"MOBILIZADOR 5G"

Components and services for 5G networks

Project nº 24539

Deliverable D3.1

M2M critical communications scenarios and analysis of architectures

Relatório D3.1

Análise de arquiteturas e cenários de comunicações críticas M2M

PPS	**PPS 3**
Activity	**A3.1 – Preliminaries studies**
Dissemination level	**Public**
Date	**June 2018**
Version	**1.0**

Project confinanced by:

Project Lider:
Altice Labs, S.A.
Rua Eng. José Ferreira Pinto Basto
3810-106 Aveiro – Portugal
http://www.alticelabs.com
Tel: +351 234 403 200
Fax: +351 234 424 723

Sumário executivo

O presente relatório pretende consolidar a actividade de Estudos preliminares associados ao PPS3, dando-se enfoque à actualização do estado da arte em termos tecnológicos e à actualiação de conhecimentos técnicos de forma a poder realizar com sucesso todas as tarefas de especificação técnica, previstas na actividade 2. No âmbito desta actividade, é feito adicionalmente, o levantamento de requisitos inerentes às várias linhas de produto a desenvolver, pretende-se fazer uma análise de perigos, riscos e de soluçoes de segurança para aplicações críticas M2M e são definidos os casos de uso dos sistemas Bodykit e de video suportado em MEC

Executive Summary

This report intends to consolidate the activity of Preliminary Studies associated to PPS3, focusing on updating the state of the art in technological terms and updating of technical knowledge so as to be able to successfully carry out all the technical specification tasks foreseen in the activity 2. In the scope of this activity, the requirements of the various product lines to be developed are also surveyed. It is intended to carry out a hazard, risk and safety solution analysis for critical M2M applications and define the use cases of the Bodykit and video systems supported in MEC

Table of Contents

Sumário executivo 5
Executive Summary 7
Table of Contents 9
List of Figures 11
List of Tables 13
Glossary 15
Definitions 17

1 Introduction 19

2 Task 3.1.1- (leader EFACEC Energia) 21
State of the art for medium voltage real time distributed protection systems 21
2.1 Analysis of scenarios 21
2.2 Technologies 21
2.3 Architectures 23
2.4 General and regulatory requirements 25

3 Task 3.1.2- (leader EFACEC Engenharia) 28
Hazard analysis and risk assessment in communications for railway signaling using 5G networks 28
3.1 Analysis of scenarios 28
3.1.1 Safety critical scenario 29
3.1.2 Non-safety critical scenario 29
3.2 Technologies 30
3.3 Architectures 30
3.4 General and regulatory requirements 32

4 Task 3.1.3- (leader Univ. Coimbra) 34
Analysis of security solutions for critical M2M applications in IoT environment, MV network control systems and railway signaling systems (operating on 5G networks) 34
4.1 Analysis of scenarios 34
4.2 Technologies 35
4.3 Architectures 38
4.3.1 BK Device 38
4.3.2 MQTT Server(s) 39
4.3.3 TICK Stack 39
4.3.4 BK Servers 39
4.3.5 CCC App 39
4.4 The architecture General and regulatory requirements 40

5 Task 3.1.4- (leader IT Univ. Aveiro) 42
Requirements analysis and mechanisms for reliable data mobility in M2M environments 42
5.1 Analysis of scenarios 42
5.2 Technologies 43
5.3 Architectures 44
5.4 General and regulatory requirements 44

6 Task 3.1.5 e 3.1.6 - (leader Ubiwhere) 46
Upgrading of the state of the art in Mobile Edge Computing (MEC) and definition of use cases of an intelligent video surveillance system (Ultra HD) in Ultra-High Mobility, using MEC 46
6.1 Mobile Edge Computing State of the art 46
6.1.1 Architecture 46
6.1.2 ETSI MEC Architecture 47
6.1.3 ETSI MEC in a NVF environment 48
6.1.4 MEC Use Cases 49
6.2 Intelligent video surveillance system (Ultra HD) in Ultra-High Mobility, using MEC 50

6.2.1 Analysis of scenarios ... 50
6.2.2 Architectures ... 50
6.2.3 General and regulatory requirements ... 52

7 Task 3.1.7 - (leader Onesource) ... 53
Definition of Use Cases and Requirements for Bodykit ... 53
7.1 Analysis of scenarios ... 53
7.2 Technologies ... 54
7.3 Architectures ... 54
7.4 General and regulatory requirements ... 56

8 Conclusions ... 58
8.1 Main Conclusions ... 58

9 References ... 59

Authors list ... 61

Versions history ... 63

List of Figures

Figure 1 – FDIR solutions 24
Figure 2 – 5G high-level requirements for the envisioned scenarios to analyse 26
Figure 3 – Level crossing signaling system architecture 28
Figure 4 – M2M signalling communications 29
Figure 5 – Safety Critical scenario - The train directly sends the information to the LX controller, whenever the train is approaching 30
Figure 6 – Safety Critical scenario - communication between the strike in points and the Level Cross controller 31
Figure 7 – Safety Critical scenario communication - the train directly sends strike in message to the LX controller at strike in distance 31
Figure 8 – Safety Critical scenario communication - the strike in sensors send strike in message to the LX controller when detects the approaching train 31
Figure 9 – Non-Safety Critical Scenario – the approaching train connects to video camera...... 32
Figure 10 – Non-safety critical scenario 32
Figure 3 - General overview of BodyKit........ 38
Figure 4 – llustrated scenario. 42
Figure 5 – Illustrated comparison of virtual machines, containers, containers within virtual machines and unikernels [3]. 43
Figure 6 – Proposed Architecture. 44
Figure 7 - MEC high level architecture 47
Figure 8 - MEC ETSI reference architecture [8] 47
Figure 9 - MEC reference architecture in NFV environment [9] 49
Figure 10 - System architecture 51
Figure 11 - Video processing components 52
Figure 12 - User equipment interaction 52
Figure 13 - BodyKit use-case scenario 55

List of Tables

Table 1– Comparative analysis of Self-Healing schemes 24
Table 2 – Examples of data and control topics in MQTT 39
Table 3 – Possible PPDR scenarios 53

Glossary

5GC	5G Core
AAA	Authentication, Authorization and Accounting
AF	Application Function
AI	Artificial Intelligence

Definitions

NA

1 Introduction

During the activity A3.1, Preliminaires studies, the studies regarding the 5G critical M2M communication scenarios and architectures were been performed. According the activity task plan, in the following sections the studies results are presented. For each task, the task leader presents the results agregated in the following sections: analysis of scenarios, technologies to be used, communications architectures, general and regulatory requirements.

2 Task 3.1.1- (leader EFACEC Energia)

State of the art for medium voltage real time distributed protection systems

The present use case exploits the use of 5G communications for improving decentralized power grid self-healing algorithms. Having access to a low-latency ultra-reliable wireless communication infrastructure will enable the implementation of advanced grid topology reconfiguration schemes based on high-speed coordination of remotely located Intelligent Electronic Devices (IEDs).

2.1 Analysis of scenarios

Scenario 1 – Protection Coordination:

Protection coordination throughout the power system is of paramount importance to ensure reliable, secure and selective fault detection and clearance.

Typical coordination schemes do not include the exchange of information between IEDs due to the absence of an adequate communication infrastructure. Coordination is achieved based on time grading and/or analogue measurements analysis with obvious shortcomings including higher fault clearance time and difficult deployment for complex power system topologies.

For the implementation of the protection coordination scenario, the testing environment shall provide high-speed communications between IEDs, allowing them to coordinate, ensuring logic selectivity on fault clearance.

Scenario 2 – Automatic Reconfiguration:

After any fault detection and isolation, it is required that only the smallest portion possible of the electric system is de-energized, ensuring minimal impact in power supply to customers. In some network topologies, to comply with this requirement, it is necessary to deploy automatic reconfiguration of the power network.

The self-healing scheme which will be exploited within the 2nd scenario proposed for the Smart Grid use case, related with the effective implementation of Self-Healing through power grid's automatic reconfiguration, will follow a decentralized architecture, supported by IED peer-to-peer GOOSE communications.

It is important to keep in mind that faults can occur at any time and cannot be predicted or avoided by the power system protection devices. For this application, it is imperative that the communication system availability is not compromised by external factors (*e.g.*, network congestion or denial of service attacks) and that reliability and a certain degree of cybersecurity are ensured by the communication infrastructure.

2.2 Technologies

Machine-to-machine (M2M) critical communications for the development of Medium Voltage (MV) protection, automation and distributed control systems, supported by secure, low-latency, ultra-reliable peer-to-peer communications based on IEC61850 protocols, such as Generic Object Oriented Substation Events (GOOSE), constitute one of the most relevant topics within the scope of the strategy for the implementation and industrial dissemination of 5G technologies. The development of these critical communication links based on 5G will enable the implementation of advanced self-healing schemes in distribution networks, that will prove faster and more effective on detecting and isolating faults, and subsequently proceeding with the service restoration through automatic power grid reconfiguration.

The use of peer-to-peer 5G communications between distributed control equipment leverages the diminishing of the response-times and the increasing of protection and automation systems' efficiency, accelerating and improving the accuracy of Fault Detection, Isolation, and service Restoration (FDIR) mechanisms. A superior performance from the protection systems is consequently translated into an overall improvement of the operational efficiency, of the system's reliability, and of the technical Quality of Service (QoS), mitigating the economic impacts associated with the unavailability of services for which the network operator is responsible.

Network automation using advanced protection, command and control systems based on high-speed communications will also involve the increase of power grid's resilience and adaptability, particularly of the MV distribution networks. It is in this voltage level that the majority of the Distributed Generation (DG) capacity from Renewable Energy Sources (RES) is installed, which has been posing new challenges of coordination to the protection systems due to the intermittent and bidirectional energy flows that they cause, affecting a wider interconnected system.

Self-healing may be based on different implementation strategies, using several distribution automation solutions for remote network operation in real time, through network high-speed communication empowering, hardware and software outfitting.

Independently of the implemented architecture, a self-healing solution includes a component layer, composed by the network physical infrastructure, a bidirectional and integrated information and communication layer, and a function layer, which includes different processes – monitoring, warnings analysis, decision-making and control actions.

The evolution of the technologies available to perform device-to-device (D2D) communications between critical devices within an advanced Distribution Automation System (DAS) and relevant standards such as IEC 61850, allowed to consolidate the dissemination of distribution automation solutions among the distribution system. Currently the market provides solutions for the advanced control of MV networks assets, namely:

- Application for reclosers, sectionalizers, fault interrupters, Ring Main Unit (RMUs);
- Protection and control of critical assets within the MV network;
- Integration in centralized systems;
- Conventional Remote Terminal Unit (RTU) functionalities;

The functionalities' range is also wide, and may include:

- Several protection functions;
- Automatic reclosing (multiple cycles);
- Algorithms to detect and isolate faults, and service restoration, and to configure different network schemes;
- Condition monitoring of power switchgear devices;
- Fault location;
- Power quality monitoring;
- IEC 61131-3 open programming;
- IEC 61850 communication including, GOOSE; messaging;

However, the key challenges in terms of innovation and differentiation of the solutions based in distributed self-healing algorithms rely on the following topics:

- Integration in systems with bidirectional power flows and distributed generation;

- Adaptive parameters;
- Plug-and-play and simplified engineering approaches;
- Peer-to-peer distributed automation and control;
- Fast and optimized FDIR strategies using IEC 61850 / GOOSE communications;
- Adequacy of communications network infrastructure.

2.3 Architectures

According to the Smart Grid Architecture Model (SGAM), which resulted from the Smart Grid reference architecture proposed by the Smart Grid Coordination Group, information and communication represent fundamental layers across the interoperability dimension of the framework of modern Smart Grids.

The effective implementation of Smart Grids relies on the continuous investment in distribution automation technologies which allow the remote operation of the power network in nearly real time. The commitment to improve the level of monitoring and controllability of the power network will ensure the possibility of implementing preventive actions to reinforce resilience according to the predicted evolution of the operating state, and deal with possible incoming contingencies, such as faults that may lead to power outages.

Within the Smart Grid, advanced protection schemes such as Self-Healing were designed to immediately detect and isolate faults and proceed with the automatic reconfiguration of the power network for service restoration. In order to supply the maximum load within a certain Distribution Grid Area (DGA) affected by a fault, the FDIR procedures must become as agile as possible, thus reducing the load restoration time to a minimum. In the first two stages of the process, the IEDs controlling the power switchgear equipment must rapidly coordinate, relying on high speed communications to ensure critical selectivity during fault detection and isolation, i.e., the closest device must clear the fault while the upstream devices should block and then reset, after fault isolation is completed trough the opening of the device immediately downstream of the fault.

FDIR solutions are part of the evolution on the application of advanced automation functionalities to the distribution networks. The recent progress on the communication channels and technologies also contributes to leverage the development of the distribution automation.

Apart from the more traditional self-healing solutions, supported by different power switchgear technologies (*e.g.*, reclosers and sectionalizers) and based on Voltage-Time (V-T) automatisms, generically the solutions presenting communication-based coordination may be classified in the following three variants:

- Centralized at the dispatch centre – SCADA/DMS/OMS;
- Semi-decentralized at the substation level, which is a substation centric solution based on the Smart Substation Controller (SSC) – the micro-DMS of Substation Automation System (SAS);
- Decentralized at the feeder level, based in distributed IEDs interacting trough peer-to-peer messaging integrating a Distribution Automation Systems (DAS).

The following figure presents the three main architectures to implement FDIR solutions framed in self-healing schemes in distribution networks.

