which has PPDR situations solved and prevented in a smart way, with data providing more effective actions before, during and after the events (B).

MCC should consider Smart City environment to have integration with other technologies and systems, changing the current process, which is centralized and isolated, depending on the dispatch center to feed the EFRs with information. Meanwhile, the dispatch center has no intelligent resources to act more effectively. Nowadays the EFRs are completely dependent on the dispatch center, which is not integrated with intelligent resources, being limited to sending information to the EFRs by voice and short messages. It is not possible, for example, for the fire brigade to have access to the building plant in their device; or for the artificial intelligence acting in a building on fire to shut down the energy before the fire brigade arrives; or to verify if the hydrant on the street has water; or to have sensors reading if there is a chemical risk in that building (C).

MCC must consider a large volume of data with intelligent processing to support the decision-making process, through intensive data collection, without violating the citizens' fundamental rights (necessity versus proportionality) (D, I).

MCC should consider Smart City environment to serve the information society with responsiveness, availability, security and resilience, making use of the new technological tools such as IoT, artificial intelligence, machine learning, and big data, with responsive and predictive action based on data (F, G, M). It should also assist in urban planning, especially in areas of greater vulnerability, always aiming to benefit the citizens to achieve the Sustainable Development Goals stipulated by the United Nations, by increasing the city's resilience and improving the citizens' quality of life (F, G). It makes no sense to say that a city is "smart" if there is no integrated communication between the various actors, allowing a quick response to emergencies that affect the resilience of the city (M).

It is a technological evolution to follow the needs of the information society intending to have access to a large volume of data and having more records and control of police action, such as, recording the action of a police officer through a bodycam (L). MCC needs this evolution to offer better mission-critical services, and it makes no sense not using commercial public networks already available in large scale in many countries. The public network must be used to offer mission-critical service, and there is a variety of forms of use that can be adjusted for each applied case, i.e., public networks offering services for different critical applications, which can be complemented by the PPDR agencies having PPDR core (PLMN) with allowed roaming for different MNOs according to coverage, and/or complementary RAN, or using a private network as a service, and so on. It is neither efficient nor economical to have several non-integrated critical networks providing parts of mission-critical services with a high cost of installation and maintenance. This also applies to countries with large territorial areas, like Brazil, that want to build their own broadband networks for MCC without using resources from existing commercial public networks — highlighting that most PPDR agencies lack technical, financial and human resources to construct and maintain an MCC network (N).

6.1.3 Main difficulties

1. Cultural issues: PPDR organizations are quite conservative and may not use new technologies and new processes if the decision is made by machines via artificial intelligence (A). The EFRs are resistant to change the technology because their lives depend on that, and new technologies take time to be trustful — although the EFRs from the new generation are less resistant to change because they are not used to terminals without connectivity (B). Public Safety agencies have their organization so embedded with certain tools used in LMR networks (based on narrowband and isolated systems) that they are not even capable of describing the tool, which has become part of the organization, as the communication split between groups (E). PDDR agencies are resistant to working in an integrated way, sharing information and working in the same technological system, preferring to operate in the systems that EFRs are already used to (M, N).
2. Lack of governance: lack of governance between centralized and decentralized organizations to decide when the new technologies will take place and to create a joint work force between the agencies to work together in that new model (A, N). Lack of Smart City initiatives to integrate both areas (MCC and Smart Cities) (C). Lack of long-term public policies, without political interference, transversal to governments, committed to the cities and their citizens, not with the politicians (F, G). Lack of centralized governance to promote digitalization considering broad aspects, such as health, education, etc. From the cities' point of view, there is a lack of platforms to share building block models on how to build the Smart City, such as models on how to contract services for the various segments; how to contract mission-critical applications; how to carry out the purchase, installation and service provided, for example, to place traffic sensors on buses, as well as analytic data for these inputs; service providers already accredited and registered on the platform, etc. The centralized governance for digitalization would help in the construction of that platform and the building blocks for Smart Cities, providing guidance to the cities and speeding up the digitalization (N). Lack of a nationwide plan to develop the MCC broadband network (L, N).
3. Costs: lack of financial budget for the MCC broadband infrastructure (A, E, M).
4. Time constraints: the timeline for building a private MCC broadband infrastructure is too long (A).
5. Management: difficulties on how to organize such a complex project in an organization that is not familiarized with that type of project, highlighting the need for a third-party agency, as the FirstNet Authority in EUA (A). Lack of long-term vision and leadership to coordinate the project (C). Lack of an orchestrated

management for the construction of the new infrastructure with all agencies involved (D, J). Lack of a neutral authority to orchestrate the resources and implement the new solution (F, L).

6. Risk Assessment: risks that were not overseen may take more time and money to develop the new MCC broadband network than the initial plan, because of the lack of a proper dimension (the risks should be well evaluated before the project takes place) (A). In most PPDR agencies, there is a lack of people with proper knowledge to realize the previous studies, such as risk analysis (C).
7. Technical difficulties: in places where the LMR network already exists, there is a difficulty to integrate the LMR network with the 3GPP network, since the integration is not standardized from the LMR side, depending on the vendor (E, H, N). Despite the 3GPP having standardized the direct mode for 4G and 5G networks, this has not yet been fully implemented for 4G (E, H, L), because no chipset vendor has developed direct mode for LTE using 3GPP standardization (H). Meanwhile, for 5G that will work, due to the combination of Wi-Fi mesh, Direct Mode, and Push-to-Talk over 5G (E). There is also the sidelink initiative[22] addressing this topic, but until the moment it is not known if that will work well, because it is driven by V2X communication (D2D communication for vehicles) (H). Also, the 4G/5G UEs don't have the high power in uplink as the LMR radios, making use of higher frequencies — meaning they will not reach the same coverage for direct mode operation (H, L). If a new technology is introduced in Smart Cities, that technology needs to be at least as good as the old ones (E, H). Meanwhile, the new solutions are quite expensive, and they are still not able to deliver the same benefits of the legacy solutions (E).
8. Distrust: in Latin America, there is a general mistrust from citizens in the public institutions, which implies that they may not be comfortable sharing information to collaborate with a social computing tool (G). PS agencies don't trust each other, which makes the integration of communication and information difficult (G). The fear of cybersecurity threats is bigger when compared with what in fact exists (since there are technological solutions to mitigate that risk) (E).
9. Spectrum: broadband applications require broadband spectrum, and some countries have not designated spectrum for PPDR purposes (H). Other countries have designated spectrum, but the bandwidth is not sufficient to provide a good service (L).

[22] Sidelink is a 3GPP standardized technology that enables direct user-to-user communications, and "defines mission-critical services such as push-to-talk voice and video and prioritized access of different services over the same communications channel" (Barnes & Maheu, 2023).

10. Lack of examples: there is a lack of examples of concrete and successful experiences (A, B, O).
11. Lack of qualified personnel: there is a lack of trained managers to conduct the governance process for digitalization, and a lack of personnel with knowledge within the agencies to lead the processes (A, C, N).

6.1.4 Priority aspects to be solved to make MCC in Smart City environment possible

1. Down-top change based on User Experience (UX) solutions: EFRs working better together, using customized tools with processes for information and communication sharing. Getting them used to these tools will make EFRs themselves wanting to change the processes and the technologies involved (A). Give voice to the EFRs to develop tools, processes, and technologies to address their needs. If the EFRs from all agencies work together, that will force the top managers to change the technology (A). Design the new system by mapping the EFRs' necessities (C). User designed applications available in an app store for PPDR purposes, e.g., the FirstNet store, which has more than 200 applications tailored to PPDR agencies' and EFRs' needs (broadband networks allow the development of 3GPP compliance customized solutions, which is a big advantage compared to the LMR systems that are closed systems vendor's dependent) (H).
2. Training: if the PPDR agencies don't have people trained on the use of the new tools, they will not know what to do. Even if they have the most advanced tool available, it will be useless and the EFRs will show resistance to using it (B).
3. Pilot or Key event: put in place a real case use with the MCC working in a Smart City environment and follow the indicators before and after the technology application, showing the benefits in a real-world application (B, O). A key event with high visibility, such as the Olympic games, should be the milestone to the new network (H).
4. Governance: need of a municipal master plan for Smart City, approved by law, with a management control to monitor the development and delivery of the solution (C, J). The project should follow the triple helix of innovation[23] through the university-industry-government interactions, being a knowledge-based solution, allowing economic growth and social development to the society (C). The commitment with a long-term well-organized plan to deploy the solution.

[23] Recognized model of innovation studies based on university-industry-government interactions to develop and/or apply innovative solutions in local, regional, national and multinational levels (Etzkowitz & Zhou, 2017).

Currently the agencies conduct a PoC with the latest technological solution, but they don't follow a plan. Later they have another PoC with another latest technological solution, and so on, without a long-term plan for using the technology already deployed, like 4G, or for other technologies, like 5G, and without a broader view to include financial budget for 3 to 5 years ahead, regardless of political timeframes (E). Long-term public policies, transversal and independent from governments (not attached to political timeframes) (F, G). Agency that promotes centralized governance for digitalization, considering broad aspects such as health, education, etc. That agency would help in the construction of a platform to help the cities to became smart, with building blocks of models on how to build up the Smart City, such as models on how to contract services for the various segments, how to contract mission-critical applications, service providers already accredited and registered on the platform, etc., providing guidance to the cities and speeding up the digitalization (N).

5. Integration: make all PPDR agencies interact and design a solution involving all stakeholders (D, J, F, G, M).
6. Top-Down changings: change the PPDR working processes and the management process of the CCC to be based on situation awareness resources. Acting this way, the EFRs will be forced to change their devices (H). Change the way PPDR agencies work, from voice centric to data centric, in a standardized way (H).
7. Frequency spectrum: the designated frequency spectrum bandwidth should be sufficient to develop the new MCC broadband network (H, L).
8. Regulation affairs: proper legislation addressed to the MCC broadband network, such as priority and preemption in regular MNO networks (A, B, C, E, H, J).

6.1.5 Possible negative consequences in the use of MCC in Smart City environment

9. Bad use of information by EFRs and agencies: EFRs using the information in a negative way, since they can gather more information, not respecting privacy and data treatment policies (A, J, L, G, O), which can lead to the population losing confidence regarding the use of the new system (O). Violation of the citizens' fundamental rights (D). How to prevent: all should be aware of the limits of use of information, as well as the consequences of a bad behavior (not respecting data and privacy regulations) (A, R). Private information should not feed the system, meaning the system should be prepared to identify when it is a private information and discard that (A, O). Having protocols and control devices to

monitor the destination and use of information (J, L, C, O), considering the proportionality versus necessity of the use of the information (C).

10. Poor quality of the data feeding the system: people not collaborating with the system via social computing / social sensing due to lack of confidence in public institutions (G, L, M), or due to lack of technological knowledge, imagining dystopic scenarios as the ones presented in science fiction movies like "Minority Report". Meanwhile, the emergency situations will continue to happen and the PPDR agencies will not be able to act effectively due to the lack of proper information (B, N). How to prevent: educating the population about the technology and the use of the information (L, B, M, N). Having control devices to monitor the destination and use of information, so people can be confident to share information (J, L).
11. Collective fear: people feeling insecure due to misinformation and unfamiliarity with technology (N). How to prevent: educating the population about the technology and the use of the information (L, B, M, N).
12. Wrong decisions made by the machines: when new technologies are implemented, that can generate false alarms. This has happened in Buenos Ayres, Argentina, where the face recognition in cameras along the city integrated to the police database generated false alarms, which could result in the detention of a wrong person (B). How to prevent: using mature technologies and well-trained AI (B). Constantly monitoring the technology results, since distorted information from sensors can lead to wrong conclusions about a group of people (F).
13. Social control: if not well regulated and delimited, information can be used to control citizens rather than benefit them (C, M). How to prevent: data protection legislation (M).
14. Security risks: leakage of private information, hacker attacks, and increasing risks that previously did not exist because they were isolated systems (C, E, M). Cyber-attacks all over the place, with disruption to the services, such as a shutting down the power grid of the city (E, M, O). The efficiency gain in the EFRs' performance does not compensate for the increase in security risks by changing a closed and secure network for an open network and with more risk (I). Mix of private and public communications such as a personal WhatsApp running on the EFR smartphone and at some point, the agent mixing up the information, sharing sensitive data in private groups. That could also allow the public to discover the EFRs' phone number, which should be confidential (C, H). If the devices are open to the internet, then they have an open door to cyber-attacks. How to avoid: the system should have protection against cyber-attacks (C, M). The UEs should have

protection to avoid mixing up information between the different domains (private and public). Creating different profiles in the same UE could be a solution (C).

15. Becoming vendor dependent: creating something that is vendor dependent, which could be the mobile network, infrastructure, backhaul or other crucial part of the system, which is not easy to anticipate (E). Dependency on network equipment, chips, microchips, power grid, and so on (E). How to prevent: creating a MCC infrastructure that should not be tied to one vendor, being a proof of future solution (E). That vulnerability could be avoided using different technologies from different vendors (E).
16. Being vulnerable: when creating a MCC infrastructure, that should be resilient to everything and always available (E, M). The risk of being vulnerable could be avoided by proper regulation about the protection of critical infrastructure (E).
17. Becoming a technology that leverages bias: false targets due to the bias embedded in the technology (B). The technology can enhance bias, increasing discrimination against people who already suffer some type of discrimination in society (F). How to prevent: using mature technology, such as well-trained and well tested Artificial Intelligence (AI) (B). Constantly monitoring the technology results, since distorted information from sensors can lead to wrong conclusions about a group of people, collaborating to exclude even more people that already suffer some type of discrimination (F). It is possible to monitor if the technology application affected the society on a positive way by using metrics (KPIs). The measurements should be made before and after using the technology — preferably the ones recommended by international and recognized institutions, e.g., ISO and UN's Sustainable Development Goals, related to the citizens' quality of life and the city's resilience (F). Also, measurement of reduction in crime rates, reduction in the number of arrests, reduction of lethality in police actions (L).
18. Bad management: disruption of services, such as shutting down the city's power grid, due to bad management of the Smart City, e.g., a maintenance in the main server's air conditioning system without a backup planning or a lack of energy backup. A failure in one server can stop the entire city. How to avoid: the Smart City must be a city heritage, not a legacy from governments and politicians (F). Preparing and training managers (N). Smart City management is not to be linked to political management, having an authority responsible for the system orchestration in the CCC (F).

6.1.6 Aspects to consider in the decision-making process of changing the LMR technology for broadband networks in Smart City scenarios

1. Social Costs: the governments must show to the society the balance between the cost values of investing in technology, versus the prevention costs in society. When this comparison is made, it is possible to see that the investments are not so big when compared with the damage that the system will be able to avoid (B, C, N). However, the evaluation of the social cost gain must be made according to each applied case, comparing the problems that a city faces and the possible gain when the solution is applied. Another city will likely have other issues that need to be addressed, i.e., in this city the measurement of the social costs must be different (C). Make an analysis of how the solution will affect the city and the citizens, cost of technology versus returns on society related to improvements in people´s quality of life (N).
2. Objective Evaluation: a benchmark study case must be done at local, national and international level, to compare the existing and future solutions, intending to do a criterions evaluation by surveying possible scenarios, without neglecting the technological path already taken by the agencies and the cities (L, F, G). A Technology Assessment should be carried out with a clear definition of the target KPIs to be achieved, such as, improvement in public health, education, environment, Gross Domestic Product (GDP), crime reduction, and so on (C, F, G, O, N). It is necessary to assess whether the legacy LMR solution already meets the needs of a given location, not all regions need more complex solutions to address existing problems, sometimes process changes are more efficient than changing technologies, not being necessary to switch from a limited, but closed and secure system, to an open system with more resources but also with more threats such as cyber-attacks (I).
3. Governance: through a centralized authority, do a decision with transparency, with previous evaluation and proper dimension of the financial budget, such as the FirstNet Authority (C). The cost of the solutions should be well dimensioned (D, F, G, J), adapting the available financial budget to the technological solutions (G). What exists a lot are adventurous companies that present miraculous solutions to managers without knowledge, resulting in bad decisions in very expensive purchases that do not solve the problems that should be solved. There is no Smart City with managers without proper knowledge (F, G). In the smart city, system governance must involve all agencies and stakeholders (M, O).
4. Prototype development: the design of the solution should be based on eliciting user requirements of all stakeholders involved, including the Smart City´s actors

(C), also, evaluating what the legacy technology already delivers, in terms of user requirements, and the gap that the new technologies should bridge (C, D, F). If there is no solution available in the market that address the problem, a development plan strategy should take place, with clear goals to reach, according to the problem to be solved (D). Understanding the problem that should be solved, for example, the biggest problem of a city "A" could be high number of criminalities and a city "B" could be traffic congestion everywhere, the solutions should be proper addressed according to each applied case (D, F, G, O). The manufacturers and companies that sell technology solutions should first listen to the problems that cities and agencies have, then propose technological solutions to the problems that already exist, and not present solutions for problems that managers don't even know if they exist or not (G). The solution should be user friendly (H). The solution must be thought from the beginning as a critical solution, build with geo redundant core with virtualized infrastructure to the datacenter where everything is spread geographically to increase the resilience of the network. The base station´s location should be reinforced, making sure that the base station will not be stollen, damaged, or vandalized. The backhaul should be resilient with self-healing and self-configured functions. The network should have power resilience to the equipment with power generators and battery banks with many hours of autonomy (H).

5. Frequency Spectrum: evaluation if in the country already exist designated spectrum for the MCC broadband networks with enough bandwidth (H).
6. Risk Assessment: concerns with cyber-security, availability and resilience of the solution (H, I, M). The MCC should be in any point isolated from the EFR private communications (C, H, I).
7. Necessity versus proportionality: it should be evaluated whether the new system can protect citizens' personal data. The use of information to deliver public services must be legal and proportional, just used to achieve a defined goal and not impacting on citizens´ rights and individual freedoms (A, C, D, I, J, M).
8. Holistic view: Construct systems to integrate with the Smart Cities, helping the cities to achieve the ISO indicators 37120 (referring to quality of life and sustainability), 37122 (efficiency of municipal services and quality of life that the city offers to citizens), 37123 (referring to prevention and action in the face of natural disasters and the city’s economy, that is, the city’s resilience) (M).
9. Financial: Conduct an economic analysis and think of solutions to fund the new system (C, N).

6.1.7 Broadband MCC in Smart City Activity System, Ecosystem and Technology Assessment Model

From the analysis of the interviews, it was possible to construct the MCC in Smart City Activity System, by grouping the answers according to canvas categories, namely: Tools, Object of the activity, Division of Work, Community, Rules, and Subject of the activity, as shown in Figure 52.

Figure 52 - MCC in Smart City Activity System (Author).

The Ecosystem shown in Figure 53 (53a represents the right side and 53b represents the left side of the entire Figure) is described by its Composition, Environment, Structure and Mechanism (CESM). It proposes indicators to evaluate the system, some of which were cited in the interviews, while others were identified in the SLR (section 4.4), as indicated in Figure 54.

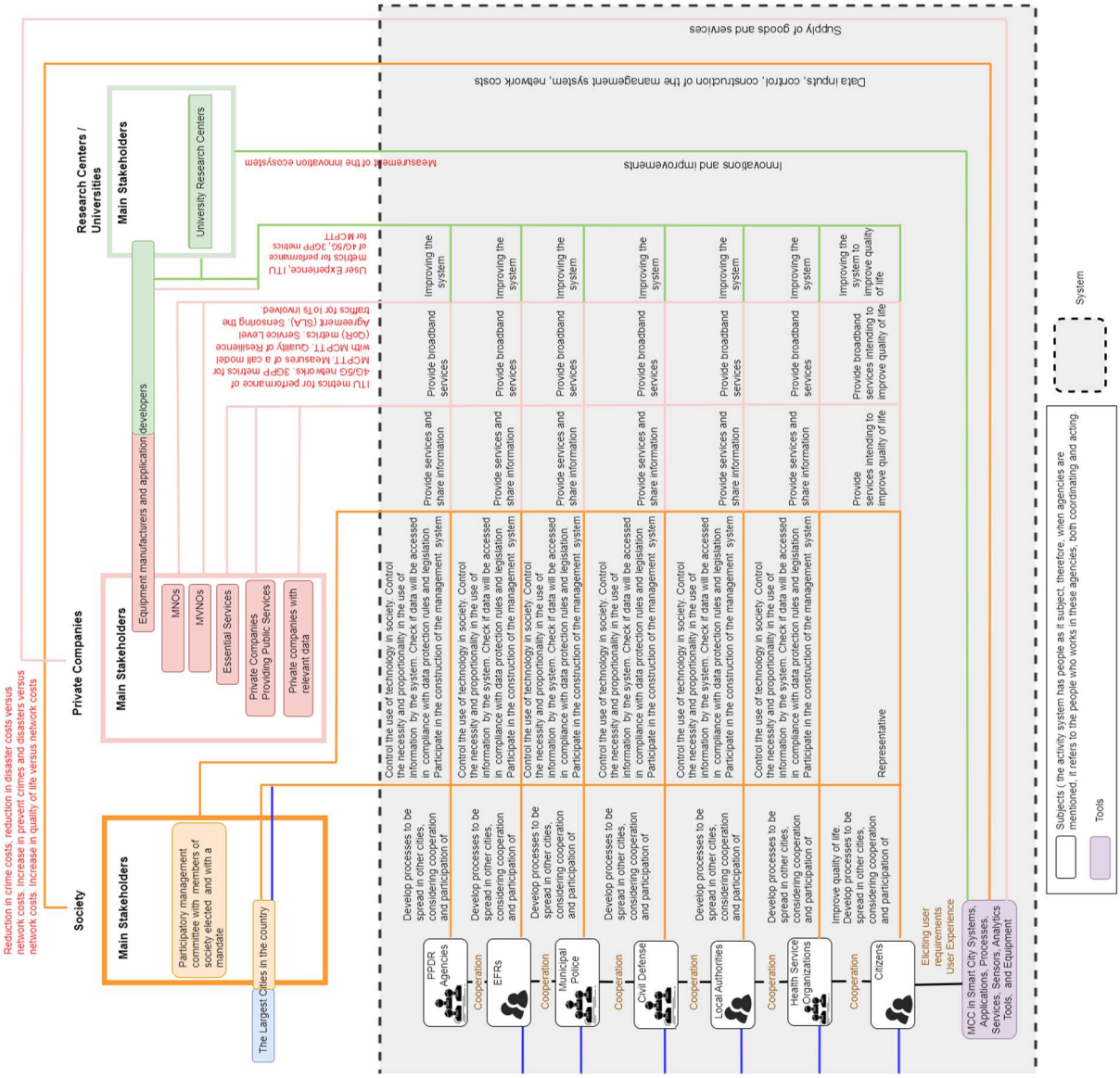


Figure 53a - CESM System (right side) representing the MCC in Smart City Ecosystem (Author).