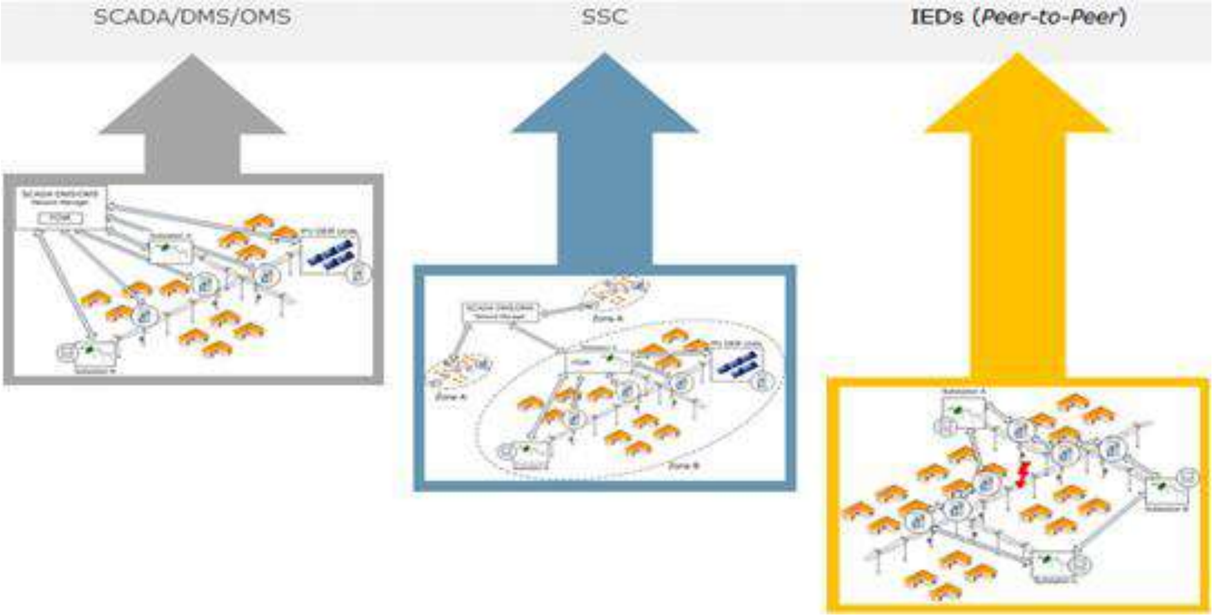

Figure 1 – FDIR solutions

The following table presents a comparison between the three solutions mentioned above for implementing self-healing in MV distribution networks. The focus of the analysis is on the main characteristics of the presented solutions, mainly the architectural framework and configuration possibilities, the hardware specificity regarding the compatible RTUs/IEDs, the control infrastructure specificities, the flexibility, scalability and complexity of each solution, and the respective response-time.

Table 1– Comparative analysis of Self-Healing schemes

	CENTRALIZED FDIR **SCADA/DMS/OMS**	SEMI-DECENTRALIZED FDIR **SUBSTATION CENTRIC SOLUTION**	DECENTRALIZED FDIR **DISTRIBUTED IEDS (*PEER-TO-PEER*)**
ARCHITECTURE / CONFIGURATION	Centralized on the dispatch centre DMS/OMS, which may control DGA or an entire distribution network; Central failure point and dependency of the communication networks between the devices and the control centre; Full integrated configuration with the control centre.	Implemented on the SSC – the micro-DMS – which usually controls a local DGA, aggregating neighbour substations; A central failure point per DGA; The configuration may be integrated with the control centre;	Without a central failure point; Ability to manage more complex failure modes.
RTU / IED	Allows any type of RTU.	Allows any type of RTU.	Allows only specific RTUs/IEDs.
REMOTE AND TELE-CONTROL INFRASTRUCTURE	Adaptable to any tele-control infrastructure.	Adaptable to any tele-control infrastructure, but implies additional access from the RTUs to the substation.	Adaptable to modern tele-control and communications infrastructures – distributed intelligence –, impossible to be adapted to conventional infrastructures presenting low performance

FLEXIBILITY, SCALABILITY AND COMPLEXITY	High flexibility, wide area scalability, and complexity.	Medium flexibility, wide area scalability, and complexity.	Low flexibility, wide area scalability, and complexity.
RESPONSE-TIME	Slower response-time	Average response-time	Faster response-time

2.4 General and regulatory requirements

The regulators' demands and the ever-higher performance and QoS expectations from end-users and other stake-holders lead to an increased necessity from the utilities invest in order to more effectively and efficiently address the various stages of an energy supply interruption's lifecycle, including the large-scale outages usually caused by adverse weather conditions.

In order to reach a new level of operational performance, utilities will need to invest in more sophisticated solutions, strengthen systems' integration and data sharing, promote the analysis of all available information and identify new solutions and improvements across the entire process management chain, before and after the incidents. The energy companies, particularly in the area of electricity distribution, have as their main challenges reliability, resilience to anomalous situations, operational efficiency and global QoS preservation that consequently will lead to a high index of customer satisfaction.

The regulators also have a relevant role to play in this process, and the decisions and the strengthening of regulatory frameworks may influence the utilities' investment roadmap, particularly in the area of protection, automation and control, supervision and monitoring, data privacy and security, whether at the consumer or at the power grid level.

The occurrence of faults, temporary or permanent, in the distribution network, is one of the most significant factors with direct impact on the degradation of key performance indicators of the network's operation, such as SAIFI, MAIFI or SAIDI – the System Average Interruption Frequency Index, Momentary Average Interruption Frequency Index, and System Average Interruption Duration Index – which characterize the reliability of the service provided. In addition, power outages have a significant economic impact on the operator's operational activity, once they result directly in a reduction of the revenues due to the cost of the Energy Not Supplied (ENS), the elimination of incentives to improve QoS, and generation curtailment, manly DG from RES.

The possibility of using public radio networks, such as the 5G networks, presents a new paradigm for the management of critical systems in electric power networks, since it allows the installation of equipment at any point in the electric grid, without the need to change the existing communication infrastructure. However, the use of a public communications network for the transmission of data relating to critical systems raises considerable concerns both in terms of security (in terms of resilience of the solution against attacks on its safety and integrity), as it exposes the systems to possible remote attacks, as well as quality of service, including signal coverage, availability and maximum latency values. This latter factor is especially important for distributed protection systems, which impose demanding latency requirements that the technology present in the current public communications networks can hardly bear.

The future 5G mobile networks, unlike previous generations (which focused essentially on transmission performance increments), promise to evolve the current communication networks and their underlying functioning in terms of the flexibility and dynamism of the network's own functioning, and to its security, allowing the network to be configured to meet the requirements of the services in use, namely aspects of maximum latency guarantee in the order of a few milliseconds and a coverage and availability close to 100%, making possible the use of radio communications in distributed protection systems with self-healing algorithms.

The passage of communications necessary for the management of the electricity networks from a private network to the public network requires major changes in the interfaces and protocols used by the critical systems concerned and by the core of the 5G network in recognizing and making them more flexible its operation. In this sense, we propose to evolve EFACEC's protection solutions, providing them with physical and logical interfaces to communicate over 5G networks and to implement protocols that comply with international standards directed to the energy sector, with the aim of increasing future competitiveness and interoperability solutions at international level.

To foster the use of the new solution proposed at national and international level, it is mandatory to ensure a wide range of very demanding requirements in terms of: 5G network availability, reliability and integrity of communications, maximum communication latency in the order of milliseconds, high security in the communication network and global energy management systems, among others.

Regardless of the functional architecture adopted, the high-end protection, automation and control solutions used to implement the advanced self-healing schemes may benefit from ultra-Reliable Low Latency Communications (uRLLC) provided by a 5G network slicing framework. Depending on the functional architecture different high-level requirements may be requested from the ICT infrastructure. A SCADA/DMS centric solution may be integrated in the dispatch centre. Will be able to implement complex self-healing schemes, using different types of remote control technologies within a high wide area. A semi-decentralized solution is usually integrated in the primary substation controller, where a micro-DMS will be able to implement less complex self-healing schemes within the primary substation wide area, leading to a more satisfactory performance in terms of response time. A completely decentralized solution is achievable using specific IEDs – IEC61850-compliant –, D2D communications – peer-to-peer GOOSE messaging – and distributed intelligence algorithms to implement faster self-healing schemes within a local area – lower scalability.

In figure 2 is presented a radar diagram that characterizes the level of importance that some of the 5G high-level requirements have, considering the above-mentioned scenarios: protection coordination, and automatic reconfiguration.

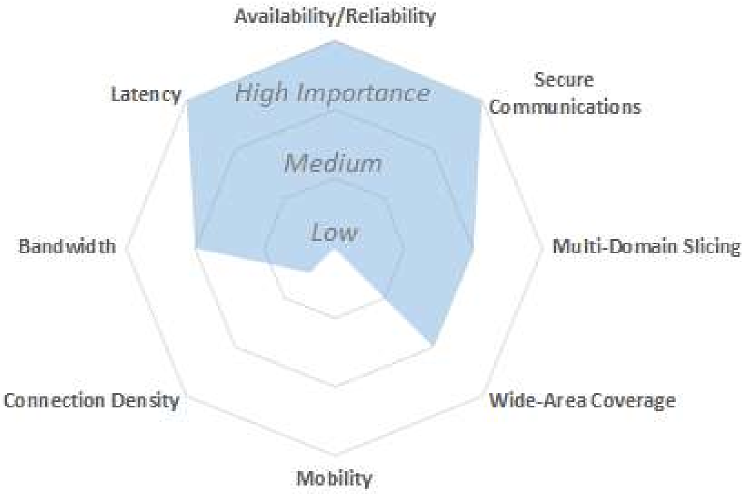

Figure 2 – 5G high-level requirements for the envisioned scenarios to analyse

With this framework, investing more expressively in Distribution Automation (DA) is one of the major challenges that utilities have at hand today. This is an outstanding opportunity for differentiating self-healing solutions such as distributed D2D communication solutions based on radio technologies, such as 5G technology, ensuring a real-time and low latency communication infrastructure.

The implementation of a distributed self-healing system involves the creation or adaptation of the communications network managed by the distribution entity to create peer-to-peer connections, which may present a high CAPEX for the network operator.

In summary, these are the main innovative and differentiating vectors addressed by this LDT for the management of electric power grids:

- **Distributed self-healing based on peer-to-peer communications:**
  - In which automatic reconfiguration of the network allows reducing the times of interruption of energy supply to consumers, improving the levels of quality of service;
  - Direct communication between intelligent units after a fault allows faster network reconfiguration;
- **Cybersecurity:**
  - By using communication networks that are shared with other users, we increase the risk of malicious use and may jeopardize the functioning of this critical system. Challenges in this regard are communications, integrity and other issues, such as defending infrastructure against external attacks;
- **Service quality:**
  - In order to ensure proper functioning of the algorithms, real-time communication with high availability and low latency, as well as adequate geographic coverage is required;
- **Use of public communications networks:**
  - The 5G networks will allow us to change the current paradigm of use of dedicated communication networks to use shared public networks, which will provide the necessary quality of service for this type of system (namely high availability, low latency and wide geographic coverage).

3 Task 3.1.2- (leader EFACEC Engenharia)

Hazard analysis and risk assessment in communications for railway signaling using 5G networks

One of the demonstration products in the PPS3 scope is the application of 5G communications networks to railway signalling applications, namely to level crossing signaling systems.

3.1 Analysis of scenarios

Typically a level crossing signaling system as the following architecture:

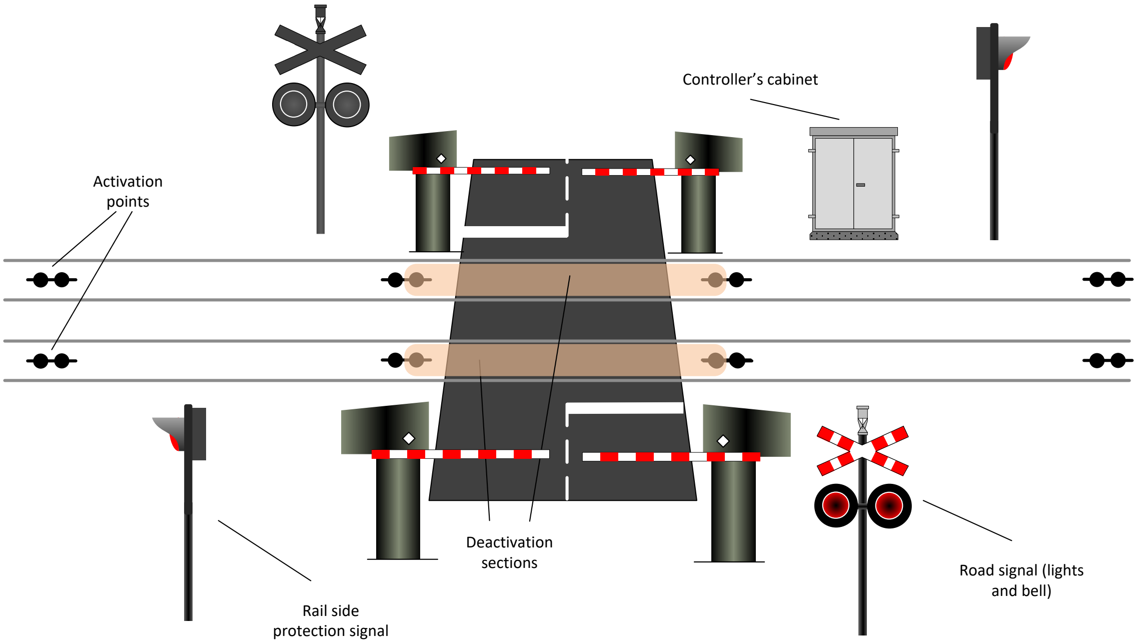

Figure 3 – Level crossing signaling system architecture

The communications between the controller's cabinet and the peripheral devices (train detectors, signals and barriers) are typically assured by means of copper cable wires.

For PPS3 the M2M signaling communications, the use cases involves, from the point of view of functional safety, two main scenarios, a safety critical scenario and a non-safety critical scenario.

Regarding the figure bellow, the D2D and V2X communications are safety critical type and X2V are non-safety critical.

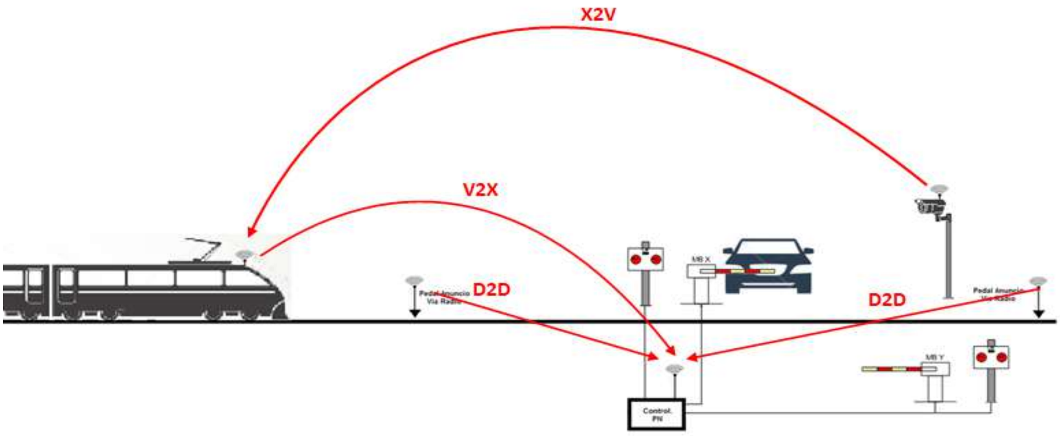

Figure 4 – M2M signalling communications

3.1.1Safety critical scenario

The safety critical scenario includes the communication of the train approaching event (level crossing strike in) from the trackside train detector device (D2D) and alternatively from the onboard computer of the approaching train (V2X) to the level crossing main controller via a wireless network using 5G technology.

The main challenges / requirements of this system are:

a) The strike in event failure rate (dangerous failures) must be compatible with the integrity level 4 (SIL4) defined in standard EN50159-2;

b) From the security point of view the data transmission also has to comply with the requirements defined in the standard E50159-2 since it is intended to transmit information with a impact in the safety functioning of the system;

c) The communication network must allow the permanent communication between the two end points, and a communication check alive transmission rate, compatible with the required level crossing system safety time shall be guaranted;

d) In case of communications failure detection the system shall return to a safety state closing the barriers;

e) In the V2X scenario, in case the approaching train doesn’t detect or communicate the approaching event the level crossing system must show to the driver a danger aspect signal at train braking distance, signaling the level crossing open state.

3.1.2Non-safety critical scenario

The non-safety critical scenario includes the communications of level crossing video images to the approaching train (X2V) using a 5G communication network. In this scenario the video images authentication and low latency I transmission shall be assured.

3.2 Technologies

Several technologies are involved, concerning this M2M approach, being, in the scope of this PPS, the NR-5G (New Radio) the main goal. However, it is possible to describe the technologies involved, according with the following list:

a) Video processing and video transmission, to assure the level crossing (LX) video images to the train
b) IP (Internet Protocol) Communications to the LX controller whenever a train is detected (directly from the train or via detectors on the track)
c) Locating tecnologies to determine the real position of the train
d) 5G CPE for the onboard comunications and for the LX controller
e) 5G Network to assure the communication between all the “actors” (train, LX)

3.3 Architectures

Concerning the safety critical scenarios, the reference arquitectures are represented in the figure 5 and 6

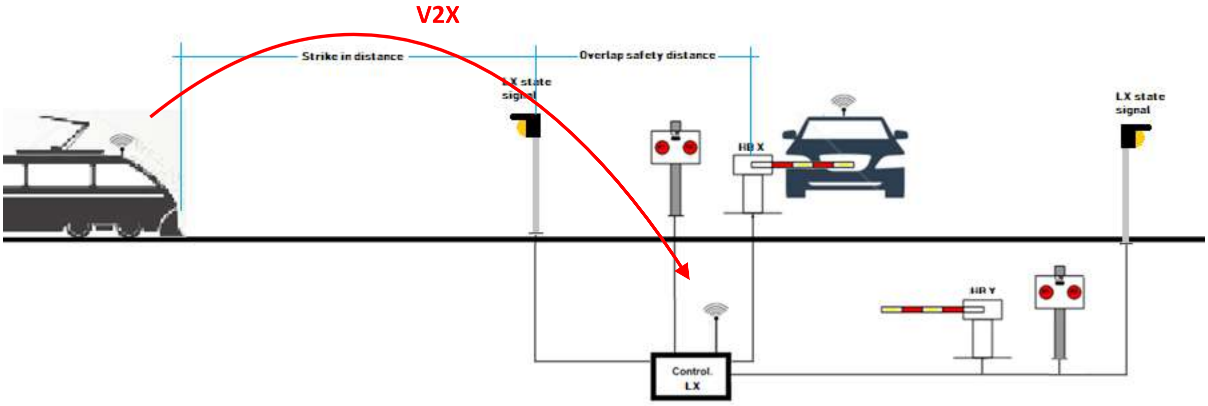

Figure 5 – Safety Critical scenario - The train directly sends the information to the LX controller, whenever the train is approaching

The following scenario includes the communication between the fix strike in sensors and the LX controller.

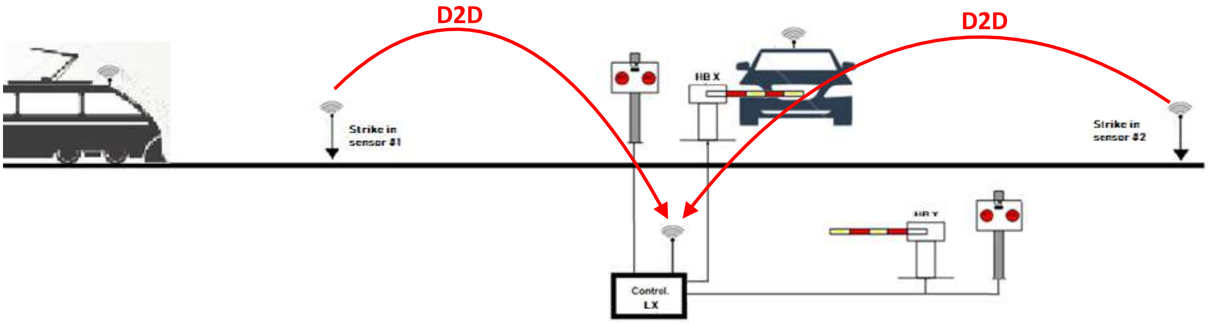

Figure 6 – Safety Critical scenario - communication between the strike in points and the Level Cross controller

In terms of block diagrams, the figures 7 and 8 reperesents the communications architectures

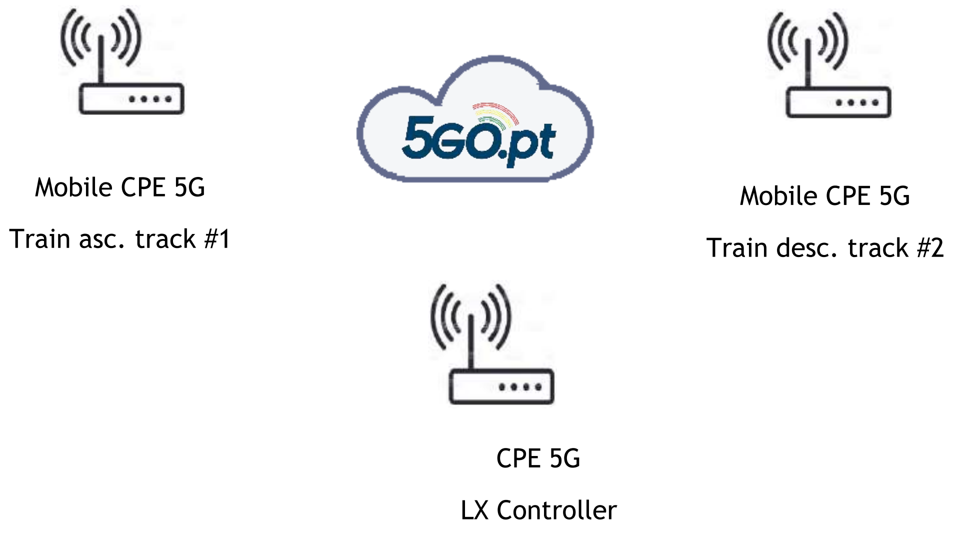

Figure 7 – Safety Critical scenario communication - the train directly sends strike in message to the LX controller at strike in distance

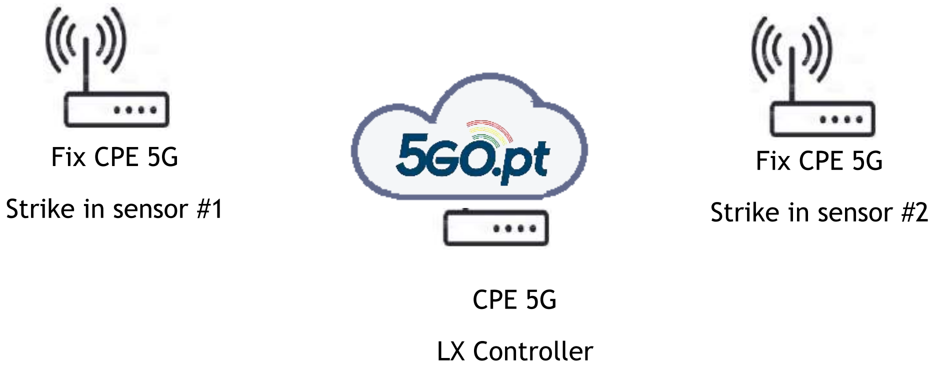

Figure 8 – Safety Critical scenario communication - the strike in sensors send strike in message to the LX controller when detects the approaching train

Concerning the non safety critical scenario, the reference architecture is represented in the figure y

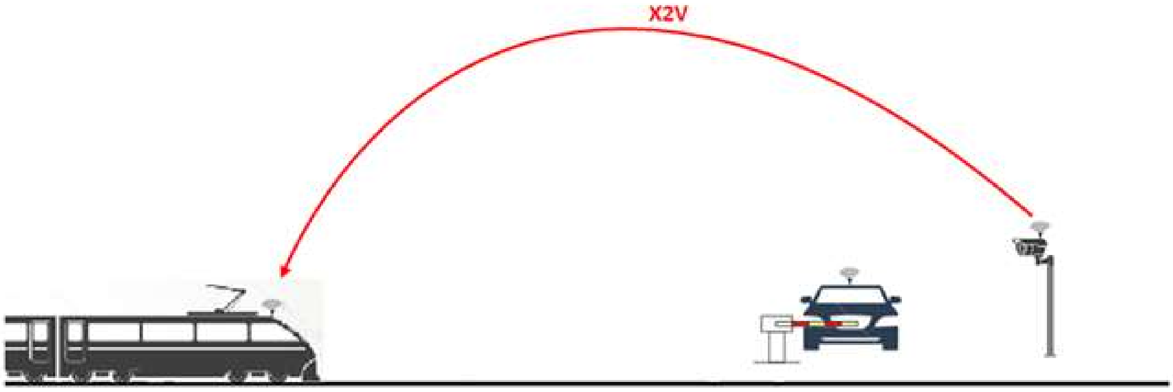

Figure 9 – Non-Safety Critical Scenario – the approaching train connects to video camera

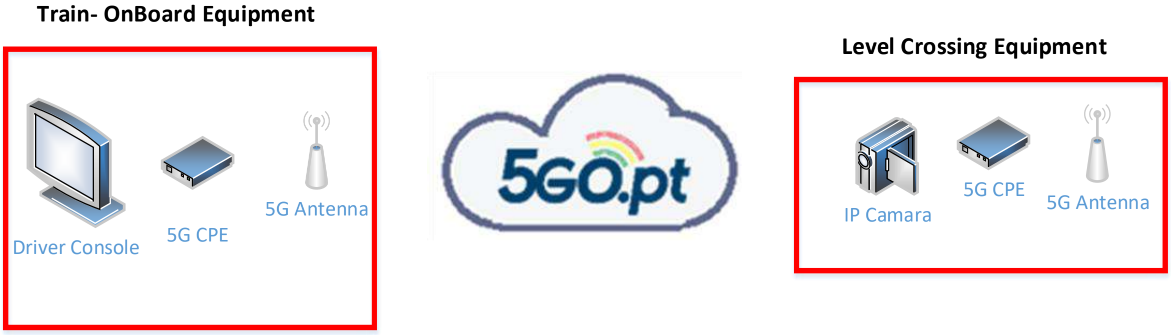

Figure 10 – Non-safety critical scenario

3.4 General and regulatory requirements

Communications in the signaling systems domain shall require a proof of RAMS properties (Reliability, Availability, Maintainability and Safety) according EN50126 (IEC62278) and EN50129 and a proof of security for Class 7 communications according EN50159 (IEC62280). In addition to this, however, high demands in terms of reliability and availability must be met, and, above all, minimum delay times of transmission (latency <10ms) and the guarantee of delivery must be ensured, the safety RaSTA (Rail Safe Transport Application) protocol according DIN VDE V 0831-200 shall be applied.

The video transmission shall be supported according IEC 62676 - Video surveillance systems for use in security application, regarding Security, Integerity, availability and latency.

4 Task 3.1.3- (leader Univ. Coimbra)

Analysis of security solutions for critical M2M applications in IoT environment, MV network control systems and railway signaling systems (operating on 5G networks)

4.1 Analysis of scenarios

One important goal of the work to be developed in the context of this PPS (PPS3, Machine-to-Machine M2M communications) is to address the employment of 5G technology to support critical applications, considering in particular the technologiy to be developed in the context of PPS 1 and PPS 2. Thus, the target are applications requiring critical communications between systems and devices enabled capable of 5G communications. In such environments, security is of major importance and new mechanisms must be developed in order to address compatibility with the 5G standards, while also benefiting from the availability of new mechanisms available in the 5G architecture.