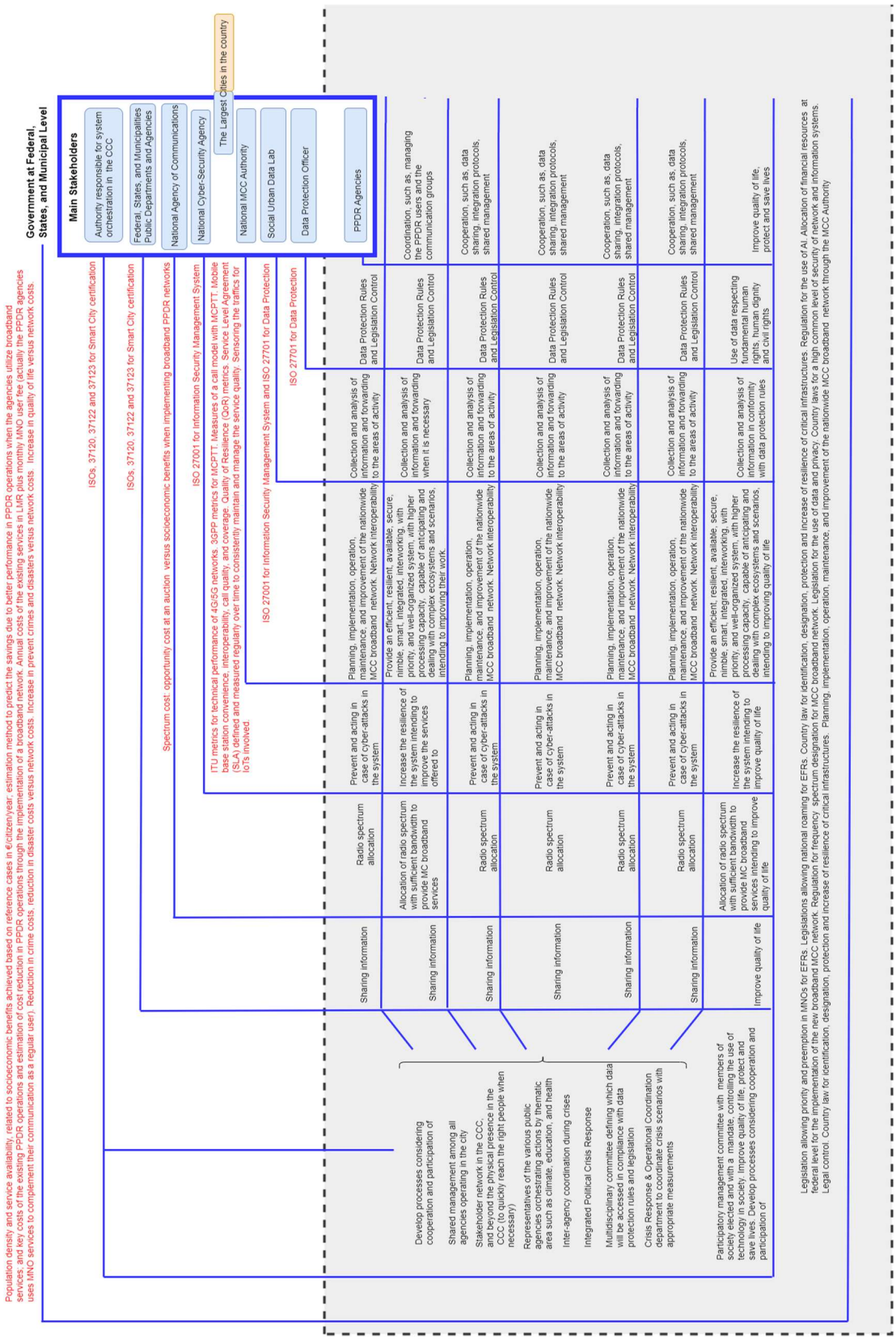


Figure 53b - CESM System (left side) representing the MCC in Smart City Ecosystem (Author).

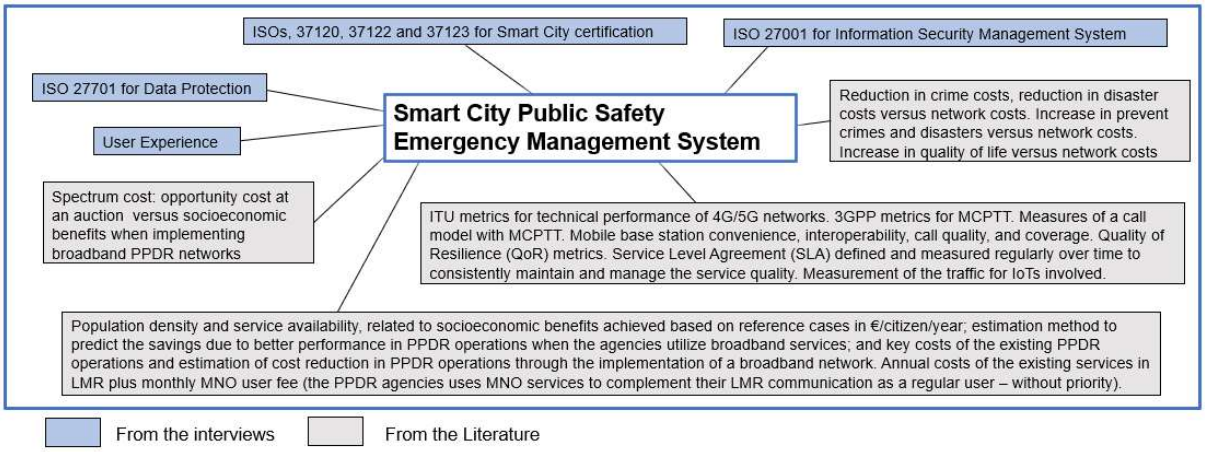


Figure 54 - Indicators to evaluate the system from literature and interviews (Author).

In the Technology Assessment model, the elements of the CESM system will be the dimensions, which may be some or all of them. The fields of study that should be analyzed for valuation in the informational flow are the links between the elements (mechanism) of the CESM, the performance indicators, and the description of relation, some or all of them should be analyzed, according to each applied case. Figure 55 shows the MCC in Smart City TA model, constructed from the CESM system considering two subjects (citizens and EFRs), and three environments (society, government and private companies), according to the applied case other elements could be considered for the TA model.

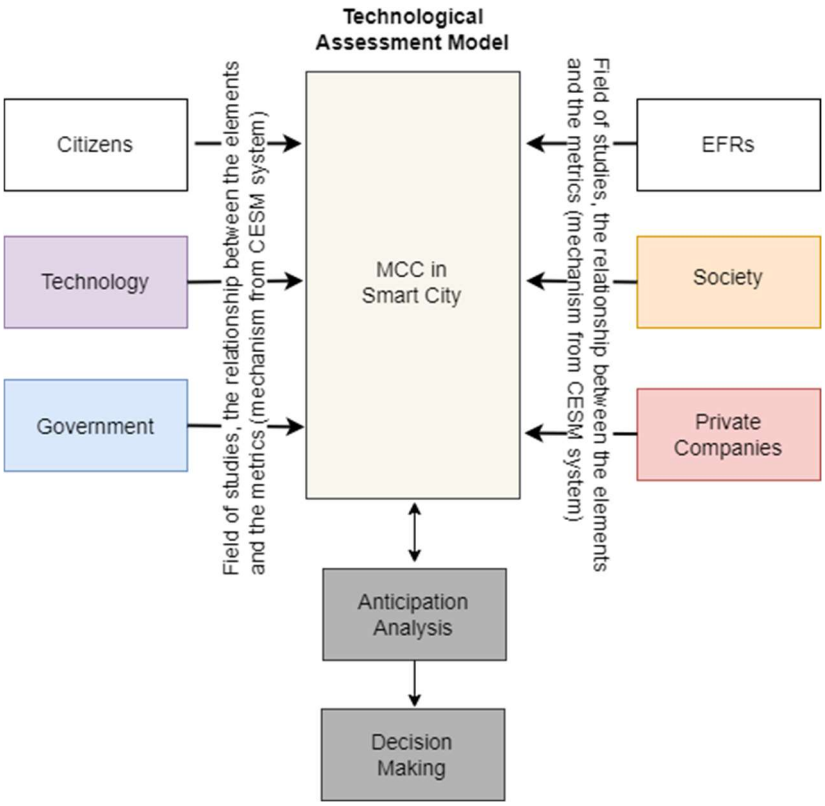


Figure 55 - MCC in Smart City Technology Assessment Model (Author).

6.2 Technology Dimension

From the SLR, before developing the broadband MCC system, some questions should be asked, as suggested by Ulema (2019), regarding to: 1) The type of organization that will use the system. 2) The number of organizations and the number of users. 3) Coverage — to map if the MCC will be local, regional, or a nationwide system. 4) Interoperability — to map if the MCC system will be interfaced with other agencies and which technologies are used by the other entities. 5) Data requirements — to map if the system will need to use significant data-intensive applications. 6) Finance — to map the available funds, how the financing will occur and if there are any issues regarding sharing the network with other entities. 7) Nationwide plan — to map if there is a nationwide MCC broadband plan already in course, and if there is any master ICT plan for the organization. 8) Frequency spectrum — to map if there are frequency spectrum bands allocated for the new MCC broadband system.

Beyond the aspects pointed out before, in a more general sense, other aspects should be taken in consideration. As highlighted by Ulema (2019, p. 176), "conducting a set of feasibility studies, developing a business case, performing a risk analysis, drawing up a roadmap, developing a set of project plans, and establishing a project team as well establishing some related policies should be all part of the planning process". A risk analysis of the possible alternatives should be carried out, looking for answers to questions such as "what can go wrong if we choose this technological path?" to assess each possible impact of each risk. Then, it is necessary to develop a business case to demonstrate the alternatives, benefits, costs and risks of all technological paths, including approaches on economical, technical and social benefits, with objective evaluations and recommendations based on scientific investigations and methods, intending to carry out an objective and well-designed decision-making process.

From the analysis of the interviews, it is possible to construct the Technology Dimension, with three inputs to consider: the main Tools and the Object of the activity, both described in the canvas, and the results of a survey on the technological scenarios. The survey is a Data Collection Modular Model constructed based on the information from the MCC in Smart City Activity System (Figure 52), and following the structure of possible combinations of questions (Figure 57), which should be constructed according to each applied case. Below there are some examples of questions constructed based on the MCC in Smart City Activity System and based on the structure of construction rules shown in Figure 57.

From the analysis of the canvas and following stage three of Mwanza's methodology, it is possible to decompose the Activity System through the group definition. From stage four of Mwanza's methodology, it is also possible to construct questions for the Data Collection Modular Model, aiming to carry out a survey of the current scenario and future applied case scenarios. The Technology Dimension is presented in Figure 56, where the Data Collection

Modular Model is represented and should also consider aspects raised in the bibliographic review and the SLR.

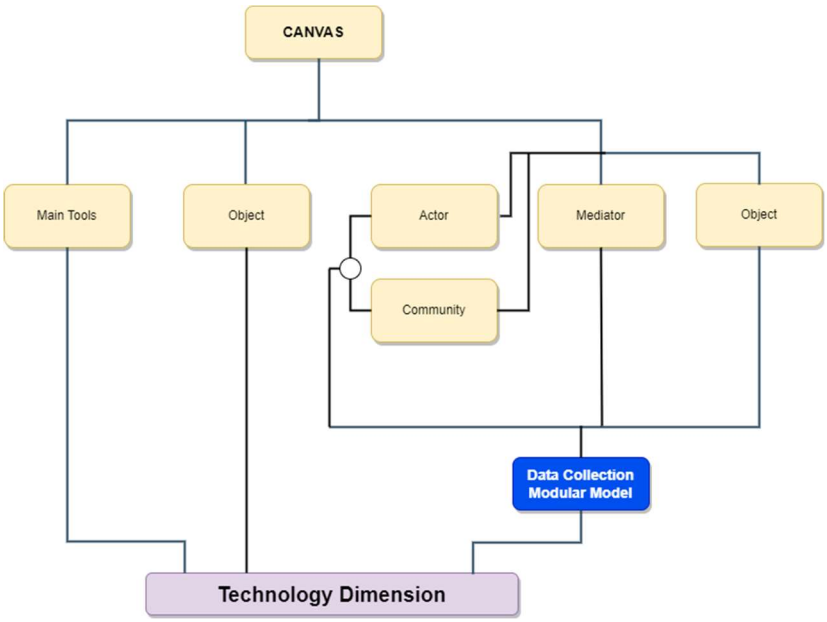


Figure 56 - Technology Dimension (Author).

The questions are formulated from the groups, articulating: 1) Actors, which can be Subject or Community; 2) Mediators, which can be Tools, Rules, Regulations, or Division of Labor; 3) Object. The questions follow the compositions shown in Figure 57, namely Subject/Tools/Object; Subject/Rules/Object; Subject/Division of Labor/Object; Community/Tools/Object; Community/Rules/Object; and Community/Division of Labor/Object. The Community relates to the social and cultural context in which the Subjects performs their activities, listed in the canvas field Community. From the Canvas, the information must go into the groups Subject, Community, Tools, Division of Work, and Object. Then, the questions are constructed following the logic represented in the Data Collection Modular Model, shown in Figure 57.

Actor		Mediator		Objective
Subject	How do they use it →	Tool	to achieve →	Object
Subject	← How does it affect	Rule	to achieve →	Object
Subject	← How does it influence	Division of Work	to achieve →	Object
Community	← How does it affect	Tool	to achieve →	Object
Community	← How does it affect	Rule	to achieve →	Object
Community	← How does it affect	Division of work	to achieve →	Object

Figure 57 - Data Collection Modular Model, adapted from de Mello (2018).

Considering the questions that should be asked, according to the SLR, and the points presented by the experts in the interviews, it is possible to construct several questions aiming to understand the best solution for each applied case. With the answers, an objective evaluation should be performed to understand how much the tool helps to achieve the Objective of the activity (MCC in Smart Cities). The canvas (Figure 52) shows the objectives indicated in the interviews (Object field); however, if city's main objective is to solve problems related to car theft, for example, which is not written in the canvas, the questions to be asked in this case must start from that objective, analyzing which tools will impact the resolution of the problem and how. Highlighting that the canvas is not intended to be an exhaustive list, other Tools, Object of the activity, Division of Labor, Community, Rules and Subjects of the activity are possible, these being the ones mentioned by the experts during the interviews.

Aiming to hierarchize the solutions, a score can be kept and used as input for the informational flow presented in the TA model. The analysis of the tools should take into account the broadband network options for MCC, presented in Figure 30 (Paths for MCC in Smart City scenarios) and Figure 21 (Panorama of Cyber-Physical Systems for PPDR purposes), representing the communication and information options to construct the system. These are presented in an integrated way in Figure 58, which describes the technological paths for the Smart City Public Safety Emergency Management system. As shown in Figure 56, the Data Collection Modular Model should be applied with the intention of analyzing the tools related to the technological scenarios, according to the objectives of the activity.

With the answers from the Data Collection Modular Model, the municipality or PPDR agencies will have a better understanding of the current scenario, and which are the best technological options for the applied case. Meaning, starting from an overview of the Smart City Public Safety Emergency System is possible to construct scenarios using combined solutions for Information and Communication technologies, according to the answers of the Data Collection Modular Model. Those solutions will be the ones analyzed on the informational flow of the Technology Assessment model (Figure 55). Some examples of question constructions are listed below, structures that make sense for the applied case should be used.

1. How do the **citizens** (subject), using **applications where they can inform the local authorities about problems that occur in the city, such as damaged equipment** (tools), help to achieve the objective of **empowering people by making them participants and beneficiaries of the system** (objective)?
2. How does the **municipal police** (subject), using **3GPP compliance applications** (tools), help to achieve the objective of **the ERFs having better situational awareness and the CCC having more resources for a better decision-making process** (objective)?

3. How does the **civil defense** (subject) make use of **IoT** (tools) to achieve the objective of **saving lives, protecting people, and acting in disasters** (objective)?
4. How does the **country laws for a high common level of security of network and information systems (following the directive 2016/1148 in EU)** (rules) affect the **local authorities** (subject) to achieve the objective of **having a system always available even when all other systems are not** (objective)?
5. How does the **frequency spectrum designation** (rules) affect the **PPDR agencies** (subject) intending to achieve the objective of **providing better services to society for mission-critical situations regarding the services offered today, with higher quality in the decision-making process** (objective)?
6. How does the **legislation allowing priority and preemption for EFRs in commercial MNOs** (rules) affect the **EFRs** (subject) intending to achieve the objective of **protecting citizens** (objective)?
7. How does the **dispatch center managing the PPDR users, and the communication groups** (division of work) influence the **EFRs** (subject) intending to achieve the objective of **having better coordination in the CCC and better information provided to EFRs** (objective)?
8. How does the **participatory management committee with members of society elected and with a mandate, controlling the use of technology in society** (division of work) influence **citizens** (subject) intending to achieve the objective of **strengthening democracy** (objective)?
9. How does the **crisis response and operational coordination agency coordinating major crisis scenarios with higher hierarchy** (division of work) influence **health service organizations** (subject) intending to achieve the objective of **serving citizens better to improve their quality of life** (objective)?
10. How does the **gateway to integrate LMR and 3GPP networks** (tools) affect the **places where a disaster is happening** (community) to achieve the objective of **having a better performance before, during and after crisis scenarios, and even being able to avoid them** (objective)?
11. How does the **license plate recognition cameras** (tools) affect the **highways** (community) intending to achieve the objective of **the Police acting with greater efficiency and lower lethality** (objective)?
12. How does the **cross-border and cross-region governance and solution** (rules) affect the **public transportation companies** (community) to achieve the objective of **PPDR agencies and the CCC taking smart actions to better serve citizens** (objective)?
13. How does the **multisectoral coordination of the CCC, among various stakeholders (government, civil society, private sector) and sectors (environment, health, etc.)**

(rules) affect **anywhere where a life is in danger** (community) to achieve the objective of **meeting the UN Sustainable Development Goals** (objective)?

14. How does the **Data Protection Officer (DPO), ensuring data usage in compliance with applicable data protection rules and legislation** (division of work), affect the **CCC** (community) to achieve the objective of **meeting MCC requirements in LMR and providing integration capabilities between PPDR agencies, being fed by a wide range of data sources from cities and other agencies (not only PPDR)** (objective)?
15. How does **a nationwide authority to deploy, operate, maintain, and improve the nationwide MCC broadband network (e.g., FirstNet Authority)** (division of work) affect **federal, states and municipalities' public departments and agencies** (community) to achieve the objective of **having an efficient, resilient, available, secure, nimble, smart, integrated, interworking, with priority, and well-organized system, with higher processing capacity, anticipating and dealing with complex ecosystems and scenarios** (objective)?
16. How do **private companies providing relevant data** (division of work) affect **pilgrimage places** (community) to achieve the objective of **protecting lives in danger with proper information and smart actions based on past data and situational awareness** (objective)?
17. How does the **social urban Data Lab, with collection and analysis of information, and forwarding to the areas of activity** (division of work), affect the **traffic management agencies** (community) to achieve the objective of **delivering real-time information to EFRs** (objective)?
18. How do **meteorological agencies providing data** (division of work) affect the **airports and harbors** (community) to achieve the objective of **having more effective plans to act in dangerous situations** (objective)?
19. How does **the National Cybersecurity Agency, acting in cases of cyber-attacks on the system** (division of work), influence **the local authorities** (subject) to achieve the objective of **having an efficient, resilient and safe city** (objective)?
20. How do **EFRs involved in solution design from the beginning, an user-centric design solution to prevent EFRs from not using new technology** (rule), affect the **research centers** (community) intending to have a **system that enables integration of resources and systems between agencies and cities** (objective)?
21. How does **citizen information versus society´s interest in the use of information (necessity and proportionality in the use of information by the system)** (rules) affect **private companies providing public services** (community) intending to achieve the objective of **having more effective plans to act in dangerous situations** (objective)?

7

Technological paths for the Smart City Public Safety Emergency Management System

All systems should make use of a Decision Support System (DSS), allowing users to improve situation assessment with information and voice/data transmission systems integrated into a single system, as proposed by the European projects FIRE IN (2023) and IN PREP (2023) and presented as a use case by Palestini (2021), who presented the impact of ICTs on rescue and emergency management in Italy. According to Palestini (2021, p. 399), "DSS is an interactive computer-based system or subsystem intended to help decision-makers use communications technologies, data, documents, knowledge and/or models to identify and solve problems, complete decision process tasks, and make decisions". In summary, DSSs are computer applications that can enhance the decision-making process. In that sense, Figure 58 presents the technological paths for the construction of a DSS for emergency management, hereby called Smart City Public Safety Emergency Management system. This Figure put together the information presented about the technological paths for information and communication in broadband technologies as part of an integrated system.

The technological paths for the Smart City Public Safety Emergency Management system, shown in Figure 58, were constructed based on the SLR, use cases analysis and on empirical data collected from the interviews, representing an overview of tools, systems and use cases. The assessment of which technological options and tools should be adopted as applied case scenario is facilitated by the presentation of the Canvas Activity System (Figure 52), the Ecosystem (Figures 53a and 53b), and the Technological Assessment (TA) model (Figure 55) with the Technology Dimension decomposition (Figure 56). The Technology dimension of the TA model is presented with indications on how to evaluate this dimension, starting from the Canvas Activity System elements, then with the construction of the Data Collection Modular

Model through the combination of information groups from the Canvas Activity System, according to the logical grouping represented in the Figure 57. These technological paths are expected to enable and support an objective evaluation of which technological application is the most indicated, according to the applied case. Then an objective evaluation of the technological solutions can be made through the mechanism (field of studies, the relationship between the elements and the metrics) from the CESM system, represented in the Ecosystem (Figures 53a and 53b).

On the technology dimension of the TA model, the questions from the Data Collection Modular Model are used to gather knowledge about the best options for the applied case scenario. With a better understanding through the answers, it is possible to build scenarios using the information and communication tools to achieve the objectives of using the technology in the city, according to the needs of the municipality and PPDR agencies.

For example, for some cities, the most relevant objectives might be "Have better plans to act in dangerous situations", "crime reduction", "meet the UN Sustainable Development Goals" and "Prevent risks based on date". In addition, some cities may face problems related, for example, to high rates of car theft, landslides in residential areas in the rainy season and large seasonal concentrations of people on pilgrimage. The results of the technology dimension will be applied case scenarios with combinations of ICTs that best suits the municipality or agency. This applied case scenarios (the combination of the tools and systems chosen) are used as input to the technology dimension of the TA model, then evaluated through the mechanism in the ecosystem.

Figure 58 considers the CCC and EFRs using the MCC system, and the community, feeding and receiving information through social computing, part of the CTA approach. Figure 59 shows how to build the applied case scenarios. However, before deciding the best scenario, Anticipation Analysis should be performed to mitigate potential adverse outcomes stemming from the implementation of the technology. For example, with technological evolution, such as the 6G networks, it is expected that more AI will be used, this increased incorporation of AI in the Smart City Public Safety Emergency Management System and the social impacts should be analyzed, for better understanding of its future use, and anticipate negative consequences. However, Anticipation Analysis is not within the scope of this research.

Figure 60 shows the framework to the construction of the applied case scenarios used in this research summarized in steps. The six-steps model (Freire, 2019), used to get empirical data, is more suitable for use when the evaluator already has an idea of the technological options that will be evaluated, allowing a better understanding of the current scenario, and what are the demands and objectives that should be achieved with the new technology, system or processes to be adopted. Also, including the realization of a PoC for new technologies that are not yet in use to facilitate an objective comparison through the same parameters with the technologies already known. For LMR systems, the six-steps model was the most appropriate

due to the comparison between APCO-25, TETRA, TETRAPOL (already known technologies with different usage models also previously mapped) and LTE (which was indicated as a new technology for MCC) with the need for a PoC in order to have a comparison between technologies, since in the case study in Brazil carried out in Freire (2019) there were no active MCC-LTE networks in this country to compare with the solutions already in use.

The framework presented in Figure 60 is best applied to situations in which the new technologies, systems, processes and models to be adopted are not clear, and it is necessary to previously know the possible adoption models, then build some scenarios for the applied case and, in the sequence, evaluate the scenarios chosen for choosing the one that best meets the objectives of using the technology. The framework for building applied cases scenarios summarized in Figure 60 can be applied for other technologies, by adapting the questions from the Step 3 to the technology to be evaluated.

For this research, since the objective is to enable the exercise of the TA for broadband MCC in smart cities, as the technologies, systems, processes and models of use were not clear (there are several options and possibilities of use), it was imperative to get to know the solutions better and present them through a general scenario to facilitate the understanding and construction of applied case scenarios. With this, it is possible to make an objective comparison through the mechanism from the CESM system (ecosystem shown in Figures 53a and 53b) and present it in a normalized way, with weights of attendances for each scenario evaluated, which will be the result of the TA exercise, as shown in Figure 60.

In resume this research delivered what is presented in Figure 61, an overview of ICTs for PPDR purposes in an integrated way, the Smart City Public Safety Emergency Management System presented as a general scenario, and possible paths to construct the applied case scenarios. Presented indicators for costing and validation of the solutions (summarized in Figure 54). Presented the Data collection Modular Model, that should be applied by the municipalities or PPDR agencies for better understanding of the applied case scenarios, and choice of the technological solutions to be used as input of the Technology Dimension. Also, presented the Ecosystem constructed through CESM, where the municipalities or PPDR agencies should choose the mechanisms to evaluate the technological solutions. With this, starting from an overview with several use case options, it is possible to select combination of solutions and systems that best suit the applied case, according to the objectives that are intended to be achieved with the use of the technology (MCC in Smart City).

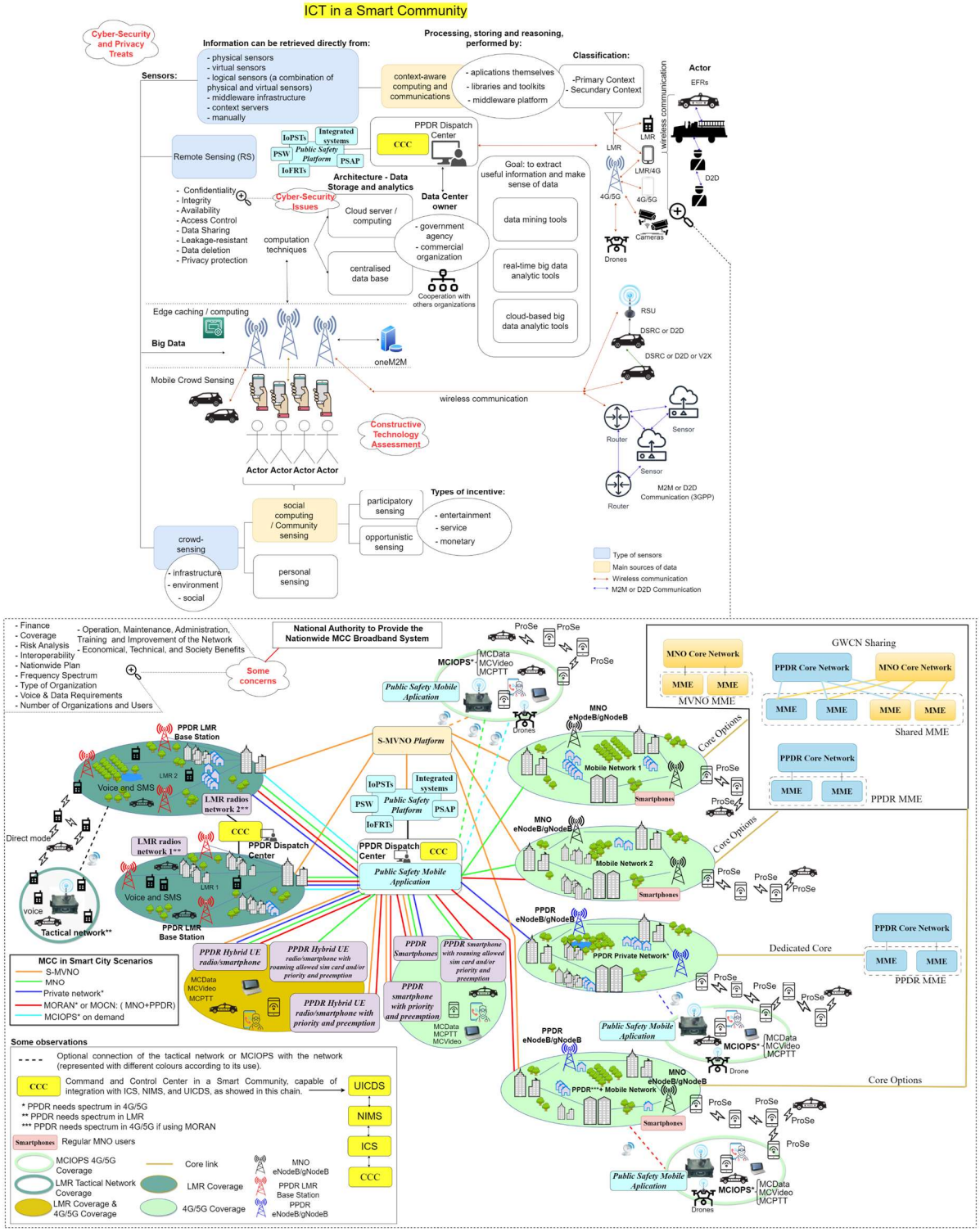


Figure 58 - Technological paths for the Smart City Public Safety Emergency Management System (Author).

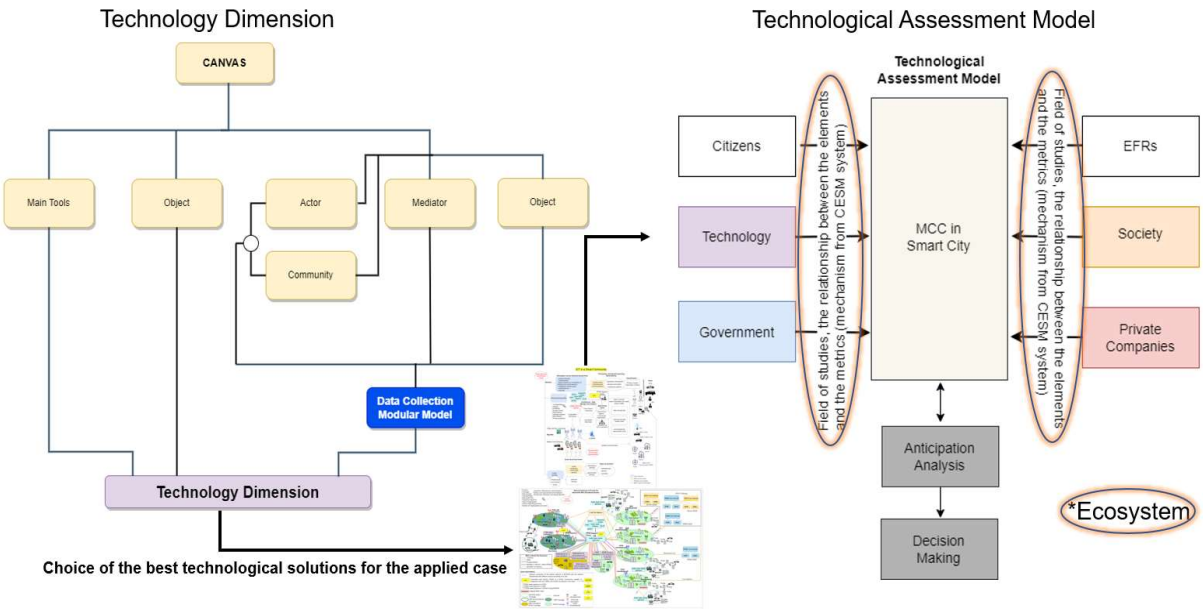


Figure 59 - How to construct the applied case scenarios (Author).

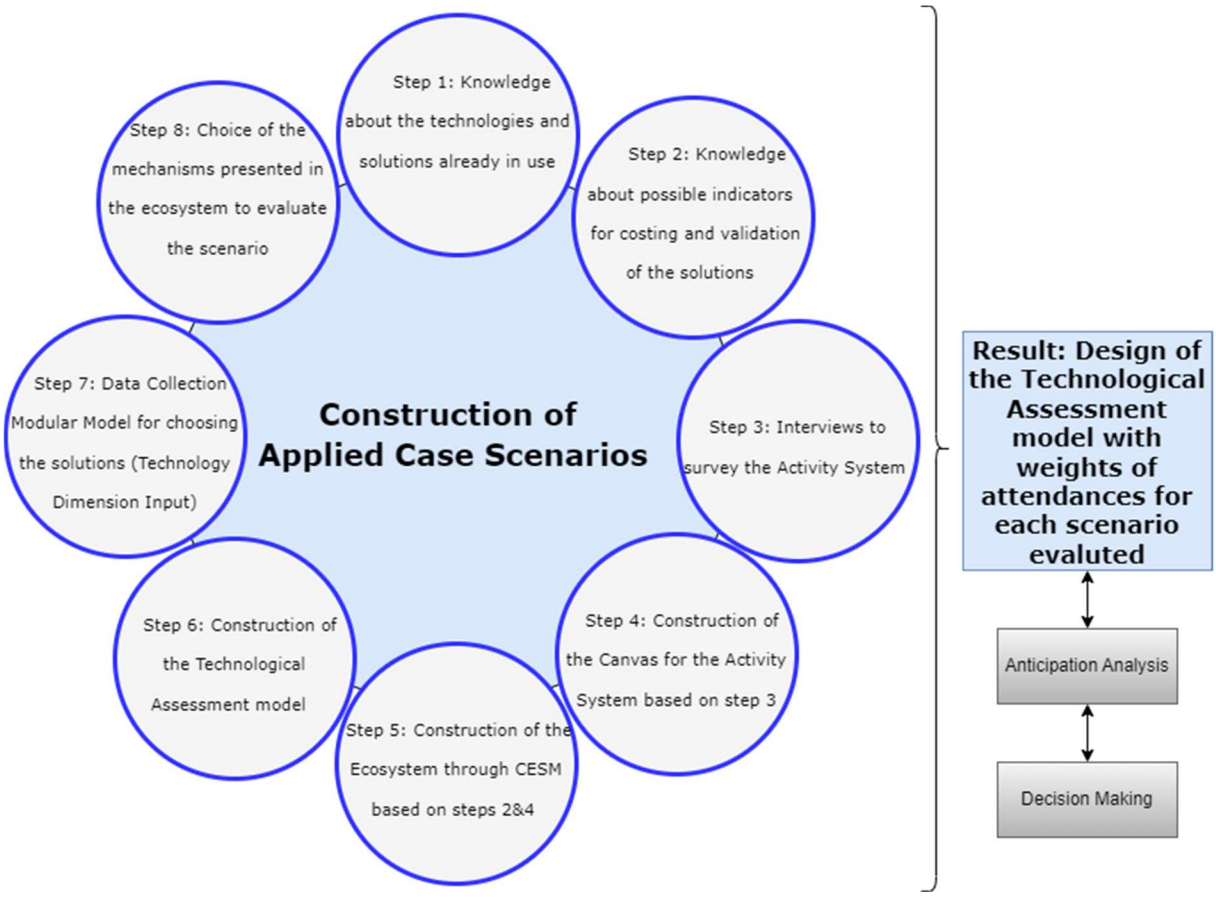


Figure 60 - Framework to construct applied case scenarios (Author).

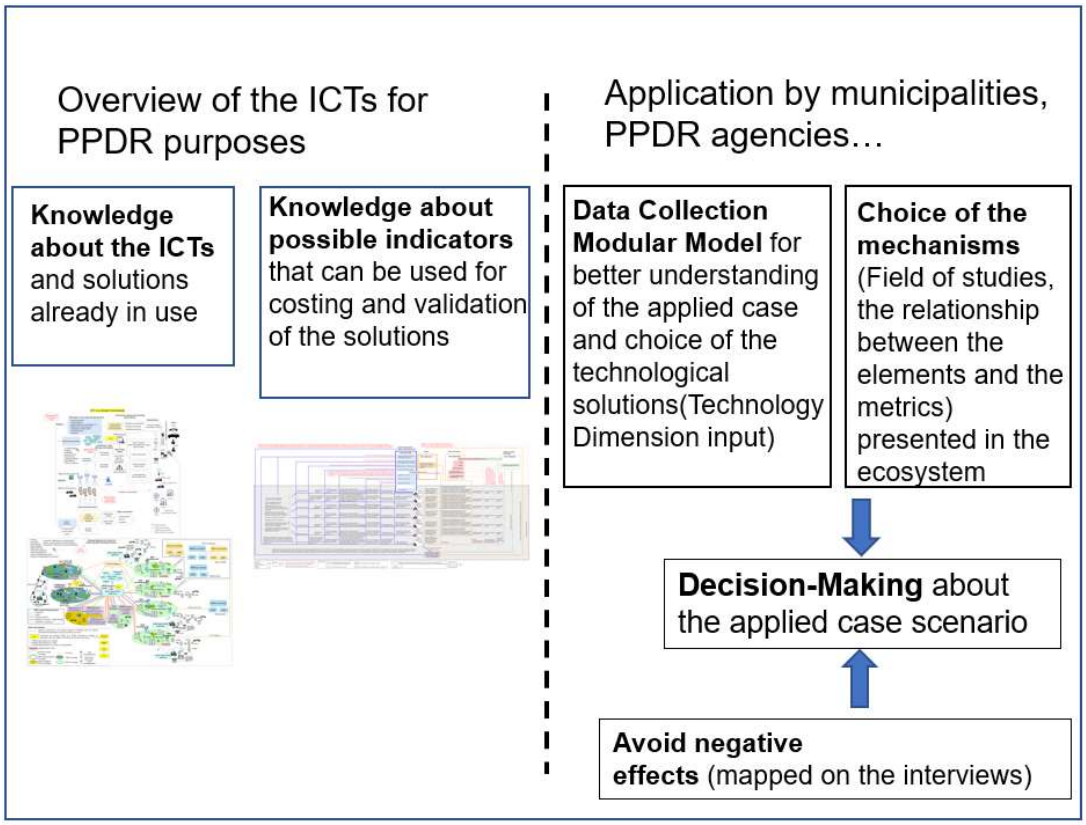


Figure 61 - Summarized outcomes and its application (Author).

When the lack of network availability can put human lives in danger, that is MCC. By placing all stakeholders involved in city management, including citizens, using a common system with orchestration, aiming to achieve the sustainable development goals, that is a Smart City scenario. When Smart City processes and information feed the MCC system, helping the city and PPDR agencies to have an integrated plan to mitigate risks and to act more effectively in PPDR scenarios and recover plans, aiming to achieve the sustainable development goals and to strengthen democracy, that is MCC in Smart City environment.

However, the use of tools that enable this interaction between cities and MCC requires broadband MCC networks. The main objective of broadband MCC in Smart City is to offer society better services for mission-critical situations, in comparison to the services offered today (through LMR networks), with higher quality in the decision-making process due to the variety of stakeholders involved, and with the collection of more information from a variety of sensors such as Remote Sensing, IoTs and Crowd-Sensing, processed with data analytics tools, such as data mining tools, real-time big data analytic tools and cloud-base big data analytic tools, using artificial intelligence and machine learning.

Data analysis and intelligence extraction should not be exclusive for PPDR, but for city intelligence, thus improving Smart City processes and outcomes, and providing real-time information to EFRs using MCC broadband networks. On the information technology side, the data center could belong to a government agency or a commercial organization, meanwhile it

is imperative the cooperation with others government and non-governmental organizations that have relevant data for the city, such as private companies that hold mobile crown-sensing information that can be used, for example, for better urban traffic management.

On the communication technology side, Broadband MCC in a Smart City scenario is expected to be an efficient, resilient, available, secure, nimble, smart, integrated, interworking, with priority, and well-organized system, with higher processing capacity, anticipating and dealing with complex ecosystems and scenarios intending to improve the services offered to EFRs and to the citizens. A broader ecosystem is also expected, with many partners and 3GPP compliance technology tools in constant evolution.

The Smart City Public Safety Emergency Management system takes place when the cities make full use of ICTs in an integrated way, intending to improve the services offered to EFRs and to the citizens through the use of sensors; cloud computing; data analysis and intelligence extraction; real-time analysis and sharing information; and 3GPP communication networks starting from 4G, being able to evolve for future developments such as 5G and 6G, and making use of all the resources made available by these technologies, such as QoS control, massive MIMO and beamforming, Network Function Virtualization (NFV), Multi-access Edge Computing (MEC), Software Defined Networking (SDN), allowing the system to support multiple use cases with different demands as eMBB, mMTC and uRLLC. The objective of the Smart City Public Safety Emergency Management system is to facilitate a better performance of the Emergency Management system and the actions of the actors involved (including other actors beyond EFRs, as the system is more open and allows interaction with other actors such as citizens), before, during and after PPDR scenarios, being able to even avoid those scenarios, delivering efficient essential social protection and disaster relief services.