Here we begin by addressing the complementary usage scenarios considered in this PPS, in particular in what regards the critical areas of wearable response emergency awareness platforms and signaling relaying systems. In this context, we address in particular the particularities and requirements of two applications in such areas: the BodyKit application, as well as signaling systems applied to railway applications.

Critical M2M applications

One main area of application for 5G communications and security technologies is in the support of critical M2M applications. In this context, areas such as disaster recovery, MV network control systems and railway signaling systems are of particular interest, due to their fundamental requirements in terms of aspects such as latency of the communications, the guarantee of delivery of information related with alarms and the security of the communications, among others. The Body Kit application, which we analyze subsequently, belongs in the context of the application area of wareable situation awareness platforms, which may be applied to disaster and emergency handling and recovery situations.

Critical alerting and signaling applications

Another important area of application considered in the context of this PPS is that of alerting and signaling systems and, more particularly, signaling systems applied to railway applications. In this area, security requirements must be fulfilled by mechanisms designed to operate in conjugation with fundamental aspects such as the latency of critical communicatons using the 5G infrastructure, the quality of service assurances provided by such infrastructure, as well as the density of devices supported. In this context, the availability of communication channels reserved for the transportation of critical communications is of particular interest.

4.2 Technologies

We now proceed with an analysis of the communication and security technologies employed in the context of the considered M2M critical application, focusing in particular on the critical areas of wearable situation awareness platforms and signaling relaying systems, which we have previously identified. We start by addressing IoT communications technologies which are candidate to be explored or applied in the context of the previously referred architectures.

6LoWPAN adaption layer

One fundamental characteristic of the Internet architecture is that it enables packets to traverse interconnected networks using heterogeneous link-layer technologies, and the mechanisms and adaptations required to transport IP packets over particular link-layer technologies are defined in appropriate specifications. With a similar goal, the IETF IPv6 over Low-power Wireless Personal Area Networks (6LoWPAN) working group (https://datatracker.ietf.org/wg/6lowpan/about/) was formed to produce a specification enabling the transportation of IPv6 packets over low-energy IEEE 802.15.4 and similar wireless communication environments. 6LoWPAN is currently a key technology for the IoT, and one that has changed a previous perception of IPv6 as being impractical for constrained low-energy wireless communication environments. 6LoWPAN may thus enable to employment of standard IP comunications over low-range and low-power wireless communications with sensors and actuators part of a critical M2M application.

The 6LoWPAN adaptation layer materializes a good example of how cross-layer mechanisms and optimizations may enable standardized communication protocols for the IoT, and enables IPv6 end-to-end communications between constrained IoT sensing devices and other similar or more powerful Internet entities, thus providing the required support for the building of future IPv6-based distributed sensing applications on the IoT. The 6LoWPAN adaptation layer maps the services required by the IP layer on the services provided by the IEEE 802.15.4 MAC layer. As for security mechanisms, security is absent from the 6LoWPAN base specification, altough several research proposals do exist addressing the design of compressed security headers for this adaptation layer, as well as key management and authentication delegation, among others.

RPL (Routing Protocol Layer)

The Routing Over Low-power and Lossy Networks (ROLL) working group of the IETF (https://datatracker.ietf.org/wg/roll/charter/) was formed with the goal of designing routing solutions for IoT applications. The current approach to routing in 6LoWPAN environments is materialized in the Routing Protocol for Low power and Lossy Networks (RPL) Protocol (https://tools.ietf.org/html/rfc6550). Rather than providing a generic approach to routing, RPL provides in reality a framework that is adaptable to the requirements of particular classes of applications. In terms of security, RPL defined secure versions of routing control messages employed in the context of the routing framekwork, altough we must note that, other than the secure versions of the routing control messages and the security modes previously discussed, no further security mechanisms are designed in the current version of the RPL Protocol standard. The remaining documents produced in the IETF ROLL group only identify general security requirements and goals, without defining particular security mechanisms.

CoAP (Constrained Application Protocol)

The only transport-layer protocol currently supported by the 6LoWPAN adaptation layer is the User Datagram Protocol (UDP), since it provides a good trade-off between reliability and energy-cost. Despite this, other transport-layer approaches supporting more advanced reliability mechanisms may be adopted for 6LoWPAN in the future. The adoption of transport-layer approaches with characteristics more close to protocols such as the Transmission Control Protocol (TCP) is still open to debate, and research is ongoing addressing the adaptation of TCP for 6LoWPAN environments. Transport protocols with such mechanisms are currently considered to be too expensive for 6LoWPAN environments, given its requirements in terms of the exchange of traffic control information and the maintenance of status information on constrained sensing devices. Therefore, the support of UDP on 6LoWPAN networks is guiding the design and standardization, at the Constrained RESTful Environments (CoRE) working group of the IETF (https://datatracker.ietf.org/wg/core/charter/), of an appropriate solution for the application layer, in the form of the CoAP (Constrained Application Protocol, https://tools.ietf.org/html/rfc7252).

In term of how CoAP support security, it defines bindings to DTLS (Datagram Transport-Layer Security) to secure CoAP messages, along with a few minimal configurations which are mandatory to implement and appropriate to constrained environments. DTLS is in practice TLS with added features to deal with the unreliable nature of the UDP transport. The impact of supporting DTLS on constrained wireless sensing devices is due to the cost of supporting the initial handshake, plus the processing of security for each exchanged CoAP messages. The fact that the current strategy is to address security at the transport layer also opens research opportunity considering different strategies, such as the design of security mechanisms at the application-layer protocol itself (granular security or semantic security) or the delegation of costly DTLS handshake-related operations to more capable devices (e.g. gateways supporting communications between the IoT and Internet domains).

Bluetooth and Bluetooth Low Energy

The Bluetooth wireless standard support short-range communications targeted at personal, portable, and handheld electronic devices. Bluetooth 4.0, and known as Bluetooth Low Energy, is aimed at applications in areas such as healthcare, fitness, location beacons and home entertainment, among others. Compared with previous versions of the standard, Bluetooth Low Energy is intended to provide considerably reduced power consumption and cost while maintaining a comparable communications range.

In terms of security, Bluetooth provides various security modes, and it is up to the device manufacturer to determine which mode to include in a given Bluetooth-enabled device. Frequently, users configure trusted devices with which data is exchanged without subsequent permissions being required. A Bluetooth device can be protected against unauthorized data transmissions using service-level security and device-level security. Authorization and identification procedures limit the use of Bluetooth services to the registered user and require confirmation from the user when a file is to be opened or transfered. Bluetooth wireless communications, due to its low-power and short-range focus, may be part of a critical application M2M running over 5G wireless communications, as subsequently discussed in the context of the architectures analyzed. On the other side, the security mechanisms provided by the standard may be complemented by other mechanisms designed in the context of the application at hand or available in 5G.

MQTT

The MQ Telemetry Transport (MQTT) protocol is designed to operate in a publish/subscribe model as is a simple messaging protocol, as is targeted at constrained devices opeating over low-bandwidth and high-latency and unreliable networks. In this context, MQTT complements the previously discusse low-range communication protocols. Similarly to the devices employed with 6LoWPAN or Bluetooth, MQTT devices are frequenty powered by batteries. As for security, MQTT was designed with the constraints of the devices in mind, and all common implementations employ SSL/TLS to enable transport security for the communications of telemetry data. As with 6LoWPAN, MQTT is a protocol focused on low-energy and short-range communications, and other security solutions may be developed for MQTT. For example, rather than adopting security at the transport layer, an alternative strategy could be to add security in the context of push/subscribe protocol, thus adopting an approach enabling semantic or more granular security. As with Bluetooth, we also observe that the lack of security mechanisms in the standard, in particular to support the subsequently identified requirements, represents an avenue to research and the design of innovative applications for critical M2M applications running over 5G wireless networks.

ZigBee

Zigbee (http://www.zigbee.org) is a standard for wireless technology designed to use low-power digital radio signals for personal area networks, similarly to IEEE 802.15.4. In fact, the suite of communication protocols defined by ZigBee are based on the IEEE 802.15.4 MAC and PHY layers, and are currently employed to enable low-power networks in areas as diverse as home automation, industrial control and smart cities, among others. ZigBee applications share much similarities with pure IEEE 802.15.4 applications, in terms of how communications are enabled and employed at the lower layers of the stack. Contrary to IEEE 802.15.4, the ZigBee stack supports a set of security-related mechanisms which may be used to enable more secure applications. ZigBee's security architecture is based on the employment of symmetric-key cryptography, and and also defines a key manegement protocol. Regarding key management, the standard defines mechanisms for key preinstallation, key transportation and key establishment.

RaSTA (Rail Safe Transport Application)

The RaSTA communications protocol (Rail Safe Transport Application) was designed with the safety requirements of railway signaling systems in mind. In order to adequate the protocol to the requirements of safety-critical applications and infrastructures, in particular of railway signaling systems, the protocol implements a set of reliability-oriented functionalities. This protocol provides reliable message transmission without unnoticed packet loss, thus offering a reliable transport service similar to the Transport Control Protocol (TCP). The procotol also implements channel quality monitoring via heartbeat messages and delivery guarantee within a particular time window. Reliability is also provided via the capabiity of using multiple transport channels for increased reliability. RaSTA is independent of the application protocol and can, as such, be used with other applications with similar requirements.

The RaSTA protocol sits between the application layer and the transport layer, in the context of the TCP/IP reference architecture. Two layers are defined here, one responsible for security and retransmission of messages, and the other for redundancy of the communication channels used for transporting data from applications. In the security layer, messages are verified against its integrity and passed to the retrainsmission layer to ensure a retransmission of the message if it has not acknowledged by the client. Thus, a checksum is appended to each message to implement integrity verifications. Other layer of the protocol is the redundancy layer, which is responsible for combining several physically separate transport channels into a logical transport channel, in order to increase reliability of the network connection and guarantee delivery in the event of a single channel failure.

We must note that, while the protocol implements security in terms of integrity, it suffers from major limitations in this respect. An integrity code (a MAC or Message Authenticaiton Code) is used, but the RC4 algorithm is used for this purpose, which is not considered to be suficiently safe anymore. Also, the protocol clearly lacks other security mechanisms, for example to provide confidentiality, support key management and data authentication. In this context of critical M2M railsafe applications, it Is also important to consider the conjugation of this protocol with the communications and security mechanisms provided by a 5G wireless communications infrastructure.

KISA/CISA (Communication infrastructure for security-related applications)

The KISA/CISUC communications protocol belongs in the context of a communication infrastructure for data security-related applications in the field of control and safety systems (LST) of a rail-mounted transport with the aid of an open transmission system. The protocol provides secure communications between modules via standard interfaces, as well as set of central management control procedures to set the state of secure communication channels in the infrastructure. The communications protocol defines a network security layer, which supports the transmission of data via a secure communications channel. Data must be transmitted via a "secured connection". The solution to be implemented must not interfere with the operation of the CCT. This protocol is currently being designed, and further access to its specifications in expected in the near future, in order to extend its analysis.

4.3 Architectures

Critical M2M applications and the Body Kit application

The architecture of the Bodykit follows an IoT architecture, using the TICK stack from Influxdata (https://www.influxdata.com/time-series-platform/). This stack uses a timeseries database (InfluxDB), an alert system (Kapacitor), a metric collecting mechanism (telegraf) and a dashboard (Chronograf) to verify the functionality of the TICK stack. The MQTT server (based on eMQTT) requires authentication and employs an ACL plugin to authenticate users and to manage the access control to topics. Figure 1 illustrates the general architecture of the BodyKit application

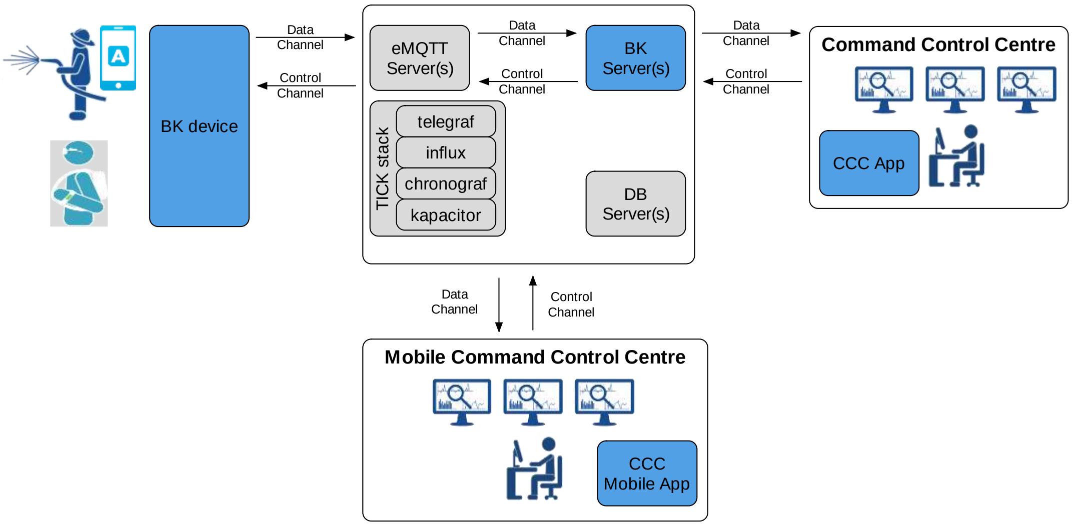

Figure 11 - General overview of BodyKit

In this architecture, two types of channels are considered, one for data (used to send data, alerts or other types of information flows), and the other for control purposes (to allow the management of devices). What follows is a descrition of the main components of the architecture illustrated in the previous figure.

4.3.1BK Device

There are two types do BK devices, in particular, the BodyKit Device that is a wearable platform with biosensors and environmental sensors and an application running in a mobile phone. The BodyKit device is the equipment that the users wear that transmits to the BodyKit Server the user sensors data (e.g. location, body position, and biosensors data) and the video/audio communication, through a public or private mobile network (4G). This device is composed of a wearable backpack, wearable sensors harnerss, video/audio glasses and a backpack interface (with na emergency button).

4.3.2MQTT Server(s)

The MQTT Server(s) employ a eMQTT solution (http://emqtt.io). The eMQTT is configured to force the authentication of users in publish and subscribe operations and also includes support for ACL of the different topics. Table 1 summarized some of the topics employed in the context of this broker.

Table 2 – Examples of data and control topics in MQTT

Topic Name	Description
tenantid/deviceid/data/<SENSOR_ID>	Topic for a specific/event
tenantid/deviceid/control/device tenantid/deviceid/control/server	Topic to manage a device: ● CRUD Topics ● Authentication /Permission ● Device Management (Confs, Status of device) ● Control Actions: WIPE, LOCK, MESSAGES, ACTIVATE GPS ● Manage Apps: List, retrieve apk, install/uninstall ● Alerts for CCC

4.3.3TICK Stack

As previous discussd, the TICK of the architecture relies on the Open Source solution from InfluxData. This stack provides a time series platform, designed from the ground up to handle metrics and events, and consists of the projects Telegraf, InfluxDB, Chronograf and Kapacitor.

4.3.4BK Servers

As part of the BodyKit architecture, the Servers manage the communication between the components of the service, as well as all other operations that are computationally heavy. These communications include authentication and authorization procedures, BKD configuration, data transmission (e.g. sensors, location, body position), video and audio streams and alert messages. With the received data, BK Server perform data aggregation, data inspection and data store. With data agregation data is aggregated per user and forwarded to the registered CCC (according to their authorization). As for data inspection, with this operation data is inspected to detect alert situations (e.g. location, vital signs). Finally, the data is stored in a database for off-line processing and history visualization. This component is currently implemented in the BodiKit architecture based in PostgreSQL.

4.3.5CCC App

The Command and Control Center (CCC) applications are stateless and do not store any information locally. All data required to support the CCC features is provided by the BKS (e.g. authentication and authorization, users list, users' data, history data). The CCC App is developed using the Ionic framework (https://ionicframework.com) to allow the development of applications in multiple Operating Systems.

Critical M2M applications for railway signaling systems

Critical M2M applications for the purpose of supporting railway signaling systems are very demanding in terms of requirements such as security, latency, integrity of communications, availability and reliability. All such requirements are clearly in line with the main goals of the 5G architecture, that is, the support of pervasive, high-performance and low-latency communications. In this area, any mechanisms designed to support security must, not only consider the previous requirements, but also be compliant with international railway satefy standards, namely EN50129/128 and EN50159 1-2 safety standards and requirements. It is in this context that we find of interest to analyze and consider the application of protocols being designed in the railway area, in particular RaSTA (*Rail Safe Transport Application*) and KISA/CISA (Communication infrastructure for security- related applications), as previously discussed.

4.4 The architecture General and regulatory requirements

The implementation of the previously discussed use cases raises many technical and research challenges. On the one hand, 5G technology must be developed along the technical requirements identified. On the other hand, it is also necessary to verify existing international standards and regulatory requirements which may influence or determine the development of the security mechanisms for such architectures. Also, it is important to guarantee that the 5G network is able to support the mechanisms required to cope with the strict functional and security requirements of the applications. In general, the usage of (5G) public networks to support the beforementioned critical applications brings many challenges in aspects such as network availability, response time, latency, resistance to radio interfeerences, security and protection against network intrusions, among others.

Security and functional requirements

We are able to identify the following security requirements we deem to be fundamental to support critical applications in 5G networks, particularly those previously discussed employing M2M communications, as well as situational anareness functionalities at the service of disaster recovery:

- Confidentiality: applications in 5G networks need to provide security against external eavesdroppers, either by using encryption communication mechanisms already avalable in the communications platfrom or, on the other end, by adopting approapriate mechanisms designed for the critical application at hand.

- Integrity: if for some applications confidentiality is required, for others integrity will also be important, and this situation hashing or digital signing mechanisms may be used to provide assurances in terms of the data communicating between entities of the system.

- Authenication (data, device and user): authentication is a transversal requirement, as it may apply to the authentication of the data being sent (data authenticaiton), of the user of the application (user authentication) or of the device (device authentication). Thus, in some applications it can be useful to consider authentication at more than one level.

- Non-repudiation: related with integrity and authentication is non-repudiation, which is related with mechanisms that can be used to ensure that the sender of a particular communication is not able to later deny having sent such data. In this context, the employment of digital signing mechanisms or of some for of hashing codes encrypted with unique keys which can be related with the sender can be explored.

- Privacy (user, location): privacy can be a requirement even in critical 5G network because, if on the one hand the application may have to share information about the user of the application or its location, on the other hand the acceptance of applications may be dependant on offering its users some form of control over the level of exposition of its private information. Thus, the control over privacy and over what data he or she shares should be in the hands of the user, and applications must be designed with this aspect in mind.

Other than security requirements, and in complement with security in the context of critical 5G networks, we need also to consider that critical applications must be designed considering also some critical functional requirements, as we proceed to identify:

- Resilience: resiliance of critical applications may be considered and guaranteed in terms of its architecture, thus considering the design of critical components of the infrastructure, and also of anomaly and intrusion detection and avoidance. Resiliance is thus a requirement which may be fulfilled both at the architectural level and also by the design of the applicaion itself.

- Latency: latency of communications is a critical aspect, particularly considering the transportation of alarms and security-related communications. In this context, applications may benefit from the availability of quality of service and latency-controlled communication mechanisms in the 5G architecture, for sending security-management data and to prioritize secure communications.

- Quality of service: Quality of Service (QoS) mechanisms are interrelated with latency control, and can thus provide the required support to address the need to transport critical security-related communications in a timely fashion, in the context of critical 5G applications.

- Reliability: reliable communications, as well as reliability in terms of the operation of the critical application, is certainly fundamental. In this context, reliability mechanisms should be applied to communications, to data and other functional aspects of the solution. As for the previous requirements, during the design of the application, its requirements should be conjugated with the mechanisms already provided by the 5G architecture itself.

- Efficiency: efficiency should be provided in terms of how well the application performs the tasks it was designed to. Certainly, there are different ways of measuring and evaluating effiency, among which we need to consider data communications efficiency, which may be measure as the capability to move the highest possible volume of accurate information through the network, and the higher the volume, the greater the resulting network's efficiency. Also, in this context the mechanisms and guaranteed of the 5G network should be explored and complemented by appropriate mechanisms designed in the context of the critical application.

- High availability: which should be, at least, with the availabiity targeted by the 5G architecture, of 99.999%.

- Coverage of the wireless communications infrastructure: the support of high-density and high-bandwidth devices in a given physical location or area.

We note that privacy is particularly relevant in the context of distributed monitoring and control applications as the analysed here. In general, the fact the 5G public networks will be used to support communications belonging in the context of critical applications, raises risks that must be certainly dealt with. Thus, challenges related with security arise in the context of communications, privacy and others, such as the defense of the infrastructure against external and internal attacks.

5 Task 3.1.4- (leader IT Univ. Aveiro)

Requirements analysis and mechanisms for reliable data mobility in M2M environments

This section addresses the role and impact that fundamental tools for enabling 5G networks, namely Software Defined Networks, Network Function Virtualisation and other network core/infrastructure enhancements, can have in supporting and enhancing services that have reliable and critical data requirements in machine-to-machine scenarios.

5.1 Analysis of scenarios

For a critical/reliable scenario we have considered the perspective of a ISP/Cloud Service Provider that is hired by a hypothetical industrial corporation to host critical Virtual Network Functions (VNF's). Due to the nature of these VNF's, they need to be handled as black boxes (that is, the cloud service provider cannot modify how the VNF operated, and can only interact with it via well specified and standardized APIs). Via this API, the industrial corporation needs to be able to send new versions of the VNF's to the ISP so that the older versions are automatically replaced. This approach is generically depicted in figure 1.

Since we are talking about a critical and reliable environment, the ISP has to ensure reliability and near zero-time between updates of the new version.

An example of such scenario is the provision of a network firewall in a critical environment. Due to the nature of the system where the firewall is placed (where it is important that the system is never suspended, even if for an upgrade of the function), there is the need for a more flexible way to allow new versions of the filter rules to be deployed in the firewall. It is important to consider that the nature of this scenario prevents that the new filter rules are inserted directly into the firewall, modifying and updating it: the black-box nature requirement of the VNF prevents that. As such, a new version of the firewall (with the new rules) needs to be deployed, and all the existing network flows redirected to it, before the old version of the firewall is disconnected and shut down.

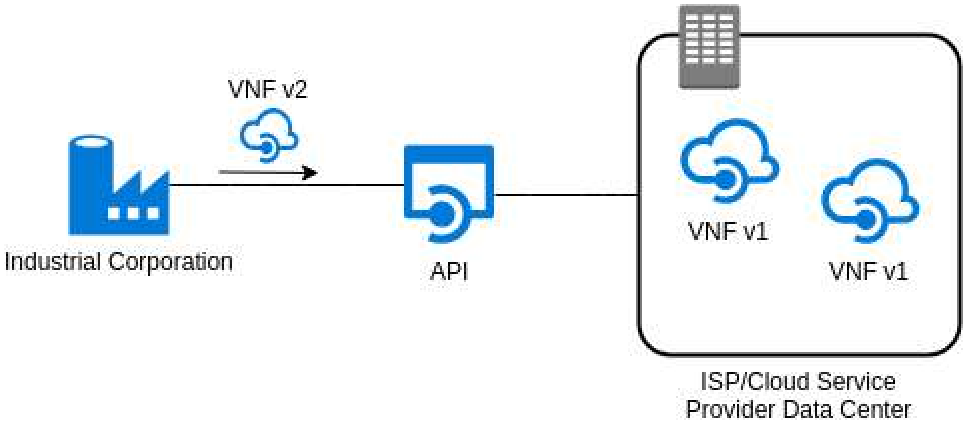

Figure 12 – llustrated scenario.

5.2 Technologies

Regarding technologies for enhancing critical and reliable data mobility, apart from New Radio (NR), Network Function Virtualization (NFV) and Software Defined Networks (SDN) will play a big part, particularly in the enablement of a virtualized form of network functions in the network operator’s core.

With the upcoming SDN networks, ensuring reliable connectivity is becoming more and more feasible. A reliable connectivity can be defined as the ability to recover quickly and smoothly from certain types of failures or overload. With SDN-based networks, the network control functions are decoupled from the data plane, therefore, a failure in the data plane may not impact the control functions. When used with the adequate mechanisms, this separation of planes allows us to rapidly recover an impacted session and achieve a reliable connectivity [1].

As for NFV, with the continuous development of cloud computing, network functions can be dettached from their specific hardware “boxes” and can be instantiated in the form of NFVs in the cloud or in standard hardware near the user. Switching from Physical Network Functions (PNF’s) to VNF’s allow us to create, scale and deploy network components whenever they are needed, all in accordance with the particular real-time traffic conditions optimizing the OPEX of the network [2]. Currently there are two major virtualization techniques for instantiating VNF’s, Virtual Machines (VMs) and Containers:

- Virtual Machines: This virtualization technique can be subdivided in two other categories:
  - Traditional VMs: These VMs are the most common virtualized platform in cloud services. A full system is virtualized, which has drawbacks like large memory footprints which make the instantiation of traditional VMs slow compared with other techniques.
  - Unikernels: This technique consists of a really tiny VM that runs directly on a hypervisor (such as KVM). Unikernels don’t require a Guest OS, which reduces the overhead significantly as the hypervisor doesn’t need to instantiate unnecessary things, making the system fully optimized to perform a specific task [3].
- Containers: Containers are an abstraction at the application layer that packages code and dependencies together. Multiple containers can run on the same machine and share the same Guest-OS with other containers, each running as isolated processes in user space [4]. As the OS is shared containers take a lower amount of storage (low overhead).

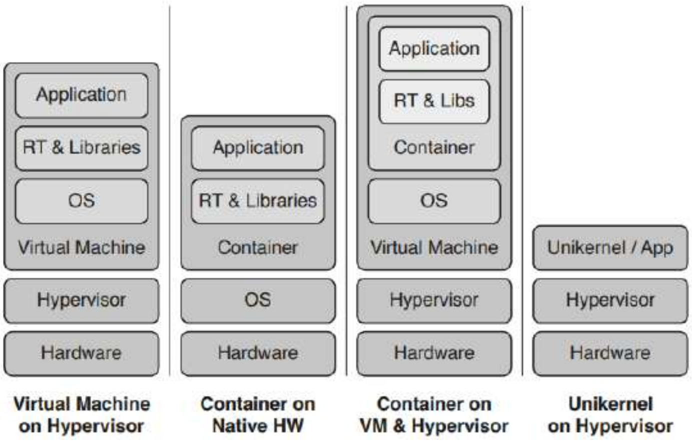

Figure 13 – Illustrated comparison of virtual machines, containers, containers within virtual machines and unikernels [3].

5.3 Architectures

To validate the scenario from 12.1, we propose a simulation with the following architectural components:

- APU Single Board Computer - A physical device running Ubuntu 17.10 Server. This server will run as a base layer (Hypervisor) for the virtualization of the critical network functions. It will play the role of the ISP/Cloud Service Provider Data Center.
- Terminal - A simple Ubuntu command line that will represent the API through which the industrial corporation will send the new versions of the VNF.
- VNF - Firewall - As the name implies this will be our critical VNF, it will be a virtual Firewall that only allows TCP traffic on port 80 and 443 to a certain whitelist of IP addresses.
  - This VNF will be instantiated as both a Docker Container [4] and an IncludeOS Unikernel [5]. Their performance will be compared to conclude which one better serves our critical and reliability needs.