Meanwhile, the protection of the individual and society must strike the right balance between the citizens' and the society's interest in data use, respecting fundamental human rights, human dignity and civil rights, in compliance with applicable data protection rules and legislation. To make this possible, the technological risks should be mitigated to maintain an efficient, resilient and secure system, capable of increasing city resilience and avoiding service disruptions.

Also, a clear definition of the target KPIs to be achieved is needed, such as improvements in public health, education and environment, GDP, crime reduction, and so on, with frequent measurements of KPIs and taking actions to mitigate possible negative consequences on society that deviate from the goal of achieving the SDGs and strengthening democracy (avoid negative effects). In MCC in Smart City environment, citizens and EFRs are subjects and part of the objectives of this new system, through a more open system that makes use of technology to empower them, making them simultaneously participants and beneficiaries.

For all this to happen, governance, coordination, preparation, and inclusive and participatory management are necessary, with risk assessment, well-defined plans for the

present and the future, correct sizing of resources, and Anticipation Analysis of the technology use on society (including the evolution of the technology). In that new ecosystem there are numerous stakeholders with differing interests and positions, which is challenging.

Legacy LMR networks will continue to play a key role in the new system, both in the transition from narrowband to broadband, while new technologies do not meet all requirements for MCC, as well as a safe and reliable network, tested in several mission-critical scenarios, that can be used on demand, taking advantage of benefits such as greater range due to the high uplink power of the radios and use of lower frequencies. With a broadband network as the goal, existing resources can be used as part of the new system.

Implementing technological solutions for the use of data could help delivering essential social protection services and disaster relief before, during and after disasters, and even predicting disasters, what justifies the use of MCC considering Smart City environments. It could also help delivering essential Public Safety services, analyzing spatial and temporal data of an area to take more effective actions, and even predicting the characteristics of a PPDR event, e.g., a disaster or a crime. The data collected by IoT devices can be process by Machine Learning (ML) algorithms to provide better accuracy for the Smart City Public Safety Emergency Management system, providing real-time information to the EFRs and Emergency Alert Service to the population. In order to provide early warning information, communication and cooperation in different levels (regional, national and global) are required.

Such system could use a variety of ML technology and a variety of, sensors such as remote sensing, android-based sensors, satellites, IoTs, and UAVs. Heat, smoke and radiation sensors installed in offices, homes and other public places could also be used for detection. With accurate information, early signals can be delivered to the population at the right time, avoiding causalities. The use of UAVs solves the accessibility problem in areas that are difficult to reach and monitor, having been used to capture images, map real-time data, and monitor nearby activities during disasters, helping to localize victims and optimize safe routs. It can also help analyzing the losses in the post-disaster phase, integrating an IoT-powered UAV-based Smart City management system.

The Cyber-Physical System (CPS) data collection and processing can be speeded up through cloud computing, with the parallel processing and execution of tasks and queries. Caching at the edge, distributing the processing, and caching execution tasks, using cloudlets whenever possible, is another strategy for a better processing workflow. Transforming the data in manageable sizes is an efficient way to help dealing with big data. Also, methods of big data analytics are used to accelerate the processing and optimize the information extraction from big data. At the CPS devices' side, the use of M2M and D2D communication can help dealing with the enormous volume of communication from the devices to the network, reducing latency and accelerating data delivery.

Security and privacy issues are the main concerns in cloud computing, fog computing, M2M communications and, from the user side, with the possibility of private information leakage. Predictive policing is another concern, since software are designed to learn from big data analysis and reproduce patterns; if biased data is used to train the predictive models, the result is discriminatory policing, resulting in ineffective models. In that sense, the algorithm should have transparency, allowing some external auditing, in an attempt to make predictive policing source code open and providing a framework for deploying predictive models based on crowd-sourced information, with a high level of algorithmic transparency.

Big data collected from a variety of sensors and ML algorithms to process data and delivery results can be used to overcome issues and improve the Smart City Public Safety Emergency Management system. The use of appropriate techniques can improve the security in terms of data confidentiality, integrity, availability, access control, data sharing, leakage of data, data deletion, and privacy protection. Nevertheless, it is quite necessary to incorporate different strategies to face security; combining different techniques appears to be the best solution to ensure a robust system against attackers.

About the scenarios for the digital transformation of Mission-Critical Communication considering Smart City options, to achieve integration with Smart Cities, broadband technology using an entire commercial system, private systems, MVNO or hybrid scenarios is needed, in order to leave the isolated world of LMR and become integrated with IoT and data from the cites' intelligent systems. The LMR system can also be integrated as part of the new system, to facilitate the transition from narrowband to broadband and act as reliable backup network to complement the Smart City Public Safety Emergency Management system.

The proposed system is more open than the current LMR system and enables the performance of several actors, where the market is also more open through the use of information and communication solutions with well-defined and open standards, such as 3gpp compliance, for this reason, it is expected that the market will have a great interest in the construction of this system. To make the model less generic, it is essential to carry out applied cases and the open ecosystem can facilitate these applications. In regions that already have technological innovation partnerships with universities, research centers, government entities and private companies, the application of this model may encounter less difficulties to happen, being fundamental the creation of this open ecosystem and the broad participation of several actors in the design of the solution, in a Constructive Technology Assessment approach.

8

CONCLUSION

This chapter brings some reflections about the topics investigated in this research.

8.1 Social aspects

When it comes to data protection and privacy in a Smart City context, with the possibility of accessing various information from different agencies, such as electricity, water, gas, police, and traffic, among others, legal issues and data privacy issue arises. What information should PPDR agencies be able to access and handle? How to use this information in a transparent way, bringing real benefits to the population without going beyond legal principles? How to use artificial intelligence to process information without introducing prejudice or losing control of the processed data? How to involve citizens in these discussions?

In addition to the technological analysis, the democratic states and the society should reflect on what surveillance and privacy should be, and what should be the limit of access to information in the cities. Regarding the use of data combined with artificial intelligence to anticipate criminal events, if it replicates a program carried out by a person who is inserted in society, the society should reflect on how much of the stigmas of the positivist school of criminal anthropology still exist.

In developing countries, for example, the number of the prison population, associated with their economic, social and physical characteristics, points to an elective and stigmatizing system that seems to reinforce social inequalities. If the reading is carried out based on this population, it replicates Lombroso's study and the effects are amplified by technology, with the system conceiving the man as an enemy, amplified by society's fear of surveillance, almost legitimizing the enemy's criminal law.

This panorama of mapping identification and behavioral profiles, associated with the massive manipulation of computer data (such as the Cambridge Analytica) and technological ubiquity in real time, leads to the fear of a dystopian social and criminal policy, with the use of

individual data for predictive police investigation, for example, or crime futurology as a pretext for social control, as shown in science fiction movies like "Minority Report".

In this scenario, if technology is not properly regulated, it can transform the penal system into a punitive and justified machine even before the threat is absolutely proven, replicating stigmas, feedback differences and punishing in a timely manner — almost like the atavistic criminal of post modernity, the "Lombrosian" way, driven by the surveillance society, which covertly legitimizes the enemy's criminal law while showing a democratic constitution based on the pillars of human rights.

It is up to society itself to find ways to limit the use and format of the technologies, to maximize the positive effects and minimize the negative ones. In these terms, the Technology Assessment approach can help governments and civil society to find possible paths for the transformation of the cities, meeting an ethical, legal and appropriate social pact for people, communities, and cities.

As the ICT sector is experiencing a significant growth in development and solutions, several technological solutions intending to improve the PPDR services are expected. Nevertheless, there should be a better analysis of how the agencies should make the digital transition for each applied case, and how about the society consequences. Many countries still don’t have a Smart City Public Safety Emergency Management, as they still don’t have a particular solution implemented for broadband MCC. In that sense, the constructions of scenarios — role of the Technology Assessment — can help the PPDR agencies in the technological decision-making process of the digital transformation of MCC, considering Smart City options, without increasing the risks of massive disruptions in society.

In that sense, the proposition of the Technology Assessment Framework for the Smart City Public Safety Emergency Management system intends to help the governments and society in the decision-making process, presenting possible paths for the digital transformation while suggesting metrics, including society metrics.

Although, beyond the questions applied to MCC experts, and the Data Collection Modular Model to be applied, the society should be listened via Participative Methodologies, in order to bring the society to the construction of the system as an active stakeholder, being simultaneously Subject of the activity, acting inside the system and feeding it with information through participatory sensing, and acting outside the system, indirectly measured by the social impacts using metrics such as the cost of crime compared with the network costs.

In that way, society could contribute to the realization of successful e-government applications of Digital Participatory Platforms for Civic Engagement, which is aligned with participatory design approach, demanding citizens and stakeholders to the construction of the project life cycle in a Constructive Technological Assessment approach.

8.2 Technological aspects

Critical communication networks differ from commercial networks since they must deliver critical information, maintain data integrity and confidentiality, provide situational awareness and command and control capabilities, interoperate with other systems, and provide access and identity management support for officers, applications, and devices. To attend those requirements, the PPDRs agencies make use of narrowband and broadband technologies for Mission-Critical Communication (MCC). MCC is essential for the maintenance of law and order, response to emergency situations, protection of life and property, and response in disaster relief situations.

Nowadays, in most countries, MCC and Smart Cities are two areas that are not connected. Public Safety organizations look at their own needs, and Smart Cities seek to use the technology so the cities can become smart and innovative in areas such as public transport, traffic, and healthcare. Nevertheless, even with those two areas thinking separately, that integration has become critical. There is a gap of researches intending to connect the two areas, which could result in improvements for both, Smart Cities and Public Safety affairs. MCC considering a Smart City environment could integrate people and sensors providing better services to the EFRs, Public Safety agencies, cities, and citizens.

Narrowband mobile radios have played and will continue to play a significant role in the life-saving responsibilities of emergency and disaster response organizations. Meanwhile, those systems have voice and narrowband capabilities and are also closed systems, not integrated with intelligent resources — meaning they are currently incapable of exchanging real-time visual content, videos, and other vital situational awareness data with first responders. Consequently, the first responders themselves face challenges when attempting to distribute and assess the situational awareness information among their colleagues, thereby hindering their ability to conduct operations safely and effectively. Also, the closed system faces problems of interoperability, making it difficult to integrate PPDR agencies using different LMR systems. In short, legacy LMR networks are insufficient to meet the challenges of today's society, and they are not a proof of future technology.

However, wireless communication has become an important addition to mission-critical actions due to the increasing capacity of mobile broadband networks. Smart devices provide EFRs with the power to use connected components, especially those with critical video and data, changing the way they act and even predicting situations by using mission-critical intelligent services and systems. These are cognitive systems characterized by extreme reliability, ultra-low latency, massive broadband communications with high standard throughput requirements, and intensive machine type communications. To reduce latency and provide real-time performance, new technological concepts, such as Multi-Access Edge Computing (MEC) and Virtual Network Functions (VNFs), implemented at the edge of the

network, are used. Dynamic VNF deployment, exploiting the cloud network infrastructure, and MEC will be considered due to the PPDR scenario's critical requirements such as delay-sensitive traffic. Massive MIMO techniques allow a better throughput in broadband networks, playing a central role in 5G networks. Artificial intelligence (AI) is making these technologies more useful for monitoring, managing, and security, enabling functions such as application-level traffic routing automation, and analyzing large amounts of data to identify anomalies and patterns to anticipate future events.

The literature on the use of technology for PPDR purposes shows a growing interest in the application of AI in infrastructure and operations, with Machine Learning and Deep Learning algorithms, often referred to as artificial intelligence for IT Operations (AIOps). It can support critical functions in 5G infrastructure management by playing roles such as self-management, self-protecting, self-configuration, self-healing and self-optimization.

The main focus of the scientific literature nowadays is on technology-specific opportunities and challenges for enhancing PPDR actions and management, by examining technology-specific and task-specific aspects of the technology use in PPDR fields of action such as disaster relief. This literature provides theoretical and practical contributions for the area. Nevertheless, the technological changes are fast, and the most recent technological solution could be soon replaced by new ones — which could make the technology-specific literature written during this year completely irrelevant in the next few years.

Although various technologies can enhance specific functions and aspects of PPDR management, the success of a particular technique depends on the organization's overall mindset, strategic priorities, and readiness for the new digital era. This area lacks attention in the literature, highlighting a need for a focus on structural and strategic changes that new technologies bring to national management systems. It is essential to formulate new models and frameworks on how these systems can adapt and use digital transformation to address the new challenges of the information society.

Digital transformation poses a threat to a well-functioning system, and it must be approached strategically. It is not just about incorporating technology, but also implementing a strategy for the digital transformation intending to reach the Millennium Development Goals to the cities, as more effective action in natural disasters, intending to improve the city's resilience and the citizens' quality of life. Bridging the gap between physical and digital environments and bridging the literature gaps is crucial to reach technological results beyond the technology, and proof of future design solutions, with positive effects on society, strengthening democracies and improving the citizens' quality of life.

The LMR technology is isolated from intelligent services using specific devices and infrastructure, which are not integrated with other technologies beside LMR. To achieve integration with Smart Cities, broadband technology using an entire commercial system, private systems, MVNO or hybrid scenarios is needed, in order to leave the isolated world of

LMR and become integrated with IoT and data from the cites' intelligent systems. The goal is to provide better PPDR services. On the other hand, Smart Cities mean to collect massive data over a critical infrastructure with high availability, high security, and high processing capacity, complying with local legislation on data policy and privacy. Integrating these two words will be bring more resilience to the Smart Cities, since MCC has requirements that address availability and security, and will bring to MCC data and high processing capacity, both in compliance with local legislation, intending to achieve the same goal, which is improving the city's resilience and the citizens' quality of life.

Creating a new LTE/5G-based network comes with a hefty price tag of billions of dollars, which includes the costs associated with site acquisition and deployment. Therefore, it is essential to design an efficient site deployment strategy that maximizes coverage with minimal sites, while also considering the utilization of existing infrastructure. The LTE/5G-based public safety systems may be costlier than the legacy network, but there are financial and economic options available to mitigate this problem, such as allowing commercial operators to utilize excess capacity and frequency spectrum. The revenue generation opportunities, such as partnerships with utility companies and MNOs, should be explored.

When dedicated spectrum is either absent or not put into use, MNOs can offer to PPDR agencies access to the required network capacity through a combination of software-based functions. These features include prioritization; open-standard mechanisms that prioritize data streams between user devices and applications; and ruthless preemption, which allows authorized first responders to interrupt data flows between non-first responder devices during emergencies, when commercial networks become congested.

Another option is S-MVNOs making use of a single MNO or multiples MNOs, hybrid solutions and private networks. In that development, the utilization of open standards as 3GPP is essential, allowing integration with current 4G and 5G networks, and future development networks as 6G. The implementation of an open-standards technologies guarantees that PPDR agencies are not confined within a specific technology ecosystem, and it promotes lower costs and reduced complexity. Standards also guarantee interoperability between vendors, regardless of whether they are dealing with networks, handsets, or deployable equipment. The entire ecosystem plays a critical role in ensuring that the intended outcome is achieved, being important that all technologies involved are standardized.

Another challenge that must be addressed is the perception that new LTE/5G-based systems may not be as secure as existing public safety systems. While new communication technologies are more software-intensive and virtualized, they can be designed and built to meet security requirements equal to or greater than current public safety systems.

In some cases, choosing alternative scenarios involving multiple technologies may be necessary due to existing deployments that do not meet established criteria and requirements of PPDR networks. In such cases, a new system based on another technology may be used

alongside the current system to fulfill all requirements. However, the ultimate goal should be an LTE/5G technology-based approach, since it offers long-term benefits. The design of an LTE/5G network should consider the applications used by EFRs and PPDR agencies.

There are numerous stakeholders in the Public Safety (PS) ecosystem, with differing interests and positions. However, their shared goal of PS must remain at the forefront. Overcoming stakeholder resistance and educating them is a significant challenge but advocating for the critical importance and need for efficient PS systems with new technologies, additional capabilities, and new opportunities, can help overcome these obstacles.

Effective leadership is necessary to coordinate stakeholders and leverage their strengths to accomplish their tasks. There is a need for national authority to provide nationwide coverage for the MCC broadband system, as the FirstNet authority in the USA, with a national broadband policy for the entire country, addressing commercial and government needs, orchestrating resources and actions to establish the policies for the acquisition process to the new MCC network, and being responsible for the operation, maintenance, administration, training, and improvement of the network, while also coordinating to get all the stakeholders and vendors community involved in the new network. The authority also should be concerned with national and international regulations and standards. Also, setting standardization to the proper work of the system, including spectrum management policies.

The use of ICT integrated with Smart Cities can improve the preparedness and responsiveness to PPDR events, helping in the smart resilience for Smart Cities. The tools need to be smart to collect information and translate the various data in usable information, also, is imperative the coordination among multiple stakeholders with integrated information systems, and public awareness and consent of the population, ensuring privacy and engaging communities in data collection. The CCC should be able to analyze different data sources, from the communication network, and other sources as big data, cameras, information from other PPDR agencies, from its own databases matching with big data information as real-time information from cameras reading license plates, and so on. And then, sending relevant information, even real-time information to the EFRs in the field through broadband networks. The integration of system in a Smart City scenario can improve the accuracy and scientificity of the commanders' emergency decision-making.

The best solution depends on each applied case, simple solutions are also capable of solving complex problems if they are properly mapped, through jointly planned and coordinated solutions, including all actors (public agencies, citizens, etc.) If the Smart City Public Safety Emergency Management system is well design, it is possible to use ICTs to strengthen democracies and improve the quality of life of the population.

This research explores the use of the Smart Cities concept in relation to the performance of PPDR agencies, and the impact of this in society, turning attention to social innovation, with the objective of creating a positive impact for society as wide as possible. This research's main

contribution is to support PPDR agencies in finding a solution for the immediate problem of modernizing the MCC narrowband network (LMR) through 4G and 5G networks, and aggregating intelligence services in a Smart City context.

The research objectives were achieved through the analysis of technology and systems integration in order to solve problems faced in the real world, generating scientific knowledge, and helping organizations through the models, methods, methodologies, security analysis, literature review and studies developed to present the scenarios as a Technology Assessment study considering technical aspects, economic factors, social context, costs and benefits of the solution, the environment/context in which it will be applied — Smart City scenarios, also analyzing multiple actors and interactions with a Constructive Technology Assessment approach, and presenting the ecosystem and the panorama of the Smart City Public Safety Emergency Management system.

8.3 Suggestion for future research

This research constructed scenarios for evaluation of technological options through bibliography review, systematic literature review, mapping of applied cases, semi-structured interview with experts and stakeholders, and assessment of potential scenarios for MCC considering a smart city environment. The interview with experts and stakeholders enables mapping and better understanding of the Activity System through analysis and interpretation, following the Activity Theory for Human-Computer Interaction approach.

The construction of the Activity System in canvas format describing the MCC in Smart City environment, mapping the Object of the activity, the main Tools, the Subjects, the Rules, the Community, and the Division of Work, enabled the construction of the ecosystem, placing it in a broader context, dividing it into its Composition, Environment, Structure and Mechanism; distinguishing system levels; and displaying the relationships between elements, through structures and mechanisms. The technological assessment model, based on the ecosystem, mapped the dimensions that should be analyzed for valuation in the informational flow considering a broad view of the technology.

Mapping the technology dimension based on the previous inputs to carry out a survey of the current situation and possible scenarios through the Data Collection Modular Model, aims to construct the applied case scenarios. Also, the understanding about Smart City Public Safety Emergency management and its relation with MCC is facilitated by the presentation of the technological paths for MCC in Smart City (Figure 30) and the panorama for Cyber-Physical System for PPDR purposes (Figure 21), also presented in an integrated way in Figure 58, with the technological paths for the Smart City Public Safety Emergency management system.

The assessment of the ICTs chosen in the applied case scenarios (measurements of the Smart City Public Safety Emergency Management system) is facilitated by the presentation of

the Ecosystem (Figures 53a and 53b), built through a systemic view. The framework presented to construct applied case scenarios (Figure 60) enables the construction of scenarios and the measurement of system.

This research also presented a wide literature review on the topic, bridging the gap of technology assessment studies in the field of MCC considering a Smart City approach. As a suggestion for future research, application of this framework is expected, e.g., an applied case study at municipalities, or PPDR agencies to help in the decision-making process about the evolution of MCC from narrowband to broadband in a Smart City Public Safety Emergency management system.

Participatory methodologies are not within the scope of this thesis; however, the society should be consulted about the use of the technology and this topic should be better addressed before any decision about the technological path is taken by the government and public agencies. Furthermore, Anticipation Analysis is not within the scope of this thesis but should be better addressed to allow informed early decision-making on the use of technologies that impact the society, where technological risks must be anticipated and mitigated to avoid service disruption and negative impacts on the use of the technology in society.

REFERENCES

3GPP. (2016). 3GPP TS 22.179 V13.3.0 Release 13 (2016-01) (Technical Specification (TS)). https://www.etsi.org/deliver/etsi_ts/122100_122199/122179/13.03.00_60/ts_122179v130300p.pdf

3GPP. (2018). 3GPP Global Initiative LTE. http://www.3gpp.org/technologies/keywords-acronyms/98-lte

3GPP. (2018). TR 36.746, Study on further enhancements to LTE Device to Device (D2D), UE to network relays for Internet of Things (IoT) and wearables, Version 15.1.1. on-line.

3GPP. (2021). TS 23.682 — Architecture enhancements to facilitate communications with packet data networks and applications, Release 17. on-line.