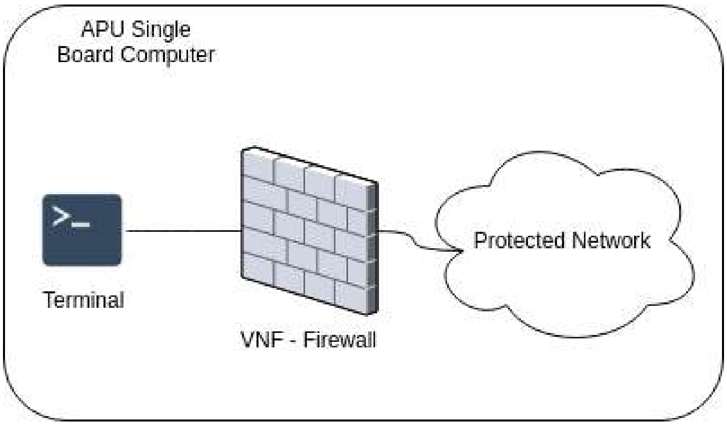

Figure 14 – Proposed Architecture.

We are focusing on a very specific case regarding critical communications and further efforts will be made to verify and realize its position in the remaining architecture of the project.

5.4 General and regulatory requirements

For identifying general requirements, 3GPP defined 6 use-case families to easily identify their needs [6] [7]:

- Higher reliability and lower latency:
  - characterized by a high system requirement for reliability and latency.
- Higher reliability, higher availability and lower latency:
  - characterized by high system requirements for reliability, availability, and latency - like industry control, drone connectivity, emergency cases, etc...
- Very low latency:
  - This use-case is described by applications and services with very low latency like real-time communications and tactile Internet.
- Higher accuracy positioning (HAP):
  - It is characterized by a high system requirement for positioning accuracy, where the location information is acquired quickly, is reliable and is available.
    - HAP with high speed moving (+60km/h): V2V communications with accuracy of ≤ 1m and two-way delay of 10 to 15 ms;

    - HAP with low speed moving (-30km/h): Locating vehicles/parking spots with accuracy of ≤ 1m;
    - HAP for low altitude UAV: Search for intruders, deliver packages, monitoring, mapping, etc…
- Higher availability.
  - This family is characterized by a high system requirement for availability. A typical case is the use of a secondary connection when a cellular network is congested or damaged.
- Mission Critical Services.
  - IIn this family are included communications that are critical and need a higher priority over other communications in the networks. Also use cases that provide coverage and services in remote or catastrophe-stricken areas:
    - Prioritized Communications;
    - Isolated Communications;
    - Protected Communications;
    - Guaranteed Communications;
    - Optimized Communications;
    - Supported Communications;

Nonetheless, it is important to assess the following considerations:

- These requirements were determined in an inception period for 5G research triggering;
- It is unclear the conditions in which such requirements need to be fulfilled;
- It is also unclear if the different requirements need to be provided in an isolated way or in an integrated way;
- Most of the requirements were being placed in specific radio mechanisms, and not considering the impact of the network core functions.

Considering this, at this time, this task will focus on the impact analysis that these virtualization procedures have at the core, and how they will influence such requirements in these kinds of scenarios. At a later point in time, alternate solutions (or mitigation approaches) can be proposed and provided.

6 Task 3.1.5 e 3.1.6 - (leader Ubiwhere)

Upgrading of the state of the art in Mobile Edge Computing (MEC) and definition of use cases of an intelligent video surveillance system (Ultra HD) in Ultra-High Mobility, using MEC

6.1 Mobile Edge Computing State of the art

Mobile Edge Computing (MEC) is the concept which aims to endow the Edge of the network with computing, storage and network resources. With the arise of the new network virtualisation techniques like Software Defined Networks (SDN), that allows the separation of the control plane from the data plane, and Network Function Virtualisation (NFV), which allows decoupling the network functions from dedicated hardware, it became easier to deploy small data centres within the network's base stations, which allows service deployments near the end user's location. The proximity between edge services and user equipment promotes a better user experience, lower latency and higher bandwidth, by reducing long distance backhaul, e.g., when a given user is consuming a video it's better effective if a cache is placed near the user than within a remote data centre in the Internet.

6.1.1Architecture

MEC's main goal is to build small data centres located at the edge of the network, also known as cloudlets, capable of empower the edge of computational resources and handle handover scenarios. These cloudlets will enable the deployment of mobile applications within the edge of the network meeting the low latency needs of 5G. The goal is to have multiple hosts across the edge of the network managed by a single platform. The MEC's high level architecture is shown in Figure 15.

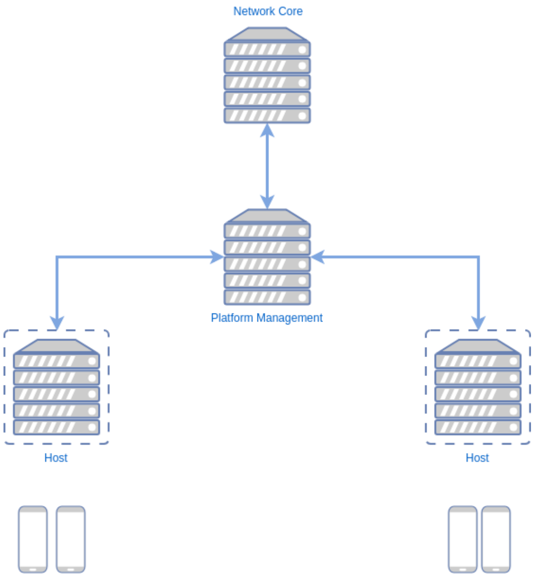

Figure 15 - MEC high level architecture

6.1.2ETSI MEC Architecture

The European Telecommunications Standards Institute (ETSI) has a Industry Specification Group (ISG) dedicated to MEC. This group has the goal to provide a specification to be commonly accepted with guidelines to follow to implement a MEC infrastructure. Figure 16 depicts the MEC reference architecture. It is composed by the following functional elements:

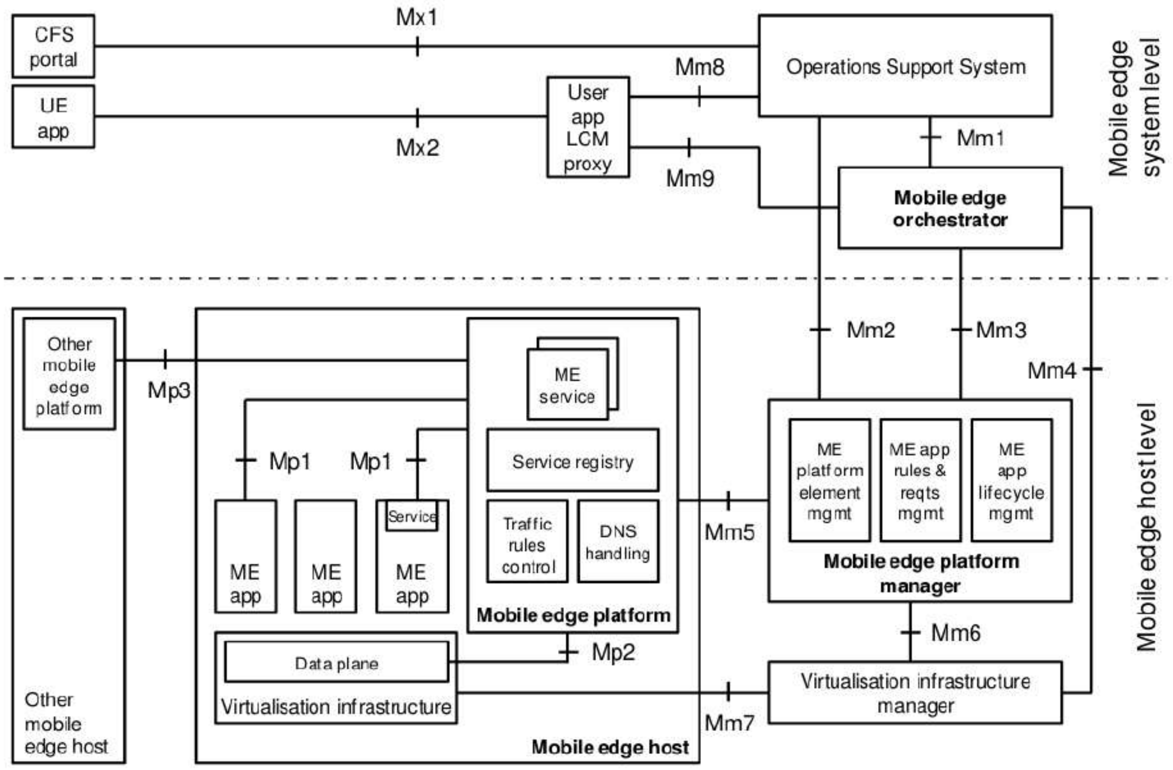

Figure 16 - MEC ETSI reference architecture [8]

- Mobile Edge host: Entity containing the mobile edge platform and the needed infrastructure to provide computing, storage and network resources to the edge of the network.

- Mobile Edge Platform: Set of functionalities needed to run mobile edge applications on its infrastructure, e.g., DNS or manage traffic rules. The mobile edge applications can discover, advertise and consume other edge services' resources within the Mobile Edge Platform.
- Mobile Edge Orchestrator: By knowing the allocated resources, the Mobile Edge Orchestrator has an overview of the mobile edge. It belongs to the Mobile Edge Orchestrator the responsibility to manage the applications by performing the following actions, (I) onboard, (II) validate, (III) instantiate, (IV) scale and (V) terminate. It is also part of the Orchestrator's responsibility to select the correct Mobile Edge Host to deploy a Mobile Edge Application.
- Mobile Edge Platform Manager: Bridges the Mobile Edge Orchestrator and the Mobile Edge Hosts. It contains the Mobile Edge platform management, Mobile Edge application rules management and Mobile Edge application lifecycle management

The interactions between each block within the reference architecture can be divided in three groups, (I) External Connection Entities (Mx), (II) Management Points (Mm) and (III) Platform Functionality (Mp). External Connection entities are responsible to interact with the user equipment or a Customer Facing Service portal to require a new mobile edge application or terminate a running one. Interactions related to management are Management Points, i.e., mobile edge lifecycle management, virtual resource management and application configuration. The Platform Functionality messages are related to the mobile edge platform, e.g., service registration and communication, communication between mobile edge platform and virtualisation infrastructure and inter mobile edge platform communication.

6.1.3ETSI MEC in a NVF environment

Due to the maturity of the ETSI MANO and given the focus on virtualizing completely the network's infrastructure, the ISG responsible for the MEC has defined a reference architecture to deploy the mobile edge as a VNF. With the ETSI MANO model in mind, not only the mobile edge platform is deployed as VNF, but also the mobile edge applications. Regarding the MEC's virtualized infrastructure is deployed as a NFVI and managed by the ETSI MANO VIM.

This new deployment environment introduces changes on the early presented reference architecture, Figure 16. Figure 17 shows the reference architecture that enables MEC deployment in an NFV environment and the mapping between MEC's reference architecture, and ETSI MANO architecture.

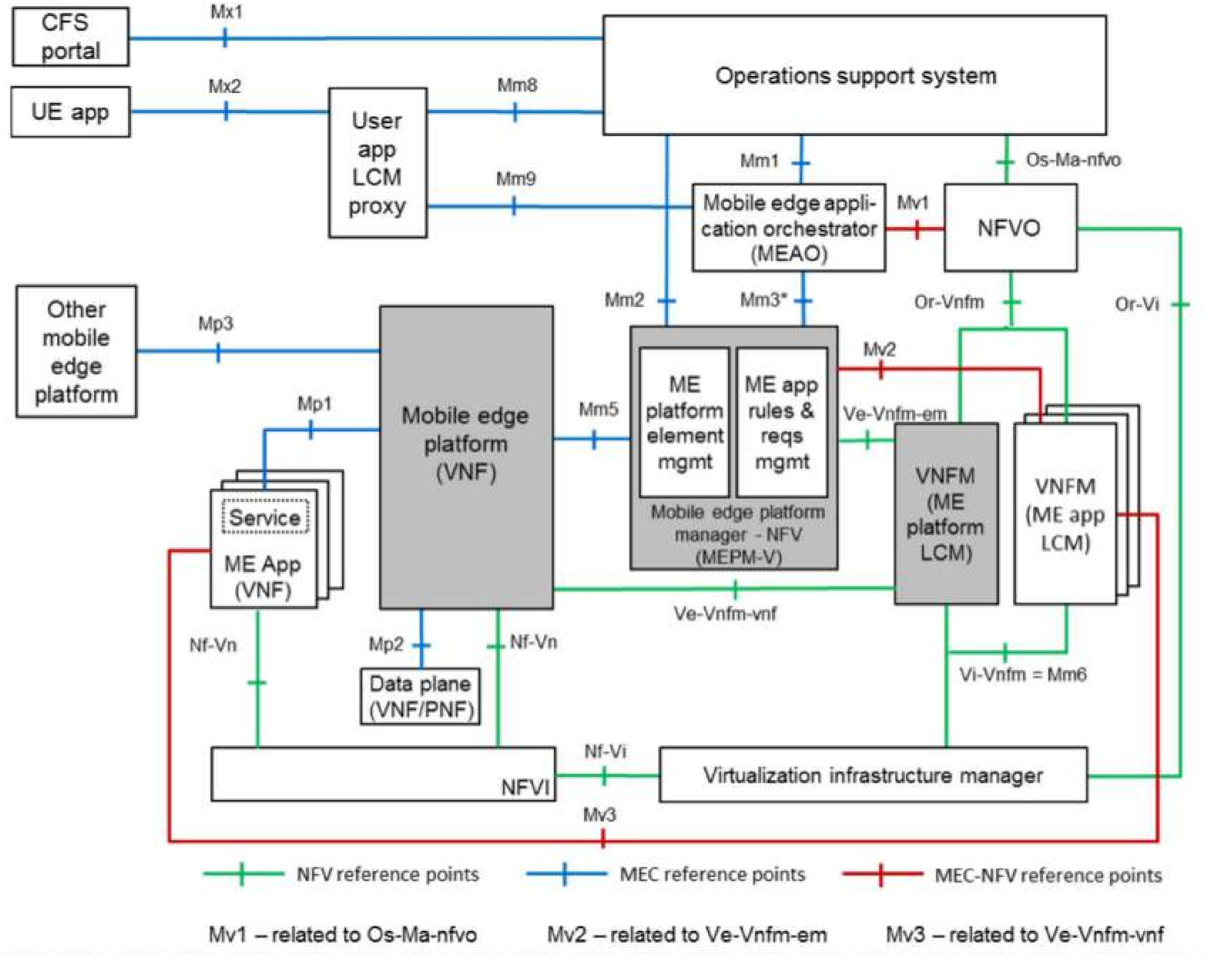

Figure 17 - MEC reference architecture in NFV environment [9]

The main concerns on running the MEC system on a NFV environment is the mobile application management. The Mobile Edge Platform delegates the mobile edge application lifecycle management to one or more VNFMs, the Mobile Edge Orchestrator is now only a Mobile Edge Application Orchestrator which uses the NFVO resources, the Mobile Edge Platform and the Mobile Edge Applications are now VNFs.

6.1.4MEC Use Cases

MEC main goals of enabling low latency services, increase bandwidth and user experience and the proximity to the end users, make possible the birth of new market opportunities in areas such video analytics, Internet of Things (IoT) or caching. In these different areas, ETSI defined a set of scenarios that can be targeted by MEC services, here are presented some of these scenarios [10]:

- Video stream analysis: A monitoring system for plate recognition. Instead of having the video processing within the cameras, which increases the monitoring system costs, or having the video processing on the network's core, which implies the transmission of high data streams, the analysis can be performed on the mobile edge and only relevant information is sent to a central processing unit.
- Connected vehicles: The developments in the automobile industry have led to the vehicles acquiring the capability to connect to the mobile network. This enhances the possibility of having inter-communication between vehicles promoting safety, road hazards and reduces traffic congestion. Once again, the cloudlets and low latency offered by MEC are key characteristics to build such inter-connectivity without arming the regular traffic flow.

- IoT gateway service: IoT consist on a set of devices connected to the network, each one with specific messages for a specialised task. Despite the small messages, increasing amount of these devices will lead to large amount of traffic generated. Since these equipments usually require low latency environments the MEC can create a gateway that can aggregate these services and perform analytics on the collected data.

6.2 Intelligent video surveillance system (Ultra HD) in Ultra-High Mobility, using MEC

6.2.1Analysis of scenarios

According to portuguese Institute for Mobility and Transport, between 2006 and 2015, 801 people were hitted by a train in Portugal. In less than 10 years, 492 suicides with the remaining 309 deaths considered accidents. Most of the accidents occurred in a railroad crossing [11], in 2017 alone, 6 people died in accidents of this nature [12]. According to Infraestruturas de Portugal, in 2013 there were 807 railroad crossings, of which 245 without guard [13]. Situations like railway accidents or the need to stop a train, are events that entail large costs for the entity responsible for the rail transport, which in Portugal is Comboios de Portugal (CP). Following a CP report, rail accidents are estimated to have caused losses of 19,62 millions [14], plus the cost of the loss of life and suffering for all of the affected parties, including train conductors that sometimes exhibit PTSD symptoms after being involved in such an event.

The situation above clearly shows the need to take action and create safety mechanisms that aim to reduce the probability of the occurrence of such accidents, and even increase the security of some dark points of the railway system, allowing the generation of alerts when potentially dangerous situations are detected.

In Portugal, there are railroad crossings that are (I) fully automated, without human intervention the railroad crossing opens and closes automatically, (II) guarded, where a person opens or closes the railroad cross when a train is arriving, and (III) railroad crossings without any kind of monitoring [13].

Despite the fact the number of accidents involving railroad crossings are decreasing, it's believed that more should be done to reduce or even completely abolish these kind of accidents [14]. By monitoring not only the railroad crossings, but also dangerous places in the railroad were accidents usually occur, it's possible to provide the means for someone to take an action in order to avoid an accident, by calling help or as a last resort stop the train.

There are advanced surveillance systems, using 4k resolution cameras with processing and storage capabilities that are able to (I) detect objects and (II) send its images to a central unit through IP connectivity [15]. Most of these advanced cameras use technology outside of the visible spectrum, by means of laser reflection, or thermal sensors. The problem with these kind of advanced surveillance solutions is the price and maintenance cost which, due to the decrease of the number of railroad crossing accidents, would be hard to justify.

6.2.2Architectures

With the arise of 5G technology as a Mobile Edge Computing (MEC) enabler, it's possible to design a surveillance system which takes advantage of the network's edge computational resources to process images from the cameras, targeting the detection of strange objects within a given area. This feature allows the design of a cheaper surveillance solution to monitor the railroad crossings. The main goal is to provide a live video feed of the railroad crossroad which a train is approaching allowing the driver to check if any hazard is present in the crossing railroad section. Furthermore, and in order to assist the driver, MEC resources will not only be used to provide video feeds to the upcoming trains but also to process in real time these videos in order to autonomously detect if any hazard is in fact occurring and a safe passage is jeopardized. An event driven surveillance solution will therefore be implemented, leveraging on the usage of MEC's computational resources to analyse a video stream of a given area and alert upcoming train drivers if a strange object is present on the railroad. However since this solution is not one hundred percent reliable, just like previously mentioned, the driver will always have access to a live feed from the camera monitoring the railroad thus the ultimate decision to stop or cross the passage will be made by the train driver based both on the existence or non existence of an alert and the real life video feed,~~.~~

Figure 18, shows a possible architecture for this solution composed by four main elements, (I) camera, to monitor a given area, (II) processing unit, placed on a mobile edge host, responsible to process incoming camera data and find strange objects, (III) a central unit, to compile multiple processing units information for audit, long time video storage and (IV) user equipment, to which the system will send alerts and live streaming.

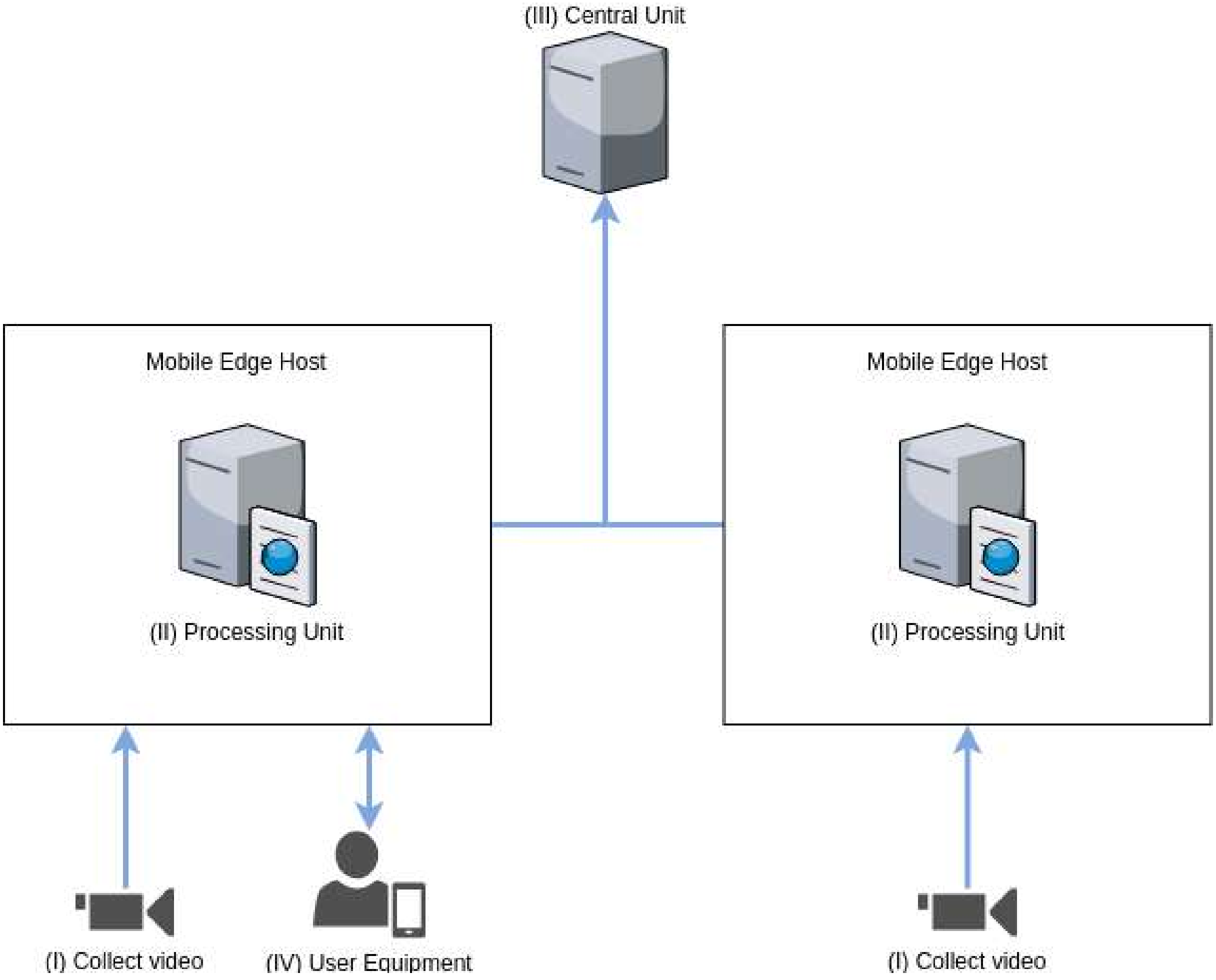

Figure 18 - System architecture

The system's behaviour is divided in two stages, (I) collection and detection phase, related to the capture of video within a given area and (II) notification phase, which consists in notifying connected devices about a strange object near the camera's area.

Figure 19 shows the interaction between the camera, processing unit, central unit and the main responsibilities of each one in the collection and detection stages. (I) The camera obtains information on the surroundings, monitoring a given area, (II) through IP connectivity the camera sends the information to the processing unit within the nearest mobile edge host, (III) the processing unit receives the images and processes it attempting to find strange objects in the images, (IV) if an object is detected the images are recorded within the processing unit and (V) an event is raised for the central unit.

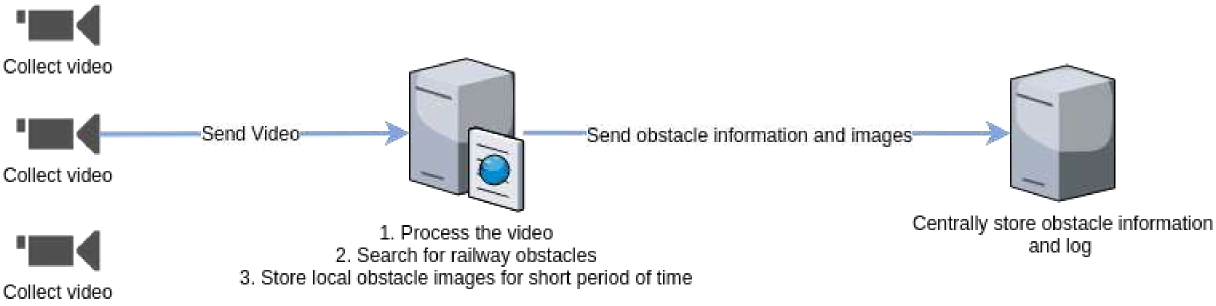
Collect video
Collect video
Collect video
Send Video
Send obstacle information and images
1. Process the video
2. Search for railway obstacles
3. Store local obstacle images for short period of time
Centrally store obstacle information and log

Figure 19 - Video processing components

The notification stage only involves the user equipment and the processing unit, Figure 20. When a user equipment is registered in a mobile edge host it will receive (I) live feed of a given camera nearb and, (II) live notifications if an object is detected. All the means to audit the information sent to the train driver is logged in the central unit.

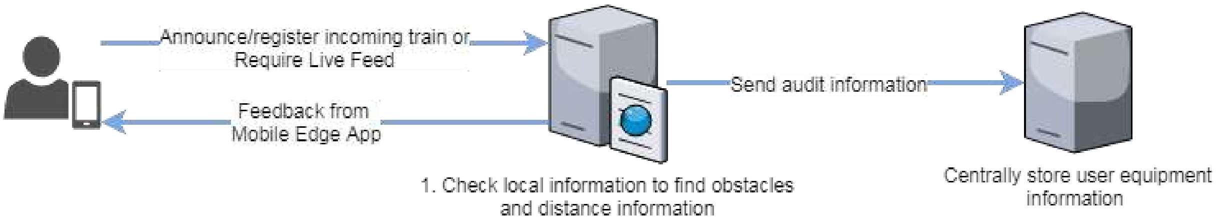
Announce/register incoming train or Require Live Feed
Feedback from Mobile Edge App
Send audit information
1. Check local information to find obstacles and distance information
Centrally store user equipment information

Figure 20 - User equipment interaction

The upcoming 5G technology using MEC infrastructure with promised low latency service response are the key that enable the service, allowing the fast video processing and live feed within the network's edge. The system is intended to start with regular IP cameras, however the design is modular to allow the adaptation of other technologies like Near Infrared cameras or LIDAR sensors as those technologies become economically viable or where the visibility conditions may require special capabilities.

6.2.3General and regulatory requirements

Dealing with such sensitive scenarios, the video's processing time and delay must be carefully handled, guaranteeing low latency and high quality video. The system must be compliant with current Video surveillance standards, such as IEC 62676 - Video surveillance systems for use in security application. Since the presented use case deals with high speed vehicles it's mandatory to guarantee that the Doppler Effect or handover do not compromise the received video.

The infrastructure must be ready to handle both TCP and UDP traffic. TCP to announce a new user,, UDP for video transmission.

The equipment needed to validate this scenario is divided in two groups, train equipment and processing e equipment. The train equipment requires a 5G router and antenna and a console to view the image, on the processing equipment side it's also required the 5G equipment an IP camera and the processing power to find obstacles on the images and the central unit.