3GPP. (2022). 3GPP TS 38.214 V17.3.0 (2022-09) (Technical Specification (TS)). https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3216

5G-EPICENTRE Project. (2023). 5G ExPerimentation Infrastructure hosting Cloud-nativE Network applications for public proTection and disaster RElief. https://www.5gepicentre.eu/

Abbas, N., Zhang, Y., Taherkordi, A., & Skeie, T. (2018, Feb). Mobile Edge Computing: A Survey. IEEE Internet of Things Journal, 5(1), 450–465. https://doi.org/10.1109/JIOT.2017.2750180

AEL Sistemas. (2022). Safe City. https://www.ael.com.br/safe-city.html

Ahmad, I., & Chang, K. (2019, Aug.). Mission Critical User Priority-Based Random Access Scheme for Collision Resolution in Coexisting PS-LTE and LTE-M Networks. IEEE Access, 7, 115505–115517. https://doi.org/10.1109/ACCESS.2019.2934778

Ahmad, I., & Chang, K. (2020). Mission-critical user priority-based cooperative resource allocation schemes for multi-layer next-generation public safety networks. Physical Communication, 38(100926). https://doi.org/10.1016/j.phycom.2019.100926

Ahmed, S., Rashid, M., Alam, F., & Fakhruddin, B. (2019). A Disaster Response Framework Based on IoT and D2D Communication under 5G Network Technology. In 29th International Telecommunication Networks and Applications Conference (ITNAC). Auckland, New Zealand: IEEE. https://doi.org/10.1109/ITNAC46935.2019.9077975

Al-Sarawi, S., Anbar, M., Abdullah, R., & Hawari, A. B. A. (2020). Internet of Things Market Analysis Forecasts, 2020–2030. 2020 Fourth World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4), 449–453. https://doi.org/10.1109/WorldS450073.2020.9210375

Almeida, L. F. M., Conforto, E. C., & Silva, S. L. (2012, fev.). Fatores críticos da agilidade no gerenciamento de projetos de desenvolvimento de novos produtos. Produto & Produção, 13(1), 93-113.

Alsaeedy, A. A. R., & Chong, E. K. P. (2020, May). 5G and UAVs for Mission-Critical Communications: Swift Network Recovery for Search-and-Rescue Operations. Mobile Networks and Applications, 25, 2063 – 2081. https://doi.org/10.1007/s11036-020-01542-2

Alsamhi, S. H., Ma, O., Ansari, M. S., & Gupta, S. K. (2019). Collaboration of Drone and Internet of Public Safety Things in Smart Cities: An Overview of QoS and Network Performance Optimization. Drones, 3(13), 1 – 18. http://dx.doi.org/10.3390/drones3010013

Anbarasan, M. et al. (2020). Detection of flood disaster system based on IoT, big data and convolutional deep neural network. Computer Communications, 150, 150 – 157. https://doi.org/10.1016/j.comcom.2019.11.022

Antunes, A. R. F. (2019). Bertillonage na Universidade de Coimbra (Relatório de Estagio do Mestrado em Patrimônio Cultural e Museologia apresentado a Faculdade de Letras). Coimbra. https://estudogeral.uc.pt/handle/10316/93351

Apostolakis, K. C. et al. (2021). Cloud-Native 5G Infrastructure and Network Applications (NetApps) for Public Protection and Disaster Relief: The 5G-EPICENTRE Project. In IEEE (Ed.), Joint European conference on networks and communications & 6g summit (eucnc/6g summit): Vertical applications and internet of things (vap). Porto, Portugal: IEEE. https://doi.org/10.1109/EuCNC/6GSummit51104.2021.9482425

Atat, R., Liu, L., Wu, J., Li, G., Ye, C., & Yi, Y. (2018, Nov.). Big Data Meet Cyber-Physical Systems: A Panoramic Survey. IEEE Access: Special Section on Internet-Of-Things (Iot) Big Data Trust Management, 6, 73603 – 73636. https://doi.org/10.1109/ACCESS.2018.2878681

Athonet. (2022). Athonet Tactical Cube. https://athonet.com/products/athonet-tactical-solution-cube/

AxxonSoft. (2022). Safe City Solutions. https://www.axxonsoft.com/industries/safe-city

Baek Byung-yeul. (2020 / Feb. 05). KT begins public safety network project. The Korea Times. https://www.koreatimes.co.kr/www/tech/2018/12/133_260835.html

Baker, W. J. (1971). A History of The Marconi Company. New York: St. Martin's Press.

Baldini, G., Karanasios, S., Allen, D., & Vergari, F. (2014, 2nd Quart.). Survey of Wireless Communication Technologies for Public Safety. IEEE Communications Surveys & Tutorials, 16(2), 619 – 641.

Banta, D. (2009, July). What is technology assessment? International Journal of Technology Assessment in Health Care, Supplement S1, 7 – 7. https://doi.org/10.1017/S0266462309090333

Barnes, L., & Maheu, B. (2023). Updated: How 'sidelink' peer-to-peer communications can enhance public-safety operations. https://urgentcomm.com/2023/02/27/how-sidelink-peer-to-peer-communications-can-enhance-public-safety-operations/

Basit, S. A. (2009). Dimensioning of LTE Network, Description of Models and Tool, Coverage and capacity estimation (Degree of Master of Science in Technology). Helsinki University of Technology.

Bauman, Z. (2003). Modernidad liquida. Mexico: Fondo de Cultura Económica.

Bauman, Z. (2014). Vigilância líquida (1. ed.). Zahar.

Becker, G. (1968). Crime and Punishment: An Economic Approach. Journal of Political Economy, 2(76), 169 – 217.

Bencadirno, M., & Greco, I. (2014). Smart City Planning for Energy, Transportation and Sustainability of The Urban System, Chapter: Smart Communities Social, Innovation at the Service of the Smart Cities. In 8th international conference innovation in urban planning and territorial (input) (pp. 39 – 51). Naples: TeMA Journal of Land Use Mobility and Environment INPUT 2014.

Bentham, J., Miller, J., Perrot, M., & Werrett, S. (2008). O Panoptico (2nd ed.). Belo Horizonte: Autentica.

Bergamaschi, E. A., & Ferasso, M. (2020). Kondratieff's economic waves and future scenarios planning: a long-path approach for organizations' forecasting. Technology innovation management review, 10(2), 51 – 61. http://doi.org/10.22215/timreview/1327

Bertillon, A. (1883). L'Identite des recidivistes et la loi de relegation. Paris: G. Masson.

Bessi, V. G., Zimmer, M. V., & Griscl, C. L. L. (2007). O panóptico digital nas organizações: espaço-temporalidade e controle no mundo do trabalho contemporâneo. Organizações & Sociedade, 14(42), 83-96. https://doi.org/10.1590/S1984-92302007000300005

Bina, R. (2009). Medicina Legal (2. ed., Vol. 13). São Paulo: Saraiva — Coleção Estudos Direcionados: perguntas e respostas).

Bittium. (2023). Secure Communications & Connectivity. https://www.bittium.com/secure-communications-connectivity

Borkar, S., Roberson, D., & Zdunek, K. (2011). Priority Access for Public Safety on Shared Commercial LTE Networks. In Technical symposium at itu telecom world (itu wt) (pp. 105 – 110). Geneva, Switzerland: IEEE.

Bouchenak, S., Merzougui, R., & Harrou, F. (2021). A hybrid beamforming Massive MIMO system for 5G: Performance assessment study. In 2021 international conference on innovation and intelligence for informatics, computing, and technologies (3ict) (pp. 371 – 375). Zallaq, Bahrain: IEEE. http://dx.doi.org/10.1109/3ICT53449.2021.9581878

Bratcher, J. (2018). FirstNet Core Delivers on the Promise of a Dedicated Network for Public Safety. https://www.firstnet.gov/newsroom/blog/firstnet-core-delivers-promise-dedicated-network-public-safety

Broadmap. (2017). Broadmap (D5.2 Final Definition of the Transition Roadmap and PCP Specification). https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5b22af60f&appId=PPGMS

BroadWay. (2022). BroadWay is Procuring Innovation activity to enable a pan-European broadband mobile system for PPDR, validated by sustainable test and evaluation capabilities. https://www.broadway-info.eu/

Buckland, M. K. (1991). Information as thing. Journal of the American Society for Information Science, 42(5), 351 – 360.

Bunge, M. (2000). Systemism: the alternative to individualism and holism. Journal of Socio-Economics, 29(2), 147 – 157. https://doi.org/10.1016/S1053-5357(00)00058-5

Bunge, M. A. (1980). Treatise on Basic Philosophy (Vol.4). Ontology II. A World of Systems. Behavioral Science, 25, 166 – 168.

Bunge, M. A. (1985). Racionalidad y Realismo. Madrid: Alianza.

Bunge, M. A. (2003). Emergence and convergence: qualitative novelty and the unity of knowledge. Toronto: University of Toronto.

Bunge, M. A. (2005). Diccionario de filosofia (3. ed.). Buenos Aires: Siglo XXI.

Burke, P. (2003). Uma história social do conhecimento: de Gutemberg a Diderot. Rio de Janeiro: Zahar.

Caprirolo, D., Jaitman, L., & Mello, M. (2017). The Costs of Crime: selected regions in detail (The Welfare Costs of Crime in Brazil: A Country of Contrasts). In I. D. B. (IDB) (Ed.), The costs of crime and violence, new evidence and insights in Latin America and the Caribbean (pp. 53 – 68). Washington, D.C.: IDB. https://publications.iadb.org/en/costs-crime-and-violence-new-evidence-and-insights-latin-america-and-caribbean

Capurro, R., Hj, B., & Orland. (2003). The concept of information. ARIST, 37.

Carreras-Coch, A., Navarro, J., Sans, C., & Zaballos, A. (2022, April). Communication Technologies in Emergency Situations. Eletronics, 11(7), 1 – 31. https://doi.org/10.3390/electronics11071155

Casoni, M., Grazia, C. A., Klapez, M., Patriciello, N., Amditis, A., & Sdongos, E. (2015, March). Integration of Satellite and LTE for Disaster Recovery. IEEE Communications Magazine, 53(3), 47 – 53. https://doi.org/10.1109/MCOM.2015.7060481

Castells, M. (2002). A Sociedade em Rede (6. ed., Vol. 1). São Paulo: Paz e Terra.

Chamola, V., Hassija, V., Gupta, S., Goyal, A., Guizani, M., & Sikdar, B. (2020, Nov.). Disaster and Pandemic Management Using Machine Learning: A Survey. IEEE Internet Things Jounal, 8(21), 16047 – 16071. https://doi.org/10.1109%2FJIOT.2020.3044966

Chih-YaoMa, Chen, M., Kira, Z., & AlRegib, G. (2019, Feb.). TS-LSTM and temporal inception: Exploiting spatiotemporal dynamics for activity recognition. Signal Processing: Image Communication, 71, 76 – 87. https://doi.org/10.1016/j.image.2018.09.003

Chitturi, S. (2021, October). Application Enablement Standards in 3GPP. 3GPP Highlights newsletter, Standards for 5G(03), 08 – 09. https://www.3gpp.org/ftp/Information/Highlights/2021_Issue03/mobile/index.html#p=9

Chochliouros, I. P. et al. (2021). 5G for the Support of Public Safety Services. Wireless Personal Communications(120), 2321 – 2348. https://doi.org/10.1007/s11277-021-08473-5

Coates, J. F. (2016). A 21st century agenda for technology assessment. Technological Forecasting & Social Change, 113, Part A, 107 – 109. https://doi.org/10.1016/j.techfore.2016.10.020

Cochrane Collaboration. (2022). Cochrane Handbook. http://handbook.cochrane.org

Commission, E. (2022). Mapping Interoperable EU PPDR Broadband Communication Applications and Technology. https://cordis.europa.eu/project/id/700380

Cooner, A. J., Shao, Y., & Campbell, J. B. (2016). Detection of Urban Damage Using Remote Sensing and Machine Learning Algorithms: Revisiting the 2010 Haiti Earthquake. Remote Sensing, 8(868), 1 – 17. https://doi.org/10.3390/rs8100868

Coscia, C., Cocina, G. G., Lazzari, G., & Manzo, S. (2020). Digital Participatory Platforms for Civic Engagement: A New Way of Participating in Society?: Analysis of Case Studies in Four EU Countries. International Journal of Urban Planning and Smart Cities (IJUPSC), 1(1), 1 – 21. https://doi.org/10.4018/IJUPSC.2020010101

Coutinho, R. W. L., Boukerche, A., Vieira, L. F. M., & Loureiro, A. A. F. (2020). Underwater Sensor Networks for Smart Disaster Management. IEEE Consumer Electronics Magazine, 9(2), 107 – 114. https://doi.org/10.1109/MCE.2019.2953686

Critical Comms. (2022). Australia public safety poised to advance with shared-network mobile broadband. https://www.criticalcomms.com.au/content/public-safety/sponsored/australia-s-public-safety-poised-to-advance-with-shared-network-mobile-broadband-491800103

CTI. (2017, October). Análise e apuramento dos factos relativos aos incêndios que ocorreram em Pedrógão Grande, Castanheira de Pera, Ansião, Alvaiázere, Figueiró dos Vinhos, Arganil, Góis, Penela, Pampilhosa da Serra, Oleiros, e Sertã, entre 17 e 24 de junho de 2017. (Análise e apuramento dos factos). https://www.parlamento.pt/Documents/2017/Outubro/Relat%C3%B3rioCTI_VF%20.pdf

Cui, C., Zhou, G., & Chen, C. (2022). Research on Intelligent Mobile Police Application Based on 5G Technology. In 2022 ieee international conference on electrical engineering, big data and algorithms (eebda) (pp. 426 – 429). https://doi.org/10.1109/EEBDA53927.2022.9744766

Cui, D. (2015). Risk Early Warning Index System in the Field of Public Safety in Big Data Era. In 2015 sixth international conference on intelligent systems design and engineering applications (isdea) (pp. 704 – 707). Guiyang, China. https://doi.org/10.1109/ISDEA.2015.180

Cybersecurity and Infrastructure Security Agency (CISA). (2022). SAFECOM. https://www.cisa.gov/safecom

da Costa Queiroz, M. I. P. S. (2015). A Companhia Portuguesa Radio Marconi na Rede Mundial de Comunicações (1906-1936) (Doutoramento em História Contemporânea, Faculdade de Ciências Sociais e Humanas, Universidade Nova de Lisboa). https://run.unl.pt/bitstream/10362/18624/1/InesQueiroz_tesePhD_Marconi2015.pdf

Das, S., Panda, K. G., Sen, D., & Arif, W. (2020). A Survey of National Disaster Communication Systems and Spectrum Allocation — an Indian Perspective. IETE Technical Review, 37(2), 111 – 136. https://doi.org/10.1080/02564602.2019.1566030

da Silva, A. M., & Ribeiro, F. (2002). Das "ciências" documentais a ciência da informação (Vol. 4). Porto: Afrontamento.

da Silva, J. C., & da Silva Horita, F. H. (2017). O Direito Penal do Inimigo no Estado de Direito. Revista Jurídica Luso-Brasileira, Ano 3(4), 845 – 864.

de Albuquerque Barreto, A. (1997). As tecnologias intensivas de Informação e o reposicionamento dos atores do setor. In Info 97. Cuba.

de Albuquerque Barreto, A. (1998). Mudança estrutural no fluxo do conhecimento: a comunicação eletrônica. Ciência da Informação, 27, nd–nd. http://www.scielo.br/scieloOrg/php/articleXML.php?lang=pt&pid=S0100-19651998000200003

Debnath, S., Arif, W., Roy, S., Baishya, S., & Sen, D. (2022). A Comprehensive Survey of Emergency Communication Network and Management. Wireless Personal Communications (124), 1375 – 1421. https://doi.org/10.1007/s11277-021-09411-1

de Mello, A. C. B. (2018). Levantamento de requisitos por meio da análise da atividade e da tarefa para sistemas digitais (Programa de Pós-graduação em Design, linha de pesquisa de Artefatos Digitais). Universidade Federal de Pernambuco (UFPE).

de Mello, A. C. B., & das Neves, A. M. M. (2018). Eliciting Requirements for Digital Systems Using Activity and Task Analysis. In I. A. for Development of the Information Society (IADIS) (Ed.), Multi conference on computer science and information systems (pp. 329 – 333). Madrid: IADIS Press.

de Molina, A. G., & Gomes, L. F. (2012). Criminologia (8th ed., Vol. 5). São Paulo: Revista dos Tribunais.

Deepak, G. C., Ladas, A., Sambo, Y. A., Pervaiz, H., Politis, C., & Imran, M. A. (2019). An Overview of Post-Disaster Emergency Communication Systems in the Future Networks. IEEE Wireless Communications, 26(6), 132 – 139. https://doi.org/10.1109/MWC.2019.1800467

Direção Geral do Património Cultural. (2011). Cadeia Penitenciária de Lisboa / Estabelecimento Prisional de Lisboa. http://www.monumentos.gov.pt/Site/APP_PagesUser/SIPA.aspx?id=7815

dos Santos, R. B. M., & Portugal, F. T. (2019). O panóptico e a economia visual moderna: do panoptismo ao paradigma panóptico na obra de Michel Foucault. Revista Psicologia Política, 19(44), 34– 49.

Doumi, T. L., Dolan, M. F., Tatesh, S., Casati, A., Tsirtsis, G., Anchan, K., & Flore, D. (2013). LTE for public safety networks. IEEE Communications Magazine, 51(2), 106 – 112. http://dx.doi.org/10.1109/MCOM.2013.6461193

Dresch, A., Lacerda, D. P., & Antunes Junior, J. A. V. (2015). Design Science Research: método de pesquisa para avanço da ciência e tecnologia. Porto Alegre: Bookman.

Du, H., Jin, T., Song, Y., Dai, Y., & Li, M. (2020). A Three-Dimensional Deep Learning Framework for Human Behavior Analysis Using Range-Doppler Time Points. IEEE Geoscience and Remote Sensing Letters, 17(4), 611 – 615. https://doi.org/10.1109/LGRS.2019.2930636

Ehrlich, I. (1973). Participation in Illegitimate Activities: A Theoretical and Empirical Investigation. Journal of Political Economy, 81(3), 521 – 565.

Electronic Communications Committee (ECC). (2013). ECC Report 199 (Technical Report). http://spectrum.welter.fr/international/cept/ecc-reports/ecc-report-199-PPDR-spectrum-requirements.pdf

Emergency Management Institute. (2023). National Incident Management System. https://training.fema.gov/nims/

Emergency Services Mobile Communications Programme (ESMCP). (2022). Emergency Services Network. https://www.gov.uk/government/publications/the-emergency-services-mobile-communications-programme/emergency-services-network

Engestrom, Y. (1987). Learning by Expanding: An Activity Theoretical Approach to Developmental Research. Helsinki: Orienta-Konsultit.

ESCAP. (2019). The Disaster Riskscape Across Asia-Pacific (Asia-Pacific Disaster Report 2019). https://www.unescap.org/publications/asia-pacific-disaster-report-2019

ETSI. (2010). ETSI TR 102 745 V1.1.1 (2009-10) (Technical Report (TR)). https://www.etsi.org/deliver/etsi_tr/102700_102799/102745/01.01.01_60/tr_102745v010101p.pdf

ETSI. (2011). ETSI TR 102 021-1 V1.3.1 (2011-07) (Technical Report (TR)). https://www.etsi.org/deliver/etsi_tr/102000_102099/10202101/01.03.01_60/tr_10202101v010301p.pdf

ETSI. (2012). ETSI TR 102 021-5 V1.2.1 (2010-12) (Technical Report (TR)). https://www.etsi.org/deliver/etsi_tr/102000_102099/10202105/01.02.01_60/tr_10202105v010201p.pdf

ETSI. (2014). ETSI TR 102 628 V1.2.1 (2014-09) (Technical Report (TR)). https://www.etsi.org/deliver/etsi_tr/102600_102699/102628/01.02.01_60/tr_102628v010201p.pdf

ETSI 3GPP. (2017). ETSI TS 136 213 V14.2.0 (2017-04) (s Technical Specification (TS)). https://www.etsi.org/deliver/etsi_ts/136200_136299/136213/14.02.00_60/ts_136213v140200p.pdf

ETSI 3rd Generation Partnership Project (3GPP). (2009). ETSI TR 136 942 V8.2.0 (2009-07) (Technical Report (TR)). https://www.etsi.org/deliver/etsi_tr/136900_136999/136942/08.02.00_60/tr_136942v080200p.pdf

ETSI 3rd Generation Partnership Project (3GPP). (2011). ETSI TS 136 106 V10.0.0 (2011-01) (Technical Specification (TS)). https://www.etsi.org/deliver/etsi_ts/136100_136199/136106/10.00.00_60/ts_136106v100000p.pdf

Etzkowitz, H., & Zhou, C. (2017). Hélice Tríplice: inovação e empreendedorismo universidade-indústria-governo. Estudos Avançados, 31(90), 23 – 48. https://doi.org/10.1590/s0103-40142017.3190003

EU4Digital. (2019). EU best practice report on releasing and reassignment of the 700 MHz band. https://eufordigital.eu/wp-content/uploads/2020/11/EU-best-practice-report-on-releasing-and-reassignment-of-the-700-MHz-band.pdf

European Commission. (2015). EUropean software defined radio for WireLEss in joint secuRity operations. https://cordis.europa.eu/project/id/218133/reporting/es

European Commission. (2017). Digital and Innovative Technologies for Security and Efficiency of First Responders operation. https://cordis.europa.eu/project/id/225404

European Commission. (2019). Aerial Base Stations with Opportunistic Links for Unexpected & Temporary Events. FP7 Project Absolute. https://cordis.europa.eu/project/id/318632

European Commission, Simon Forge, Robert Horvitz, & Colin Blackman. (2014). Is commercial cellular suitable for mission critical broadband? Publications Office. https://data.europa.eu/doi/10.2759/54788

European Telecommunications Standards Institute (ETSI). (2020). ETSI EN 300 392-5 V2.7.1 (2020-04).

https://www.etsi.org/deliver/etsi_en/300300_300399/30039205/02.07.01_60/en_30039205v020701p.pdf

European Union. (2016). Commission Implementing Decision (EU) 2016/687. Official Journal of the European Union. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016D0687&from=CS

European Union. (2015). Regulation (EU) 2015/2120. Official Journal of the European Union. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015R2120&rid=1

Exame. (2013). 2 milhões de pessoas vigiam a internet na China, diz jornal. https://exame.com/tecnologia/2-milhoes-de-pessoas-vigiam-a-internet-na-china-diz-jornal/

Fang, H., Lo, S., & Lo, J. T. Y. (2021). Building Fire Evacuation: An IoT-Aided Perspective in the 5G Era. Buildings, 11(643). https://doi.org/10.3390/buildings11120643

FASTER. (2023). First responder Advanced technologies for Safe and efficient Emergency Response. https://www.faster-project.eu/

Federal Communication Commission. (2018). 700 MHz Public Safety Broadband Spectrum — FirstNet. https://www.fcc.gov/700mhz-public-safety-broadband-spectrum-firstnet

Felemban, E., Rehman, F. U., Qamar, A. M., & Ahmed, A. (2020). A Framework to Extract Trip Informatics for Individuals and Groups Using Mobile Sensory Data in Mass Gathering Events. In 2020 ieee international conference on big data (big data) (pp. 5665 – 5667). Atlanta, USA: IEEE. https://doi.org/10.1109/BigData50022.2020.9378255

Ferrari, M. G., & Galeano, D. (2016). Polícia, antropometria e datiloscopia: história transnacional dos sistemas de identificação, do rio da Prata ao Brasil. História, Ciências, Saúde-Manguinhos, 23(n. Supl 1), 171 – 194. https://doi.org/10.1590/S0104-59702016000500010

Ferreira, M. V. G. (2015). Alocação de Blocos de Recursos em Redes LTE Utilizando Estimativa de Limitante de Retardo Através de Cálculo de Rede (Universidade Federal de Goiás, Escola de Engenharia Elétrica (EEEC) , Programa de Pós-graduação em Engenharia Elétrica e de Computação, Universidade Federal de Goiás).

Ferrus, R., Sallent, O., Baldini, G., & Goratti, L. (2013, out.). LTE: The Technology Driver for Future Public Safety Communications. IEEE Communications Magazine, 154 – 161.

FIRE-IN. (2023). EU-wide collaborative platform for First Responders, researchers and industries. https://www.fire-in.eu/

FirstNet. (2018). Wasatch Front Regional Communication Advisory Committee. https://wfrc.org/Committees/UCARAC/2018/04_Aug30/Utah_RAC_FirstNet_Presentation.pdf

FirstNet Authority. (2022). About the First Responder Network Authority. https://firstnet.gov/

Fonseca, R. N. (2022). Proposta de Fluxograma como subsídio a tomada de decisão para os Sistemas de Comunicação em Missão Crítica: Estudo aplicado em um órgão de Segurança Pública (Programa de Pós-graduação em Ciência da Informação). Universidade Federal de Santa Catarina.

Foucault, M. (2004). Vigiar e punir: o nascimento da prisão (29. ed.). Petrópolis: Vozes.

Freire, D. V. C. (2019). Proposta de Metodologia de Avaliação Tecnológica para Comunicações Críticas (Mestrado em Ciência da Informação, Universidade Federal de Santa Catarina (UFSC)). https://repositorio.ufsc.br/handle/123456789/206430

Freire, D. V. C., & Cândido, A. C. (2019). Technology Assessment as Support in the Decision-Making Process for Modernizing Critical Communication Technologies used By Public Safety Agencies in Brazil. In 4th European technology assessment. Bratislava. https://bratislava2019.technology-assessment.info/images/Preso/Preso-Freire.pdf

Freire, D. V. C., & Cândido, A. C. (2020). O Aspecto Informacional no Levantamento de Cenários para Comunicações Críticas em Segurança Pública no Brasil. Revista Conhecimento em Ação, 5(2), 76 – 97. https://doi.org/10.47681/rca.v5i2.34167

Gai, K., Qiu, M., & Zhao, H. (2016). Security-Aware Efficient Mass Distributed Storage Approach for Cloud Systems in Big Data. In 2016 ieee 2nd international conference on big data security on cloud (bigdatasecurity), ieee international conference on high performance and smart computing (hpsc), and ieee international conference on intelligent data and security (ids) (pp. 140 – 145). New York: IEEE. https://doi.org/10.1109/BigDataSecurity-HPSC-IDS.2016.68

Gai, K., Qiu, M., & Zhao, H. (2021, Oct.). Privacy-Preserving Data Encryption Strategy for Big Data in Mobile Cloud Computing. IEEE Transactions on Big Data, 7(4), 678 – 688. https://doi.org/10.1109/TBDATA.2017.2705807

Galton, F. (1892). Finger Prints. Dover Publications Inc.

Grasic, V., Kos, A., & Mileva-Boshkoska, B. (2018). Classification of incoming calls for the capital city of Slovenia smart city 112 public safety system using open Internet of Things data. International Journal of Distributed Sensor Networks, 14(9). https://doi.org/10.1177/1550147718801703

Grous, A. (2013). The socioeconomic value of mission critical mobile applications for public safety: 2x10MHz in 700MHz, preliminary research results: UK and EU. In Professional lte conference (Vol. 10). London.

Grunwald, A. (2009). Technology Assessment: Concepts and Methods, In Handbook of the Philosophy of Science, Philosophy of Technology and Engineering Sciences, 1st ed. North-Holland, pp. 1103 – 1146. https://doi.org/10.1016/B978-0-444-51667-1.50044-6

GSMA. (2018). Network 2020: Mission Critical Communications (Tech. Rep.). https://www.gsma.com/futurenetworks/wp-content/uploads/2017/02/767-Mission-critical-communications-low-res.pdf

Guedes, V. L. S., & Borschiver, S. (2005). Bibliometria: uma ferramenta estatística para a gestão da informação e do conhecimento, em sistemas de informação, de comunicação e de avaliação científica e tecnológica. In Encontro nacional de ciências da informação. Salvador.

Gulf Times. (2017, May 28). MoI Telecom Department feted by Airbus at CCW conference in Hong Kong. https://www.gulf-times.com/story/551364/moi-telecom-department-feted-by-airbus-at-ccw-conference-in-hong-kong

Guo, Y., Huang, Z., Guo, J., Li, H., Guo, X., & Nkeli, M. J. (2019). Bibliometric Analysis on Smart Cities Research. Sustainability, 11(13: 3606). https://doi.org/10.3390/su11133606

Hallio, J. et. al. (2019). Rapidly Deployable Network System for Critical Communications in Remote Locations. In 2019 ieee international symposium on broadband multimedia systems and broadcasting (bmsb) (pp. 1 – 5). Jeju, Korea (South): IEEE. https://doi.org/10.1109/BMSB47279.2019.8971954

Hardesty, L. (2022). AT&T exec says Band 14 spectrum makes FirstNet superior. https://www.fiercewireless.com/wireless/att-exec-says-band-14-spectrum-makes-firstnet-superior

Hassan, A., Hamza, R., Yan, H., & Li, P. (2019). An Efficient Outsourced Privacy Preserving Machine Learning Scheme With Public Verifiability. IEEE Access, 7, 146322 – 146330. https://doi.org/10.1109/ACCESS.2019.2946202

Hayajneh, A. M., Zaidi, S. A. R., Mclernon, D. C., di Renzo, M., & Ghogho, M. (2018). Performance Analysis of UAV Enabled Disaster Recovery Networks: A Stochastic Geometric Framework Based on Cluster Processes. Special Section on Networks of Unmanned Aerial Vehicles: Wireless Communications, Applications, Control And Modelling, 6, 26215 – 26230.

Heikkila, M. et al. (2022). Field trial with tactical bubbles for mission critical communications. Transactions on Emerging Telecommunications Technologies, 33(1:e4385). https://doi.org/10.1002/ett.4385

HEXAGON. (2022). Safe Cities Solutions. https://hexagon.com.br/synergy-solutions/safety-cities

Hill, K. (2019, March 28). Where is public safety LTE being explored around the world? on-line (RCR Wireless News). https://www.rcrwireless.com/20190328/network-infrastructure/where-is-public-safety-lte-being-explored-around-the-world

Hoyhtya, M. 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. https://doi.org/10.1109/ACCESS.2018.2883787

Hu, Y. C., Patel, M., Sabella, D., Sprecher, N., & Young, V. (2015). Mobile Edge Computing A key technology towards 5G (1st ed.). ETSI. https://www.etsi.org/images/files/etsiwhitepapers/etsi_wp11_mec_a_key_technology_towards_5g.pdf

Huawei. (2018). Huawei colabora com resgate de jovens presos em caverna na Tailândia. https://www.huawei.com/br/news/br/2018/julho/meninos%20da%20caverna

Huawei. (2023). eLTE Rapid Deployment Broadband Trunking System. https://e.huawei.com/ae/products/wireless/elte-trunking/rapid-deployment/elte-rapid

IBM. (2022). What is edge computing? https://www.ibm.com/cloud/what-is-edge-computing

IDB. (2017). The Welfare Costs of Crime in Latin America and the Caribbean (Tech. Rep.). Washington, D.C.. https://publications.iadb.org/handle/11319/8133

IEEE. (2018 / September 13th). The Prohibition-era Origins of the Police Radio. https://site.ieee.org/sb-uol/the-prohibition-era-origins-of-the-police-radio/

IN-PREP. (2023). Crossing New Frontiers in Disaster Preparedness. https://www.in-prep.eu/

Innocence Project. (2022). Innocence Project. https://innocenceproject.org/

Instituto de Antropologia, Universidade de Coimbra. (1985). Cem Anos de Antropologia em Coimbra. Coimbra: Instituto de Antropologia, Universidade de Coimbra. https://digitalis-dsp.uc.pt/bitstream/10316.2/39037/6/Cem%20anos%20de%20Antropologia%20em%20Coimbra.preview.pdf

International Telecommunication Union (ITU). (2017). Report ITU-R M.2410-0 (Tech. Rep.). https://www.itu.int/dms_pub/itu-r/opb/rep/R-REP-M.2410-2017-PDF-E.pdf

ITU. (2015). Recommendation ITU-R M.2083-0 (Recommendation ITU-R). https://www.itu.int/dms_pubrec/itu-r/rec/m/R-REC-M.2083-0-201509-I!!PDF-E.pdf

ITU. (2015, October). Focus Group on Smart Sustainable Cities (Technical Specifications and Reports). https://www.itu.int/en/ITU-T/focusgroups/ssc/Pages/default.aspx

ITU-R. (2003). REPORT ITU-R M.2033 (Technical Report). https://www.itu.int/net/ITU-R/terrestrial/res647/docs/M-2033.pdf

Jaffar, M., & Chuberre, N. (2021, October). NTN & Satellite in Rel-17 & 18. 3GPP Highlights newsletter, Standards for 5G(03), 24 – 24. https://www.3gpp.org/ftp/Information/Highlights/2021_Issue03/mobile/index.html#p=1

Jarwan, A., Sabbah, A., Ibnkahla, M., & Issa, O. (2019). LTE-based Public Safety Networks: A Survey. IEEE Communications Surveys & Tutorials, 21(2), 1165 – 1187. https://doi.org/10.1109/COMST.2019.2895658

Jilani, M. T., Rehman, M. Z. U., & Abbas, M. A. (2019). An Application Framework of Crowdsourcing based Emergency Events Reporting in Smart Cities. In 2019 international symposium on networks, computers and communications (isncc) (pp. 1 – 5). Istanbul, Turkey: IEEE. https://doi.org/10.1109/ISNCC.2019.8909146

Jonsson, H. et al. (2021). Differences between germline genomes of monozygotic twins. Nature Genetics(53), 27 – 34. https://doi.org/10.1038/s41588-020-00755-1

Jordan, P. W. (1998). An Introduction to Usability. London: Taylor & Francis.

Jorente, M. J. V., & da Costa Santos, P. L. V. A. (2009). Tecnologias, mídias, criação e hipertextualidade na transformação da informação em conhecimento interativo (Doctoral dissertation, Universidade Estadual Paulista (UNESP)). http://hdl.handle.net/11449/103362

JPS. (2023). Gateways to Communication. https://jps.com/products/communications-gateways/

Khan, A., Gupta, S., & Gupta, S. K. (2022). Emerging UAV technology for disaster detection, mitigation, response, and preparedness. Journal of Field Robotics, 39, 905 – 955. https://doi.org/10.1002/rob.22075

Kitsuse, J. I., & Cicourel, A. V. (1963). A Note on the Uses of Official Statistics. , 11(2), 131 – 139. https://doi.org/10.2307/799220

Kumbhar, A., & Guvenc, I. (2015). A Comparative Study of Land Mobile Radio and LTE-based Public Safety Communications. In IEEE (Ed.), Proceedings of the ieee southeastcon. Fort Lauderdale, Florida: IEEE.

Kunz, A., Nkenyereye, L., & Song, J. (2018). 5G Evolution of Cellular IoT for V2X. In 2018 ieee conference on standards for communications and networking (cscn) (pp. 1 – 6). Paris: IEEE. https://doi.org/10.1109/CSCN.2018.8581830

Kyakulumbye, S., Pather, S., & Bagula, A. (2020). Smart City Citizens' Service Provision using Participatory Design and Participatory Sensing: Lessons for Developing Cities. In M. Cunningham & P. Cunningham (Eds.), 2020 ist-africa conference (ist-africa) (pp. 1 – 12). Kampala, Uganda: IST-Africa.

Kyakulumbye, S., Pather, S., & Jantjies, M. (2019). Knowledge Creation in a Participatory Design Context: The use of Empathetic Participatory Design. The Electronic Journal of Knowledge Management, 17(1), 49 – 65.

Lair, Y., & Mayer, G. (2017). Mission Critical Services in 3GPP. https://www.3gpp.org/news-events/3gpp-news/1875-mc_services

Lee, J., Park, P., Chung, B., Kim, S., Nam, K., & Rhee, W. (2021). Call Model and Test-Verification Methods for PS-LTE Core Equipment. Electronics, 10(2513), 1 – 22. https://doi.org/10.3390/electronics10202513

Lee, S. K., Kwon, H. R., Cho, H., Kim, J., & Lee, D. (2016). International Case Studies of Smart Cities, Songdo, Republic of Korea. on-line. Inter-American Developed Bank.

Legros, C. (2017, December). CITIES A Marseille, le big data au service de la securite dans la ville. Le Monde. https://www.lemonde.fr/smart-cities/article/2017/12/08/a-marseille-le-big-data-au-service-de-la-securite-dans-la-ville_5226528_4811534.html

Levitt, S. D. (1998). The relationship between crime reporting and police: Implications for the use of Uniform Crime Reports. Journal of Quantitative Criminology, 14(1), 61 – 88.

Lewis, P., & Hilder, P. (2018, March 23). Leaked: Cambridge Analytica's blueprint for Trump victory. https://www.theguardian.com/uk-news/2018/mar/23/leaked-cambridge-analyticas-blueprint-for-trump-victory

Li, M., Chen, T., & Du, H. (2020). Human Behavior Recognition Using Range-Velocity-Time Points. IEEE Access, 8, 37914 – 37925. https://doi.org/10.1109/ACCESS.2020.2975676

Li, S., Xu, L. D., & Zhao, S. (2018). 5G Internet of Things: A survey. Journal of Industrial Information Integration, 10, 1 – 9. https://doi.org/10.1016/j.jii.2018.01.005

Li, T., Qiu, Z., Cao, L., Cheng, D., Wang, W., Shi, X., & Wang, Y. (2021). Privacy-Preserving Participant Grouping for Mobile Social Sensing Over Edge Clouds. IEEE Transactions on Network Science and Engineering, 8(2), 865 – 880. https://doi.org/10.1109/TNSE.2020.3020159

Li, Z., Song, Z., & Chen, X. (2020). Privacy-Preserving Cost Minimization in Mobile Crowd Sensing Supported by Edge Computing. IEEE Access, 8, 121920 – 121928. https://doi.org/10.1109/ACCESS.2020.3007168

Liu, C., Ding, M., Ma, C., Li, Q., Lin, Z., & Liang, Y. (2018). Performance Analysis for Practical UnmannedAerial Vehicle Networks with LoS/NLoSTransmissions. In 2018 ieee international conference on communications workshops (icc workshops) (pp. 1 – 6). Kansas City, MO, USA: IEEE. https://ieeexplore.ieee.org/document/8403635

Locke, J. (2022). What Is FirstNet Band 14? https://www.digi.com/blog/post/what-is-firstnet-band-14

Lombroso, C. (2013). O Homem Delinquente. Sao Paulo: Ícone — (Coleção Fundamentos de Direito).

Lopez-de-Teruel, P. E., Perez, M. G., Clemente, F. J. G., Garcia, A. R., & Perez, G. M. (2019). 5G-CAGE: A Context and Situational Awareness System for City Public Safety with Video Processing at a Virtualized Ecosystem. In IEEE (Ed.), 2019 ieee/cvf international conference on computer vision workshop (iccvw) (pp. 2749 – 2757). Seoul, South Korea. https://doi.org/10.1109/ICCVW.2019.00336

Lum, K., & Isaac, W. (2016). To predict and serve? Significance, 13(5), 14 – 19. https://doi.org/10.1111/j.1740-9713.2016.00960.x

Lwin, K. K., Sekimoto, Y., Takeuchi, W., & Zettsu, K. (2019). City Geospatial Dashboard: IoT and Big Data Analytics for Geospatial Solutions Provider in Disaster Management. In 2019 international conference on information and communication technologies for disaster management (ict-dm) (pp. 1 – 4). Paris: IEEE. https://doi.org/10.1109/ICT-DM47966.2019.9032921

Lyfo. (2023). Zero downtime mobile connectivity. https://lyfo.com/lyfo-net/

Lyon, D. (1994). The electronic eye. Minneapolis: University of Minnesota Press.

Lyon, D. (2018). The Culture of Surveillance (1st. ed.). Cambridge: Polity Press.

Lyra, C. A. (2009). PF testa sistema de rádio seguro em Fernando de Noronha. https://g1.globo.com/Noticias/Mundo/0,,MUL1181613-5602,00-PF+TESTA+SISTEMA+DE+RADIO+SEGURO+EM+FERNANDO+DE+NORONHA.html

Mannheim, K. (1972). Ideologia e Utopia. Rio de Janeiro: Zahar Editores.

Marabissi, D. et al. (2019). A Real Case of Implementation of the Future 5G City. Future Internet, 11(4). http://dx.doi.org/10.3390/fi11010004

Mariano, C. M. (2018). O Método Datiloscópico de Vulcetich e sua Importância na Prática Forense. Juiz de Fora: Universidade Federal de Juiz de Fora.

Marinescu, D. C. (2018). Chapter 12 — Big Data, Data Streaming, and the Mobile Cloud. In Cloud computing (2nd ed., pp. 439 – 487). Elsevier Inc. https://doi.org/10.1016/B978-0-12-812810-7.00016-9

Mathiesen, T. (1997). The Viewer Society: Michel Foucault's 'Panopticon' Revisited. Theoretical Criminology. https://doi.org/10.1177/1362480697001002003

Mayor's Press Office, City of Chicago. (2018). Mayor Emanuel Announces Expansion Of Smart Policing Strategy Supporting Nearly Two Years Of Consecutive Declines In Crime. 200 more License Plate Readers added to CPD fleet. https://www.chicago.gov/content/dam/city/depts/mayor/Press%20Room/Press%20Releases/2018/October/101018_ExpansionSmartPolicingStrategy.pdf

Mell, P., & Grance, T. (2011). The NIST Definition of Cloud Computing. https://csrc.nist.gov/publications/detail/sp/800-145/final

Mercy, M. S., Priya, C. G., & Merlin, R. B. (2018). Licensed Shared Access Technique for 5G Wireless Communication Systems: A Review. In 2nd international conference on trends in electronics and informatics (icoei 2018) (pp. 1158 – 1160). Tirunelveli, India: IEEE. https://doi.org/10.1109/ICOEI.2018.8553934

Messaoud, R. B., Sghaier, N., Moussa, M. A., & Ghamri-Doudane, Y. (2019). Privacy Preserving Utility-Aware Mechanism for Data Uploading Phase in Participatory Sensing. IEEE Transactions on Mobile Computing, 18(9), 2160 – 2173. https://doi.org/10.1109/TMC.2018.2869865

Mezzavilla, M. et al. (2018). Public Safety Communications above 6 GHz: Challenges and Opportunities. IEEE Access, 6, 316 – 329. https://doi.org/10.1109/ACCESS.2017.2762471

Ministere des Armee. (2022). 28e regiment de transmissions. https://www.defense.gouv.fr/terre/28e-regiment-transmissions

Mkhwanazi, K., Owolawi, P. A., Mapayi, T., & Aiyetoro, G. (2020). An automatic crime reporting and immediate response system. In 2020 international conference on artificial intelligence, big data, computing and data communication systems (icabcd) (pp. 1 – 6). Durban, South Africa. https://doi.org/10.1109/icABCD49160.2020.9183837

Mohammed, N. A., Mansoor, A. M., & Ahmad, R. B. (2019). Mission-Critical Machine-Type Communication: An Overview and Perspectives Towards 5G. IEEE Access, 7, 127198 – 127216. https://doi.org/10.1109/ACCESS.2019.2894263

Mohan, P., & Mittal, H. (2020). Review of ICT usage in disaster management. International Journal of Information Technology, 12, 955 – 962. https://doi.org/10.1007/s41870-020-00468-y

Mohler, G., & Brantingham, P. J. (2018). Privacy Preserving, Crowd Sourced Crime Hawkes Processes. In 2018 international workshop on social sensing (socialsens) (pp. 14 – 19). Orlando: IEEE. https://doi.org/10.1109/SocialSens.2018.00016

Motorola Solutions. (2017). LTE de Segurança Pública Sistemas Privados de Banda Larga de Alta Disponibilidade para Missão Crítica.