7 Task 3.1.7 - (leader Onesource)

Definition of Use Cases and Requirements for Bodykit

This section presents the use cases and the respetive requirements associated with BodyKit.

7.1 Analysis of scenarios

BodyKit is employed in Mission Critical scenarios, perfomed by Public Protection Disaster Relief (PPDR) organizations. The operations of such organizations are several, but in a generic perspective three scenarios can be devised, as summarized in Table 3.

Table 3 – Possible PPDR scenarios

Scenario	**Description**	**PPDR Operational requirements**[1]
City Security	Considers the management of public disorder events (protests that escalate to full-scale riots) with permantly deployed PPDR infrastructure in city locations. Secure communications for voice, video and data applications services are required.	Connection to CCTV Location services (vehicles and persons) Direct Mode Operation (DMO) Interoperability between organizations Wearable sensors Pre-emption and network prioritisation
Temporary Protection	Considers the management of a public protection in crowded events with the combination of permanent and temporaty PPDR infrastructure.	Connection to CCTV Location services Remote control of drones Control of jamming devices WiFi support Video streaming Database access Wearable sensors
Forest Fire Rescue	Forest fire events, which are usually cross-district and require the collaboration of fire brigades from multiple locations, as	Group Calls, Group Video Location services

[1] The PPDR Operational requirements consider the key features that are crucial for PPDR to perform their mission in the related use case.

	well as multiple public security ans safety organizations.	Direct Mode operation (DMO) Video Streaming Wearable sensors

The BodyKit appears associated with the wearable sensors, location services and communication operational requirements.

The 4G networks include already some support for critical missions [16], which usually is only found on Public Mobile Radio networks like TETRA and TETRAPOL. The support in LTE include support for group communications (R13 – GCSE), proximity services (R13 – ProSE) for device to device (D2D) communications, Mission Critical Push to Talk (MCPTT), among others.

The scenario herein defined includes support for IoT devices which can be used by fireman or other agents. In particular, the BodyKit allows collection of data from biosensors, environmental sensors and allow the communications of voice and video with Command Control Centres (CCC). One of the relevant functionalities included in the BodyKit is the safety monitorization of PPDR agents, where alarms regarding safety are sent to the CCC. Such alarms can include the detection of man-down events (e.g. falls of PPDR agents), or even the presence of adverse and dangerous atmospheric environmental conditions, like high temperatures.

7.2 Technologies

The tecnologies associated with the BodyKit scenarios include Public Mobile Radio (PMR) technologies, such as TETRA, TETRAPOL. These technologies have a high reputation for mission critical services, mainly due to their resilience and security support. For instance, all the communications over-the-air are encrypted.

The evolution of 4G networks, and in 5G networks aim to support mission critical services, for instance, MCPTT, traffic prioritisation, among other features.

The NEF component (PPS2) allows the configuration of prioritised flows like for the safety alarms. These flows must have a fixed allocated bandwidth and must be prioritized over other flows, since they contain information that is crucial to the safety and security of PPDR agents. A full situational awareness is important in CCCs. As such, commanders and operators in the CCCs may request pictures, photos, or even videos from the field. Such kind of information allows more informed operational and tactical decisions.

The QoS configuration is fundamental to guarantee the diverse operations of PPDR.

7.3 Architectures

The overall architecture of the use case where BodyKit is employed is documented in Figure 21.

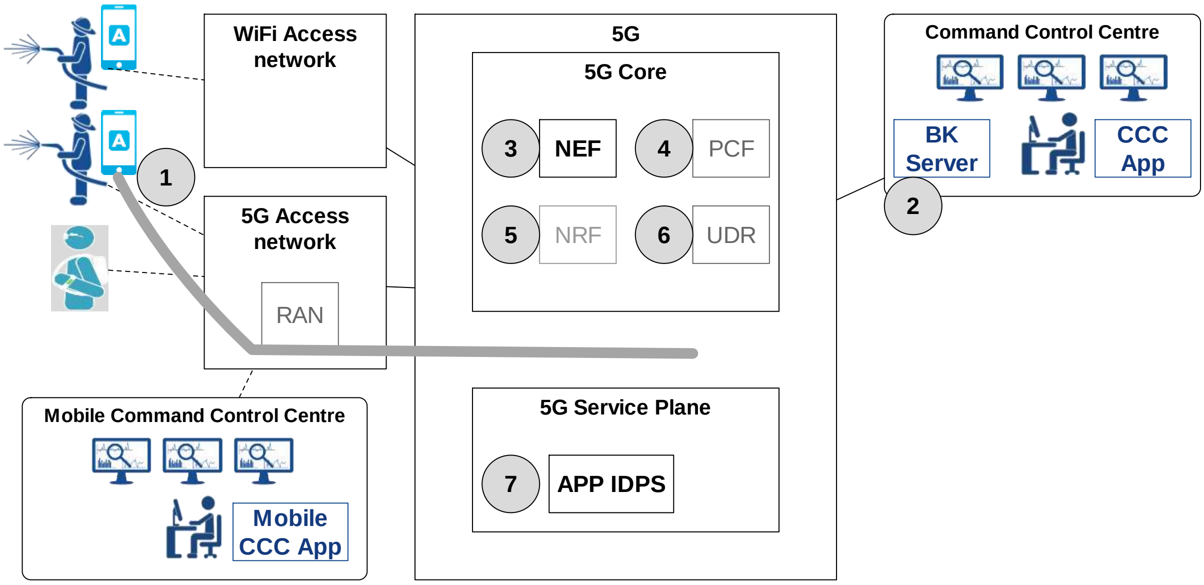

Figure 21 - BodyKit use-case scenario

This scenario includes the inicial deployment of the BodyKit (BK) components, namely the BK Server in Command Control Centre, which are connected to the 5G network.

As per the scenario figure, the steps involved in this scenario are as follows:

1. IoT devices (BodyKit) start and conclude with success all the procedures of connecting to the network (network attach). In this phase, they receive a default flow with the default levels of QoS configured for the PDU sessions.
2. The BK Server detects the presence of new devices in the network (through the authentication of devices and users in the BodyKit system). For each authenticated device, the BK Server asks NRF for the endpoint of NEF.
3. The BK Server, with the information of the NEF endpoint, starts the negotiation with NEF to assure the configuration of three types of flows by default to each device: 1-flow for priority data (i.e. alarms), 2-flows for communications in real-time of voice and video; 3-flow for sensor data.
4. The NEF component receives information of the PCF endpoint responsible for the network slice where NEF is deployed, and responsible for the PDU session where the device is attached. This phase is important to allow the configuration of the QoS requirements.
5. NEF communicates the requirements received to the responsible PCF so that QoS flows are properly configured in the respective PDU sessions of the devices. PCF exposes an interface that enables the UE or network to explicitly request a certain level of QoS for the service session in which it is involved. From the perspective of PCF, the following procedure takes place
    a. PCF determines the policy to be applied in the network, due to the new requirements of the service.
    b. PCF installs policies on the necessary network elements for differential QoS control of the data stream of the service session.
    c. PCF confirms to NEF the result of the operation (success or failure).
6. The flows are configured in the 5G network. The devices receive a notification that the QoS configuration is finalized. Such notification is sent by AMF.

7. The BodyKit periodically sends probes to APP IDPS (PPS2) in order to allow security analysis to detect possible security threats.

After the configuration of the three types of flows, the device can start using the respective flows. The prioritized flow is employed for alarms.

The disposal of the QoS configuration is performed at request (for instance, at the end of missions), from the BodyKit device upon defined thresholds of keepalive mechanisms, or upon logout procedures. The removal of the priority flows can be subject to network policies.

7.4 General and regulatory requirements

The requirements associated with this scenario includes:

1. 5G core network is deployed and is functional.
2. The 5G service plane is functional and includes services to enhance the security of BK devices.
3. CCC have a stable and performant connection to the 5G network.
4. Bodykit Devices are properly configured to have access to the 5G network.
5. Mobile CCC Applications of Bodykit are properly configured to have access to the 5G network (ideally configured with priority flows settings).
6. Bodykit Devices are able to reach the Bodykit Server, independently of the configured flows.
7. The Bodykit Devices are able to detect the different types of flows (e.g., alarms) and trigger the respective configuration actions on the 5G infrastructures through NEF.
8. Support of a control channel of the 5G infrastructure for security management purposes, e.g. via data or control plan.

The security requirements of the solution include:

1. Confidentiality, integrity and authenticity of all communications between biosensors and the BodyKit application
2. Confidentiality, integrity and authenticity of all communications between environmental sensors and the BodyKit application
3. Secure provisioning of keying materials and other security-related data in all sensors, as required for the secure bootstrap of the BodyKit application
4. Detection of internal and external security-related anomalies
5. Assurance from the network, in terms of QoS (e.g. latency, guaranteed deliveries), of delivery of security-related messages (management and alarms)

The BK Server uses APP IDPS to enable the detection and mitigation of malicious activities. Other mechanisms that will be required are:

1. Mechanisms for the application of security to messages exchanged between bio and environments sensors and the BodyKit application, in order to guarantee confidentiality, integrity and authenticity of the communications. Different low-energy communication technologies and sensors should be supported by the designed mechanisms.

2. Mechanisms related with the provisioning of security credentials and keying material in the sensors used by BodyKit.
3. Mechanisms related with the detection of internal and external attacks against the security of the application, the employed sensors and the exchanged communications. Attack and anomaly detection may be distributed and be either local (generating alarms with the help of the sensing devices employed by BodyKit) or with the help of the APP IDPS.
4. Mechanisms for the establishment of a priority flow for supporting security-related operations (security provisioning, key management, APP IDPS data and alarms).
5. Mechanisms for the integration in BodyKit of environmental sensors running over alternative low-range and low-energy communication protocols, in particular ZigBee and IEEE 802.15.4.
6. Mechanisms to support mutual authentiation and authorization between sensors and the BodyKit application, particularly in the context of the usage of its mobile (app) component.

8 Conclusions

8.1 Main Conclusions

This version describes all the achieved results in the scope of the preliminaires studies Activity, wich includes the task T3.1.1 to T3.1.7. Since the activity were postponed to 30/10/2017, mainly to consolidate T3.1.3 and T.3.1.4 tasks, a final version of this reported will available, after all tasks of the activity will be concluded (30/10/2108). As previously described, this activity, involving state-of-the-art update , technology analisys, risk and requirements analisys and also use cases, is very important for the success of the next activities and is reported in this Deliverable.

9 References

[1] S. B. Hadj Said, B. Cousin and S. Lahoud, "Software defined networking (SDN) for reliable user connectivity in 5G networks," *2017 IEEE Conference on Network Softwarization (NetSoft)*, Bologna, 2017, pp. 1-5.

[2] T. Taleb *et al*., "EASE: EPC as a service to ease mobile core network deployment over cloud," in *IEEE Network*, vol. 29, no. 2, pp. 78-88, March-April 2015.

[3] Plauth, M., Feinbube, L., & Polze, A. (2017). A Performance Evaluation of Lightweight Approaches to Virtualization.

[4] Docker. https://www.docker.com/what-docker

[5] IncludeOS. http://www.includeos.org

[6] 3GPP, "FS SMARTER - Critical Communications, TR 22.862"

[7] NGMN, "5G White Paper", https://ngmn.org/5g-white-paper/5g-white-paper.html

[8] *ETSI GS MEC 003,* 2016.

[9] *ETSI GR MEC 017,* 2018.

[10] *ETSI GS MEC-IEG 004,* 2015.

[11] J. Almeida, "CP: Maquinistas e revisores querem ajuda para lidar com suicídios na ferrovia," 24 07 2017. [Online]. Available: http://www.jornaleconomico.sapo.pt/noticias/cp-maquinistas-e-revisores-querem-ajuda-para-lidar-com-suicidios-na-ferrovia-189437. [Acedido em 15 05 2018].

[12] Lusa, "Seis pessoas morreram em acidentes em passagens de nível no ano de 2017," 21 04 2018. [Online]. Available: https://www.cmjornal.pt/portugal/detalhe/seis-pessoas-morreram-em-2017-em-acidentes-em-passagens-de-nivel. [Acedido em 15 05 2018].

[13] Infraestruturas de Portugal, "Indicadores," [Online]. Available: http://passagensdenivel.infraestruturasdeportugal.pt/indicadores/dados.html. [Acedido em 15 05 2018].

[14] N. Faria, "Maquinistas e revisores reclamam ajuda para enfrentar suicídios na ferrovia," 23 07 2017. [Online]. Available: https://www.publico.pt/2017/07/23/sociedade/noticia/maquinistas-e-revisores-reclamam-ajuda-para-enfrentar-suicidios-na-ferrovia-1779752. [Acedido em 15 05 2018].

[15] RankRed, “12 Advanced Surveillance Technologies For High Security,” 09 01 2015. [Online]. Available: https://www.rankred.com/12-advanced-surveillance-technologies-high-security/. [Acedido em 15 05 2018].

[16] H. Marques, “Next Generation Communication Systems for PPDR - The SALUS Perspective,” em *Public Safety Network Series*, Wiley-ISTE.

[17] someone, “some article name,” 2018.

Authors list

Promoter	Author
Altice Labs, S.A.	Francisco Fontes, Jacinto Vieira
EFACEC Eng. Sist. S.A.	Luis Roboredo, Paulo Paixão
EFACEC Energia S.A.	Alberto Rodrigues, Fernando Gomes
Onesource	André Gomes, Bruno Sousa, Luís Cordeiro, Pedro Silva, Vitor Fonseca
PDM&FC	Francisco Damião
Ubiwhere	Tiago Batista, Ricardo Preto
Univ. de Coimbra	Jorge Granjal, Miguel Freitas
IT	Daniel Corujo, João Barraca Filipe, Asad Rehman

Versions history

Version	Date	Description
0.1	11-06-2018	First version including all partners' contributions.
0.2	21-06-2018	Version including sumaries and conclusions
1.0	28-06-2018	Final version