Motorola Solutions. (2017). Nordic Countries Expand Cross-Border TETRA Communication. https://www.motorolasolutions.com/newsroom/press-releases/nordic-countries-expand-cross-border-tetra-communication.html

Motorola Solutions. (2023). Solução para Interoperabilidade IP MOTOBRIDGE. https://www.motorolasolutions.com/pt_xl/solutions/municipalities/mission-critical-communications/motobridge-ip-interoperability-solution.html#taboverview

Mwanza, D. (2001). Where Theory meets Practice: A Case for an Activity Theory based Methodology to guide Computer System Design. In M. Hirose (Ed.), Proceedings of interact '2001: Eighth ifip tc 13 international conference on human-computer interaction. Tokyo, Japan: IOS Press Oxford, UK.

NBC News. (2018, April 09). Facebook to send Cambridge Analytica data-use notices to 87 million users Monday. https://www.nbcnews.com/tech/social-media/facebook-send-cambridge-analytica-data-use-notices-monday-n863811

Nokia. (2020). Sendai City deploys connected drones for disaster alert and rescue. https://www.youtube.com/watch?v=_VbET8XiN_I

Nokia. (2022). 5G for public safety: Driving first responders' operational excellence, White paper. https://pf.content.nokia.com/public-safety-government-mobile-broadband-critical-communications-spectrum-tcca-5g-small-cell/the-journey-to-5G-for-public-safety-white-paper-207037?_ga=2.48449829.286534465.1677422779-420559337.1649259178#page=1

O-RAN Alliance. (2022). O-RAN Alliance is Transforming Radio Access Networks towards Open, Intelligent, Virtualized and Fully Interoperable RAN. https://www.o-ran.org/

Okumura, Y., Suyama, S., & Mashino, J. (2018). 5G Field Trials in the Smart City and Medical Service Areas toward Social Implementation of 5G. NTT Technical Review, 16(10), 47 – 53.

oneM2M. (2022). oneM2M The IoT Standard. https://www.onem2m.org/

UN. (2015). Agenda 2030: objetivos do desenvolvimento sustentável. https://brasil.un.org/pt-br/sdgs/11

Orwell, G. (2009). 1984 (Vol. 1o). Sao Paulo: Companhia das Letras.

Othman, A., & Nayan, N. A. (2021). Public Safety Mobile Broadband System: From Shared Network to Logically Dedicated Approach Leveraging 5G Network Slicing. IEEE SYSTEMS JOURNAL, 15(2), 2109 – 2120.

Palestini, L. (2021). Communication and Decision Support Systems. International Journal of Safety and Security Engineering, 11(4), 397 – 407. https://doi.org/10.18280/ijsse.110413

Park, S. H., Park, Y. J., Jeon, Y. J., & Kang, S. J. (2022). Self-organized low-power multi-hop failover protocol for a cellular-based public safety device network. IEEE Internet of Things Journal, 9(19), 18238 – 18250. https://doi.org/10.1109/JIOT.2022.3156442

Peltola, M., & Hammainen, H. (2018). Effect of population density and network availability on deployment of broadband PPDR mobile network service. Digital Policy, Regulation and Governance, 20(1), 78 – 96. http://dx.doi.org/10.1108/DPRG-07-2017-0042

Pereira, C. L., Segre, L. M., & Nascimento, R. P. (2013). A ampliação das estruturas de controle por meio das tecnologias de informação e comunicação: a onipresença do "panóptico eletrônico" no setor bancário. Cadernos EBAPE.BR, 11(1), 65 – 84.

Perry, W. L., McInnis, B., Price, C. C., Smith, S. C., & Hollywood, J. S. (2013). Predictive Policing. RAND Corporation. https://doi.org/10.7249/RR233

Pinto, A. E. M. (2012). Os efeitos da cidade digital (Pós-graduação em Direito. Área de concentração: Transformações do Direito Privado, Cidade e Sociedade., Universidade do Estado do Rio de Janeiro).

Powell, C. (2014). Technical Analysis (White Paper). https://www.rfsworld.com/userfiles/white_papers/2014/Ooredoo_White%20Paper_Mar14.pdf

Project HELP Consortium. (2011). Project HELP — Enhanced Communications in Emergencies by Creating and Exploiting Synergies in Composite Radio Systems. https://fp7-sec-help.upc.edu/index.html

Public Safety Communication Europe. (2020). H2020 BroadWay PCP Project. https://www.youtube.com/watch?v=IwbTs4Gq_yA

Punyakumpol, P. (2011). The Great Firewall of China: Background. https://cs.stanford.edu/people/eroberts/cs181/projects/2010-11/FreedomOfInformationChina/category/great-firewall-of-china/index.html

Qadir, Z., Ullah, F., Munawar, H. S., & Al-Turjman, F. (2021). Addressing disasters in smart cities through UAVs path planning and 5G communications: A systematic review. Computer Communications, 168, 114 – 135. https://doi.org/10.1016/j.comcom.2021.01.003

Raines, R. R. (2005). Signal Corps. WASHINGTON, D.C: Center of Military History United States Army. https://history.army.mil/html/books/060/60-15-1/CMH_Pub_60-15-1.pdf

Rao, S. K., & Prasad, R. (2018). Impact of 5G Technologies on Smart City Implementation. Wireless Personal Communication (100), 161 – 176. https://doi.org/10.1007/s11277-018-5618-4

Rathore, M. M. U. et. al. (2015). Real-Time Big Data Analytical Architecture for Remote Sensing Application. IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing, vol. 8(no 10), 4610 – 4621. https://doi.org/10.1109/JSTARS.2015.2424683

Regimento de Transmissões do Exército Português. (2021). Revista A Mensagem: Boletim Informativo do Regimento de transmissões. https://assets.exercito.pt/SiteAssets/RTm/5.%20Documentos/Revista%20Mensagem%202021.pdf

Rodota, S. (2008). A Vida na Sociedade da Vigilância (1st ed.). Renovar. Royal Corps of Signals. (2020). Royal Corps of Signals. https://www.army.mod.uk/who-we-are/corps-regiments-and-units/royal-corps-of-signals/

Saaf, S., Hosek, J., & Kolackova, A. (2020). Cellular-enabled Wearables in Public Safety Networks: State of the Art and Performance Evaluation. In 12th international congress on ultra modern telecommunications and control systems and workshops (icumt) (pp. 201 – 207). Brno, Czech Republic: IEEE. https://doi.org/10.1109/ICUMT51630.2020.9222459

Saaf, S., Hosek, J., & Kolackova, A. (2021). Enabling Next-Generation Public Safety Operations with Mission-Critical Networks and Wearable Applications. Sensors, 21(17:5790), 1 – 16. https://doi.org/10.3390/s21175790

Samsung. (2020, December). Massive MIMO for New Radio (Technical White Paper). https://images.samsung.com/is/content/samsung/p5/global/business/networks/insights/

white-papers/1208_massive-mimo-for-new-radio/MassiveMIMOforNRTechnicalWhitePaper-v1.2.0.pdf

Sanchoyerto, A., Solozabal, R., Blanco, B., & Liberal, F. (2019). Analysis of the Impact of the Evolution Toward 5G Architectures on Mission Critical Push-to-Talk Services. IEEE Access, 7, 115052 – 115061. https://doi.org/10.1109/ACCESS.2019.2930936

Santos, G. D. (2005). A Escola de Antropologia de Coimbra, 1885-1950 (1st ed.). Lisboa: ICS — Imprensa de Ciências Sociais.

Secretaria de Assuntos Estratégicos da Presidência da República do Brasil. (2018). Relatório de Conjuntura no 4 – Os custos Econômicos da Criminalidade no Brasil (Relatório de Conjuntura no 4). Brasília -DF. http://www.secretariageral.gov.br/estrutura/secretaria_de_assuntos_estrategicos/publicacoes-e-analise/relatorios-de-conjuntura/custos_economicos_criminalidade_brasil.pdf

Selim, M. Y., & Kamal, A. E. (2018). Post-Disaster 4G/5G Network Rehabilitation Using Drones: Solving Battery and Backhaul Issues. In 2018 ieee globecom workshops (gc wkshps). Abu Dhabi, United Arab Emirates: IEEE. https://doi.org/10.1109/GLOCOMW.2018.8644135

Sellin, T., & Wolfgang, M. E. (1964). The measurement of delinquency. John Wiley & Sons.

Sharp, I. (2018). Delivering Public Safety Communications with LTE (3GPP). https://www.3gpp.org/IMG/pdf/121218_lte_for_public_safety_rev3_-_cl.pdf

Shibata, K., & Yamamoto, H. (2019). People Crowd Density Estimation System using Deep Learning for Radio Wave Sensing of Cellular Communication. In 2019 international conference on artificial intelligence in information and communication (icaiic) (pp. 143 – 148). Okinawa, Japan: IEEE. https://doi.org/10.1109/ICAIIC.2019.8669071

Shih, T., Chen, C., Syu, B., & Deng, Y. (2019). A Cloud-Based Crime Reporting System with Identity Protection. Symmetry, 11(2: 255), 1 – 29. https://doi.org/10.3390/sym11020255

Sicari, S., Rizzardi, A., & Coen-Porisini, A. (2020). 5G In the internet of things era: An overview on security and privacy challenges. Computer Networks, 179. https://doi.org/10.1016/j.comnet.2020.107345

SIRESP, S.A. (2023). SIRESP — O futuro. https://www.siresp.pt/rede-siresp/siresp-o-futuro/

Snowden, E. J. (2019). Eterna Vigilância. São Paulo: Planeta do Brasil.

Song, H., Srinivasan, R., Sookoor, T., & Jeschke, S. (2017). Mobile Crowd-Sensing for Smart Cities. In Smart cities: Foundations, principles, and applications (pp. 125 – 154). Wiley Telecom. https://doi.org/10.1002/9781119226444.ch5

Sousa, P. L., Rodrigues, A., & Catarino, H. (2020). 5G-NR Network Planning: Impact of Massive MIMO and Beamforming in Coverage Predictions. https://fenix.tecnico.ulisboa.pt/downloadFile/844820067126457/extended_abstract_pedrosousa_final.pdf

Stigler, G. (1970). The Optimum Enforcement of Laws. Journal of Political Economy, 78(3), 526 – 536.

Streamwide. (2022, Nov 03). The Airbus-led consortium including Streamwide has successfully completed the second scenario of the BroadWay project. https://www.streamwide.com/wp-content/uploads/2022/11/PR-SW-SA-_-EUROPEAN-BROADWAY-PROJECT.pdf

Sublime, J., & Kalinicheva, E. (2019). Automatic Post-Disaster Damage Mapping UsingDeep-Learning Techniques for Change Detection: Case Study of the Tohoku Tsunami. Remote Sensing, 11(1123). https://doi.org/10.3390/rs11091123

Suomalainen, J., Julku, J., Vehkapera, M., & Posti, H. (2021). Securing Public Safety Communications on Commercial and Tactical 5G Networks: A Survey and Future Research Directions. IEEE Open Journal of the Communications Society, 2, 1590 – 1615. https://doi.org/10.1109/OJCOMS.2021.3093529

Swedish Civil Contingencies Agency (MSB). (2014). A Quick Guide to the Norwegian-Swedish ISI project: A cross-border development scheme. https://www.msb.se/siteassets/dokument/publikationer/english-publications/a-quick-guide-to-the-norwegian-swedish-isi-project-a-cross-border-development-scheme.pdf

Swedish Civil Contingencies Agency (MSB). (2020). Three country cross-border collaboration with ISI-FINOSE talk groups: Appendix to FISE, FINO and NOSE guidelines. https://www.nodnett.no/siteassets/bibliotek/brukerveiledninger/guidelines-finose-eng.pdf

Taleb, T., Dutta, S., Ksentini, A., Iqbal, M., & Flinck, H. (2017). Mobile Edge Computing Potential in Making Cities Smarter. IEEE Communications Magazine, 55(3), 38 – 43. https://doi.org/10.1109/MCOM.2017.1600249CM

TCCA. (2019). TCCA White Paper (TCCA White Paper). Newcastle. https://tcca.info/documents/january-2019-ppdr-broadband-roadmap.pdf/

TCCA, & ACCF. (2020). The impact of 3GPP critical broadband on the critical LMR industry (White Paper issued by ACCF and TCCA). https://criticalcommsforum.com.au/wp-content/uploads/2020/06/The-Impact-of-3GGP-Critical-Broadband-on-the-LMR-Industry-June2020.pdf

Techplayon. (2019). MORAN vs MOCN. https://www.techplayon.com/5g-network-sharing-concept-benefits-and-architectures/moran-vs-mocn/

Telecommunications Industry Association (TIA). (2002). Compendium of Emergency Communications and Communications Network Security-related Work Activities within the Telecommunications Industry Association (TIA). https://web.archive.org/web/20111216004655/http://tiaonline.org/standards/technology/ciphs/documents/EMTEL_sec.pdf

Telstra. (2022). Telstra LANES Emergency service. https://www.telstra.com.au/business-enterprise/industries/public-safety/lanes-emergency

TETRA Critical Communications Today. (2017). (36).

TETRAPOL forum. (2022). TETRAPOL forum. https://www.tetrapol.com/

The FirstNet Authority. (2023a). APP Catalog. https://apps.firstnet.att.com/?auth=false

The FirstNet Authority. (2023b). Featured Apps from the App Catalog. https://www.firstnet.com/apps/featured-apps.html

The FirstNet Authority. (2023c). The FirstNet Core. https://www.firstnet.gov/network/TT/firstnet-core

The National Commission on Terrorist Attacks Upon the United States (9-11 Commission). (2004/July 22). The 911 Commission Report (Tech. Rep.). Wasgington, D.C. https://www.911commission.gov/report/911Report.pdf

The Punjab Safe Cities Authority (PSCA). (2022). Safe Cities Projects. https://psca.gop.pk/

Thiruvasagam, P. K., & Chakraborty, A. (2021). Resilient and Latency-aware Orchestration of Network Slices Using Multi-connectivity in MEC-enabled 5G Networks. IEEE Transactions on Network and Service Management, 18, 2502 – 2514.

Top Optimized Technologies. (2018). Estudio sobre los requisitos técnicos que permitan caracterizar la cobertura con tecnología LTE necesaria para proporcionar determinados servicios de datos (Estudio de requisitos técnicos que permitan caracterizar la cobertura con tecnología LTE). Madrid. https://www.academia.edu/35997066/Estudio_de_requisitos_t%C3%A9cnicos_que_permitan_caracterizar_la_cobertura_con_tecnolog%C3%ADa_LTE

Toure, I. (2017). Real Time Big Data Analytics for Predicting Terrorist Incidents (Doctor of Philosophy). University of Maryland, Baltimore County. ISBN: 978-0-3552-3792-4.

Tran, T. A., & Daim, T. (2008). A taxonomic review of methods and tools applied in technology assessment. Technological Forecasting & Social Change, 75(9), 1396 – 1405. https://doi.org/10.1016/j.techfore.2008.04.004

Treguer, F. (2019, May). Safe city, ou o governo dos algoritmos. Le Monde Diplomatique (143). https://diplomatique.org.br/safe-city-ou-o-governo-dos-algoritmos/

Ulema, M. (2019). Fundamentals of Public Safety Networks and Critical Communications Systems (First Edition ed.). New Jersey: IEEE Press, John Wiley & Sons, Inc.

United States. (2010). United States Code, 2006 Edition, Supplement 4, Title 6 — DOMESTIC SECURITY. Chapter 1 — Homeland Security Organization. § 194. Enhancement of public safety communications interoperability, 101–1405. https://www.govinfo.gov/content/pkg/USCODE-2010-title6/pdf/USCODE-2010-title6.pdf

U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency. (2020). SAFECOM Guidance on Emergency Communications Grants (Tech. Rep.). https://www.cisa.gov/sites/default/files/publications/fy_2020_safecom_guidance_on_emergency_communications_grants_final.pdf

Versteeg, T., Baumann, M., Weil, M., & Moniz, A. (2017). Exploring emerging battery technology for grid-connected energy storage with Constructive Technology Assessment. Technological Forecasting & Social Change, 115, 99 – 110. https://doi.org/10.1016/j.techfore.2016.09.024

Violos, J., Violos, J., Berdelis, A., Tsanakas, S., Tserpes, K., & Varvarigou, T. (2019). Predicting Visitor Distribution for Large Events in Smart Cities. In 2019 ieee international conference on big data and smart computing (bigcomp) (pp. 1 – 8). Kyoto, Japan. https://doi.org/10.1109/BIGCOMP.2019.8679181

Volk, M., & Sterle, J. (2021). 5G Experimentation for Public Safety: Technologies, Facilities and Use Cases. IEEE Access, 9, 41184 – 41217. https://doi.org/10.1109/ACCESS.2021.3064405

Vucetich, J. (1895). Instrucciones generales para el sistema de filiación "Provincia de Buenos Aires". La Plata: Imprenta de la Policía de la Provincia de Buenos Aires.

Wang, H. (2022). Research on key technologies of mobile crowd sensing for privacy preserving. In 2022 3rd international conference on computing, networks and internet of things (cniot) (pp. 23 – 27). Qingdao, China: IEEE. https://doi.org/10.1109/CNIOT55862.2022.00013

Wang, J., Chen, Y., Hao, S., Peng, X., & Hu, L. (2019). Deep learning for sensor-based activity recognition: A survey. Pattern Recognition Letters, 119, 3 – 11. https://doi.org/10.1016/j.patrec.2018.02.010

Wang, J., Cheng, W., & Zhang, H. (2020). Caching and D2D Assisted Wireless Emergency Communications Networks with Statistical QoS Provisioning. Journal of Communications and Information Networks, 5(3).

Wang, Q., Liu, H., Gao, K., & Zhang, L. (2019). Improved Multi-Agent Reinforcement Learning for Path Planning-Based Crowd Simulation. IEEE Access, 7, 73841 – 73855. https://doi.org/10.1109/ACCESS.2019.2920913

Wang, S., & Li, M. (2021). Research on public safety emergency management of "Smart city". In 2021 2nd international conference on computer science and management technology (iccsmt) (pp. 169 – 172). Shanghai, China: IEEE. https://doi.org/10.1109/ICCSMT54525.2021.00041

Wei, G., & Sheng, Z. (2019). Image quality assessment for intelligent emergency application based on deep neural network. Journal of Visual Communication and Image Representation, 63(102581). https://doi.org/10.1016/j.jvcir.2019.102581

Wellford, C. F., & Wiatrowksi, M. (1975). On the Measurement of Delinquency. The Journal of Criminal Law and Criminology, 66(2). https://doi.org/10.2307/1142781

Wu, C. K., Tsang, K. F., Liu, Y., Zhu, H., Wang, H., & Wei, Y. (2020). Critical Internet of Things: An Interworking Solution to Improve Service Reliability. IEEE Communications Magazine, 58(1), 74 – 79. https://doi.org/10.1109/MCOM.001.1900526

Wu, Q., & Yu, X. (2020). Research on Public Safety Management under the Application of Big Data and Internet of Things. In 2020 international conference on big data economy and information management (bdeim) (pp. 9 – 12). Zhengzhou, China: IEEE. https://doi.org/10.1109/BDEIM52318.2020.00010

Wu, S., & Mastronarde, N. (2018). Improving the Coverage and Spectral Efficiency of Millimeter-Wave Cellular Networks using Device-to-Device Relays. IEEE Transactions on Communications, 66(5), 2251 – 2265.

Xie, J., & Yang, T. (2018). Using Social Media Data to Enhance Disaster Response and Community Service. In 2018 international workshop on big geospatial data and data science (bgdds) (pp. 1 – 4). Thoothukudi, India: IEEE. https://doi.org/10.1109/BGDDS.2018.8626839

Xu, G., Li, H., Dai, Y., Yang, K., & Lin, X. (2019). Enabling Efficient and Geometric Range Query with Access Control Over Encrypted Spatial Data. IEEE Transactions on Information Forensics and Security, 14(4), 870 – 885. https://doi.org/10.1109/TIFS.2018.2868162

Xu, Z., Liu, Y., Yen, N. Y., Mei, L., Luo, X., of Technology, X. W. S. I., & Hu, C. (2016). Crowdsourcing Based Description of Urban Emergency Events Using Social Media Big Data. IEEE Transactions on Cloud Computing, 8(2), 387 – 397. https://doi.org/10.1109/TCC.2016.2517638

Yang, C., Liang, P., Fu, L., Cui, G., Huang, F., Teng, F., & Bangash, Y. A. (2022). Using 5G in smart cities: A systematic mapping study. Intelligent Systems with Applications (200065). https://doi.org/10.1016/j.iswa.2022.200065

Yang, G., Shi, X., Feng, L., He, S., Shi, Z., & Chen, J. (2020). A Cost-Effective Crowdsensing System for Detecting and Localizing Drones. IEEE Transactions on Mobile Computing, 19(9), 2208 – 2043. https://doi.org/10.1109/TMC.2019.2921962

Yang, P., Xiong, N., & Ren, J. (2020). Data Security and Privacy Protection for Cloud Storage: A Survey. IEEE Access, 8, 131723 – 131740. https://doi.org/10.1109/ACCESS.2020.3009876

Yang, Y., Hou, C., Lang, Y., Guan, D., Huang, D., & Xu, J. (2019). Open-set human activity recognition based on micro-Doppler signatures. Pattern Recognition, 85, 60 – 69. https://doi.org/10.1016/j.patcog.2018.07.030

Yetis, Y., Sara, R. G., Erol, B. A., Kaplan, H., Akuzum, A., & Jamshidi, M. (2016). Application of Big Data Analytics via Cloud Computing. In 2016 world automation congress (wac) (pp. 1 – 5). Rio Grande, PR, USA. https://doi.org/10.1109/WAC.2016.7582986

Yim, J., Bang, J., Kim, S., Jeong, S., & Lee, Y. (2017). UAV Planning to Optimize Efficiency of Image Stitching in Disaster Monitoring Using Smart-Eye Platform. In 2017 international conference on platform technology and service (platcon) (pp. 1 – 4). Busan, South Korea: IEEE. https://ieeexplore.ieee.org/document/7883734

Yu, X., & Wu, Q. (2020). Multi-source Heterogeneous Data Association Technology to Build Public Safety Big Data Integration Research. In 2020 international conference on big data economy and information management (bdeim) (pp. 17 – 20). https://doi.org/10.1109/BDEIM52318.2020.00012

Yy,W., Xu, H., Nguyen, J., Blasch, E., Hematian, A., & Gao,W. (2018). Survey of Public Safety Communications: User-Side and Network-Side Solutions and Future Directions. Special Section on Emerging Technologies for Device to Device Communications, 6(18), 70397 – 70425. https://ieeexplore.ieee.org/document/8523665

Zahid, J. I., Hussain, F., & Ferworn, A. (2019). A Model of Computing and Communication for Public Safety Integrating FirstNet, Edge Computing, and Internet of Things. In 2019 ieee 10th annual information technology, electronics and mobile communication conference (iemcon) (pp. 0619 – 0623). https://doi.org/10.1109/IEMCON.2019.8936153

Zanine, G., de S. Pinto, M. D., & Filippim, E. S. (2012). Analise bibliométrica aplicada a gestão do conhecimento. Conhecimento Interativo, 6(2), 124 – 140.

Zeydan, E., Ba, stug, E., Bennis, M., Kader, M. A., Karatepe, I. A., Er, A. S., & Debbah, M. (2016). Big Data Caching for Networking: Moving from Cloud to Edge. IEEE Communications Magazine, 54(9), 36 – 42. https://doi.org/10.1109/MCOM.2016.7565185

Zhang, X., Yang, Z., Sun, W., Liu, Y., Tang, S., Xing, K., & Mao, X. (2016). Incentives for Mobile Crowd Sensing: A Survey. IEEE Communications Surveys & Tutorials, 18(1), 54 – 67.

Zhang, X., Zhao, J., Xu, C., Li, H., Wang, H., & Zhang, Y. (2021). CIPPPA: Conditional Identity Privacy-Preserving Public Auditing for Cloud-Based WBANs Against Malicious Auditors. IEEE Transactions on Cloud Computing, 9(4), 1362 – 1375.

Zhou, I. et al. (2021). Internet of Things 2.0: Concepts, Applications, and Future Directions. IEEE Access, 9, 70961 – 71012. https://doi.org/10.1109/ACCESS.2021.3078549

Zhou, J., Mi, B., Huang, D., Liu, Y., Li, Y., & Weng, Y. (2021). Privacy-preserving Machine Learning Based on Homomorphic Conjugate Search Problem. In 2021 caa symposium on fault detection, supervision, and safety for technical processes (safeprocess) (pp. 1 – 6). Chengdu, China. https://doi.org/10.1109/SAFEPROCESS52771.2021.9693640

Zhou, J., Zhou, C., Kang, Y., & Tu, S. (2021). Integrated satellite-ground post-disaster emergency communication networking technology. Natural Hazards Research, 1(1), 4 – 10. https://doi.org/10.1016/j.nhres.2020.12.002

Zhou, X., Durrani, S., & Guo, J. (2020). Drone-Initiated D2D-Aided Multihop Multicast Networks for Emergency Information Dissemination. IEEE Access, 8, 3566 – 3578. https://ieeexplore.ieee.org/document/8943207/

Zins, C. (2006). Redefining information science: from "information science" to "knowledge science". Journal of Documentation, 62(4), 447 – 461. http://dx.doi.org/10.1108/00220410610673846

Zins, C. (2007). Conceptions of information science. JASIST, 58(3), 335 – 350.

A

Appendix: –Systematic Literature Review results

Nº String	String	Nº of Occurrences SCOPUS	Nº of Occurrences Web of Science	Nº of Occurences IEEE	SCOPUS Selection	Web of Science Selection	IEEE Selection
1	(("Public Safety" OR "PPDR" OR "Public Protection and Disaster Relief") AND ("5G mobile communication" OR "5G"))	1774	139	121			
2	(("Public Safety" OR "PPDR" OR "Public Protection and Disaster Relief") AND ("Technology Assessment" OR "Technological Assessment"))	214	3	2			
3	(("Public Safety" OR "PPDR" OR "Public Protection and Disaster Relief") AND ("LTE" OR "Long Term Evolution" OR "Long-Term Evolution" OR "4G"))	1416	108	106			
4	(("Public Safety" OR "PPDR" OR "Public Protection and Disaster Relief") AND ("Mission Critical Communication" OR "MCC"))	92	4	7			
5	(("Public Safety" OR "PPDR" OR "Public Protection and Disaster Relief") AND ("Smart City" OR "Safe City" OR "Smart Cities" OR "Safe Cities" OR "City Safety"))	1701	145	107			
6	(("5G mobile communication" OR "5G") AND ("technology assessment" OR "technological assessment"))	167	4	4			
7	(("5G mobile communication" OR "5G") AND ("LTE" OR "Long Term Evolution" OR "Long-Term Evolution" OR "4G"))	30468	3865	3474			
8	(("5G mobile communication" OR "5G") AND ("Mission Critical Communication" OR "MCC"))	572	41	22			
9	(("5G mobile communication" OR "5G") AND ("Smart City" OR "Safe City" OR "Smart Cities" OR "Safe Cities" OR "City Safety"))	11772	747	553			
10	(("technology assessment" OR "technological assessment") AND ("LTE" OR "Long Term Evolution" OR "Long-Term Evolution" OR "4G"))	133	1	1			
11	(("technology assessment" OR "technological assessment") AND ("Mission Critical Communication" OR "MCC"))	133	0	0			
12	(("technology assessment" OR "technological assessment") AND ("Smart City" OR "Safe City" OR "Smart Cities" OR "Safe Cities" OR "City Safety"))	408	2	0			
13	(("LTE" OR "Long Term Evolution" OR "Long-Term Evolution" OR "4G") AND ("Mission Critical Communication" OR "MCC"))	320	11	11			
14	(("LTE" OR "Long Term Evolution" OR "Long-Term Evolution" OR "4G") AND ("Smart City" OR "Safe City" OR "Smart Cities" OR "Safe Cities" OR "City Safety"))	4399	157	142			
15	(("Mission Critical Communication" OR "MCC") AND ("Smart City" OR "Safe City" OR "Smart Cities" OR "Safe Cities" OR "City Safety"))	421	20	24			
16	(("Public Safety" OR "PPDR" OR "Public Protection and Disaster Relief") AND ("5G mobile communication" OR "5G") AND ("technology assessment" OR "technological assessment"))	9	0	0	5	0	0
17	(("Public Safety" OR "PPDR" OR "Public Protection and Disaster Relief") AND ("5G mobile communication" OR "5G") AND ("LTE" OR "Long Term Evolution" OR "Long-Term Evolution" OR "4G"))	965	36	47	21	23	35
18	(("Public Safety" OR "PPDR" OR "Public Protection and Disaster Relief") AND ("5G mobile communication" OR "5G") AND ("Mission Critical Communication" OR "MCC"))	47	1	2	7	1	2
19	(("Public Safety" OR "PPDR" OR "Public Protection and Disaster Relief") AND ("5G mobile communication" OR "5G") AND ("Smart City" OR "Safe City" OR "Smart Cities" OR "Safe Cities" OR "City Safety"))	494	14	11	6	7	4
20	(("Public Safety" OR "PPDR" OR "Public Protection and Disaster Relief") AND ("technology assessment" OR "technological assessment") AND ("LTE" OR "Long Term Evolution" OR "Long-Term Evolution" OR "4G"))	7	0	0	3	0	0
21	(("Public Safety" OR "PPDR" OR "Public Protection and Disaster Relief") AND ("technology assessment" OR "technological assessment") AND ("Mission Critical Communication" OR "MCC"))	2	0	0	0	0	0
22	(("Public Safety" OR "PPDR" OR "Public Protection and Disaster Relief") AND ("technology assessment" OR "technological assessment") AND ("Smart City" OR "Safe City" OR "Smart Cities" OR "Safe Cities" OR "City Safety"))	8	0	0	4	0	0
23	(("Public Safety" OR "PPDR" OR "Public Protection and Disaster Relief") AND ("LTE" OR "Long Term Evolution" OR "Long-Term Evolution" OR "4G") AND ("Mission Critical Communication" OR "MCC"))	45	0	1	5	0	1
24	(("Public Safety" OR "PPDR" OR "Public Protection and Disaster Relief") AND ("LTE" OR "Long Term Evolution" OR "Long-Term Evolution" OR "4G") AND ("Smart City" OR "Safe City" OR "Smart Cities" OR "Safe Cities" OR "City Safety"))	274	4	4	3	4	2
25	(("Public Safety" OR "PPDR" OR "Public Protection and Disaster Relief") AND ("Mission Critical Communication" OR "MCC") AND ("Smart City" OR "Safe City" OR "Smart Cities" OR "Safe Cities" OR "City Safety"))	12	0	0	6	0	0
26	(("5G mobile communication" OR "5G") AND ("technology assessment" OR "technological assessment") AND ("LTE" OR "Long Term Evolution" OR "Long-Term Evolution" OR "4G"))	39	0	1	2	0	0
27	(("5G mobile communication" OR "5G") AND ("technology assessment" OR "technological assessment") AND ("Mission Critical Communication" OR "MCC"))	3	0	0	0	0	0

Figure 62 - Strings 1 to 27

Nº String	String	Nº of Occurrences SCOPUS	Nº of Occurrences Web of Science	Nº of Occurrences IEEE	SCOPUS Selection	Web of Science Selection	IEEE Selection
28	(("5G mobile communication" OR "5G") AND ("technology assessment" OR "technological assessment") AND ("Smart City" OR "Safe City" OR "Smart Cities" OR "Safe Cities" OR "City Safety"))	46	0	0	5	0	0
29	(("technology assessment" OR "technological assessment") AND ("LTE" OR "Long Term Evolution" OR "Long-Term Evolution" OR "4G") AND ("Mission Critical Communication" OR "MCC"))	2	0	0	0	0	0
30	(("technology assessment" OR "technological assessment") AND ("LTE" OR "Long Term Evolution" OR "Long-Term Evolution" OR "4G") AND ("Smart City" OR "Safe City" OR "Smart Cities" OR "Safe Cities" OR "City Safety"))	18	0	0	0	0	0
31	(("LTE" OR "Long Term Evolution" OR "Long-Term Evolution" OR "4G") AND ("Mission Critical Communication" OR "MCC") AND ("Smart City" OR "Safe City" OR "Smart Cities" OR "Safe Cities" OR "City Safety"))	57	1	1	3	0	0
32	(("Mission Critical Communication" OR "MCC") AND ("Smart City" OR "Safe City" OR "Smart Cities" OR "Safe Cities" OR "City Safety") AND ("5G mobile communication" OR "5G"))	158	1	1	6	0	0
33	(("Mission Critical Communication" OR "MCC") AND ("Smart City" OR "Safe City" OR "Smart Cities" OR "Safe Cities" OR "City Safety") AND ("technology assessment" OR" technological assessment"))	5	0	0	0	0	0
34	(("Mission Critical Communication" OR "MCC") AND ("5G mobile communication" OR "5G") AND ("LTE" OR "Long Term Evolution" OR "Long-Term Evolution" OR "4G"))	195	7	6	38	3	3
35	(("Smart City" OR "Safe City" OR "Smart Cities" OR "Safe Cities" OR "City Safety") AND ("LTE" OR "Long Term Evolution" OR "Long-Term Evolution" OR "4G") AND ("5G mobile communication" OR "5G"))	2859	73	67	4	9	8
36	(("Public Safety" OR "PPDR" OR "Public Protection and Disaster Relief") AND ("5G mobile communication" OR "5G") AND ("technology assessment OR technological assessment") AND ("LTE" OR "Long Term Evolution" OR "Long-Term Evolution" OR "4G"))	0	0	0	0	0	0
37	(("Public Safety" OR "PPDR" OR "Public Protection and Disaster Relief") AND ("5G mobile communication" OR "5G") AND ("technology assessment" OR "technological assessment") AND ("Mission Critical Communication" OR "MCC"))	0	0	0	0	0	0
38	(("Public Safety" OR "PPDR" OR "Public Protection and Disaster Relief") AND ("5G mobile communication" OR "5G") AND ("technology assessment" OR "technological assessment") AND ("Smart City" OR "Safe City" OR "Smart Cities" OR "Safe Cities" OR "City Safety"))	3	0	0	2	0	0
39	(("5G mobile communication" OR "5G") AND ("technology assessment" OR "technological assessment") AND ("LTE" OR "Long Term Evolution" OR "Long-Term Evolution" OR "4G") AND ("Mission Critical Communication" OR "MCC"))	2	0	0	0	0	0
40	(("5G mobile communication" OR "5G") AND ("technology assessment" OR "technological assessment") AND ("LTE" OR "Long Term Evolution" OR "Long-Term Evolution" OR "4G") AND ("Smart City" OR "Safe City" OR "Smart Cities" OR "Safe Cities" OR "City Safety"))	14	0	0	3	0	0
41	(("technology assessment" OR "technological assessment") AND ("LTE" OR "Long Term Evolution" OR "Long-Term Evolution" OR "4G") AND ("Mission Critical Communication" OR "MCC") AND ("Smart City" OR "Safe City" OR "Smart Cities" OR "Safe Cities" OR "City Safety"))	2	0	0	0	0	0
42	(("LTE" OR "Long Term Evolution" OR "Long-Term Evolution" OR "4G") AND ("Mission Critical Communication" OR "MCC") AND ("Smart City" OR "Safe City" OR "Smart Cities" OR "Safe Cities" OR "City Safety") AND ("Public Safety" OR "PPDR" OR "Public Protection and Disaster Relief"))	5	0	0	2	0	0
43	(("LTE" OR "Long Term Evolution" OR "Long-Term Evolution" OR "4G") AND ("Mission Critical Communication" OR "MCC") AND ("Smart City" OR "Safe City" OR "Smart Cities" OR "Safe Cities" OR "City Safety") AND ("5G mobile communication" OR "5G"))	45	1	1	3	0	0
44	(("Mission Critical Communication" OR "MCC") AND ("Smart City" OR "Safe City" OR "Smart Cities" OR "Safe Cities" OR "City Safety") AND ("5G mobile communication" OR "5G") AND ("technology assessment" OR "technological assessment"))	2	0	0	0	0	0
45	(("Mission Critical Communication" OR "MCC") AND ("Smart City" OR "Safe City" OR "Smart Cities" OR "Safe Cities" OR "City Safety") AND ("Public Safety" OR "PPDR" OR "Public Protection and Disaster Relief") AND ("5G mobile communication" OR "5G"))	8	0	0	1	0	0
46	(("Mission Critical Communication" OR "MCC") AND ("Smart City" OR "Safe City" OR "Smart Cities" OR "Safe Cities" OR "City Safety") AND ("Public Safety" OR "PPDR" OR "Public Protection and Disaster Relief") AND ("technology assessment" OR "technological assessment"))	0	0	0	0	0	0
47	(("Mission Critical Communication" OR "MCC") AND ("Smart City" OR "Safe City" OR "Smart Cities" OR "Safe Cities" OR "City Safety") AND ("Public Safety" OR "PPDR" OR "Public Protection and Disaster Relief") AND ("LTE" OR "Long Term Evolution" OR "Long-Term Evolution" OR "4G"))	5	0	0	1	0	0
48	(("Smart City" OR "Safe City" OR "Smart Cities" OR "Safe Cities" OR "City Safety") AND ("Public Safety" OR "PPDR" OR "Public Protection and Disaster Relief") AND ("5G mobile communication" OR "5G") AND ("technology assessment" OR "technological assessment"))	3	0	0	2	0	0
49	(("Smart City" OR "Safe City" OR "Smart Cities" OR "Safe Cities" OR "City Safety") AND ("Public Safety" OR "PPDR" OR "Public Protection and Disaster Relief") AND ("5G mobile communication" OR "5G") AND ("LTE" OR "Long Term Evolution" OR "Long-Term Evolution" OR "4G"))	211	2	2	39	2	2
50	(("Smart City" OR "Safe City" OR "Smart Cities" OR "Safe Cities" OR "City Safety") AND ("Public Safety" OR "PPDR" OR "Public Protection and Disaster Relief") AND ("5G mobile communication" OR "5G") AND ("Mission Critical Communication" OR "MCC"))	8	0	0	3	0	0
51	(("Public Safety" OR "PPDR" OR "Public Protection and Disaster Relief") AND ("5G mobile communication" OR "5G") AND ("technology assessment" OR "technological assessment") AND ("LTE" OR "Long Term Evolution" OR "Long-Term Evolution" OR "4G") AND ("Mission Critical Communication" OR "MCC"))	0	0	0	0	0	0
52	(("Public Safety" OR "PPDR" OR "Public Protection and Disaster Relief") AND ("5G mobile communication" OR "5G") AND ("technology assessment" OR "technological assessment") AND ("LTE" OR "Long Term Evolution" OR "Long-Term Evolution" OR "4G") AND ("Smart City" OR "Safe City" OR "Smart Cities" OR "Safe Cities" OR "City Safety"))	3	0	0	2	0	0
53	(("5G mobile communication" OR "5G") AND ("technology assessment" OR "technological assessment") AND ("LTE" OR "Long Term Evolution" OR "Long-Term Evolution" OR "4G") AND ("Mission Critical Communication" OR "MCC") AND ("Smart City" OR "Safe City" OR "Smart Cities" OR "Safe Cities" OR "City Safety"))	2	0	0	0	0	0
54	(("Public Safety" OR "PPDR" OR "Public Protection and Disaster Relief") AND ("5G mobile communication" OR "5G") AND "LTE" OR "Long Term Evolution" OR "Long-Term Evolution" OR "4G") AND ("Mission Critical Communication" OR "MCC") AND ("Smart City" OR "Safe City" OR "Smart Cities" OR "Safe Cities" OR "City Safety")	4	0	0	4	0	0
55	(("technology assessment" OR "technological assessment") AND ("LTE" OR "Long Term Evolution" OR "Long-Term Evolution" OR "4G") AND ("Mission Critical Communication" OR "MCC") AND ("Smart City" OR "Safe City" OR "Smart Cities" OR "Safe Cities" OR "City Safety") AND ("Public Safety" OR "PPDR" OR "Public Protection and Disaster Relief"))	0	0	0	0	0	0
56	(("5G mobile communication" OR "5G") AND ("technology assessment" OR "technological assessment") AND ("Mission Critical Communication" OR "MCC") AND ("Smart City" OR "Safe City" OR "Smart Cities" OR "Safe Cities" OR "City Safety") AND ("Public Safety" OR "PPDR" OR "Public Protection and Disaster Relief"))	0	0	0	0	0	0
57	(("5G mobile communication" OR "5G") AND ("technology assessment" OR "technological assessment") AND ("LTE" OR "Long Term Evolution" OR "Long-Term Evolution" OR "4G") AND ("Mission Critical Communication" OR "MCC") AND ("Smart City" OR "Safe City" OR "Smart Cities" OR "Safe Cities" OR "City Safety") AND ("Public Safety" OR "PPDR" OR "Public Protection and Disaster Relief"))	0	0	0	0	0	0
	Results	59552	5387	4718	180	49	57
	Results without repetition				124	13	9
	Total Results	286					
	Total Results without repetition	146					

Figure 63 - Strings 28 to 57

2023

DÉBORA VANESSA CAMPOS FREIRE

MISSION-CRITICAL COMMUNICATIONS FROM LMR TO 5G:
A Technology Assessment approach for Smart City scenarios