# “MOBILIZADOR 5G”

*Components and services for 5G networks*

Project nº 24539

## Deliverable D3.2 and D 3.3

## Use cases, requirements *and solutions architecture for* M2M critical communications

## *Relatório D3.2 e D3.3*

## *Casos de uso, requisitos e arquitetura de soluções para comunicações críticas M2M*

| | |
|---|---|
| PPS | **PPS 3** |
| Activity | **A3.2 – Technical Specifications** |
| Dissemination level | **Public** |
| Date | **December 2019** |
| Version | **2.0** |

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 documenta a atividade de Especificação Técnica (A3.2) do PPS3, em particular no que respeita às tarefas de identificação de casos de uso, requisitos e arquitetura, inerentes às várias linhas de produto a desenvolver. Este relatório resulta de uma fusão dos *deliverables* D3.2 e D3.3 tendo como título, “Casos de uso, requisitos e arquitetura de soluções para comunicações críticas M2M”.

Para melhor interpretação do documento, as primeiras secções, que envolvem as tarefas T3.2.2, T3.2.3, T3.2.4, T3.2.6, T3.2.7, T3.2.8, T3.2.9, T3.2.10, T3.2.11 e T3.2.12 são dedicadas aos casos de uso e requisitos e as finais, que envolvem as tarefas T3.2.1, T3.2.5, T3.2.13 e T3.2.14, abordam questões associadas à arquitetura das soluções.

# Executive Summary

This report documents the PPS3 Technical Specification (A3.2) activity, in particular related the use cases identification, requirements and architecture to be carry out in the several product lines to be developed. This report is achieved from a merger of deliverables D3.2 and D3.3 under the heading, “Use Cases, Requirements and Solution Architecture for M2M Critical Communications”. For a better interpretation of the document, the first sections, which involve tasks T3.2.2, T3.2.3, T3.2.4, T3.2.6, T3.2.7, T3.2.8, T3.2.9, T3.2.10, T3.2.11, and T3.2.12 are dedicated to the use cases and requirements, and the final ones, which involve tasks T3.2.1, T3.2.5, T3.2.13, and T3.2.14, address issues associated with solution architecture.

# Table of Contents

# List of Figures

# List of Tables

# Glossary

| | |
|---|---|
| **5GC** | 5G Core |
| **AAA** | Authentication, Authorization and Accounting |
| **AF** | Application Function |
| **AI** | Artificial Intelligence |
| BKD | BodyKit Device |
| **CAPEX** | CAPital EXpenditure |
| **CPE** | Customer Premises Equipment |
| **D2D** | Device To Device |
| **DA** | Distribution Automation |
| **DAS** | Distribution Automation System |
| **DDNS** | Dynamic Domain Name System |
| **DG** | Distributed Generation |
| **DGA** | Distribution Grid Area |
| **DMS** | Distribution Management System |
| **DNS** | Denial of Service |
| **ENS** | Energy Not Supplied |
| **FDIR** | Fault Detection, Isolation, and Restoration |
| **GOOSE** | Generic Object Oriented Substation Events |
| **ICT** | Information and Communication Technologies |
| **IED** | Intelligent Electronic Devices |
| **IDPS** | Intrusion Detect and Prevention Systems |
| **M2M** | Machine-to-Machine |
| **MAIFI** | Momentary Average Interruption Frequency Index |
| **MEC** | Multi access Edge Computing |
| **MD4** | Message-Digest algorithm (hash algorithm) |
| **MV** | Medium Voltage |
| **N.C.** | Normally Closed |
| **NF** | Network Function |
| **N.O.** | Normally Open |
| **OMS** | Outage Management System |
| **QoS** | Quality of Service |
| **RASTA** | Rail Safe Transport Application |
| **RES** | Renewable Energy Resources |
| **R-GOOSE** | Routable-GOOSE |
| **RMU** | Ring Main Unit |

**RTU** Remote Terminal Unit

**SAIDI** System Average Interruption Duration Index

**SAIFI** System Average Interruption Frequency Inde

**SAS** Substation Automation System

**SCADA** Supervisory Control and Data Acquisition

**SDN** Software Defined Networking

**SGAM** Smart Grid Architecture Model

**SSC** Smart Substation Controller

**SSL/TLS** Secure Sockets Layer/Transport Layer Security

**uRLLC** ultra-Reliable Low Latency Communications

**V2X** Vehicle to Device/Vehicle/other

**VNF** Virtual Network Function

**V-T** Voltage-Time

**Not Applicable** (NA)

# 1 Introduction

.

During the A3.2 activity (“Technical Specifications”), huge efforts have been conducted regarding the specification of 5G critical M2M communication systems and sub-systems focused in the following key issues: i) Scenarios ii) Use cases iii) requirements and iv) and architectures. According to the activity task plan, in the following sections the obtained results are presented. For each task (T3.2.1 to T3.2.14), the specific partner in charge (task leader) presents the results, aggregated in the following sections: analysis of scenarios, requirements, technologies to be used, and solutions architectures.

# 2 Task 3.2.2

## *T3.2.2 Specification of the MV network real-time protection and distributed automation use case*

This task is led by EFACEC Energia

The present use case comprises two complementary scenarios centered on fully-distributed self-healing and power system protection coordination for Medium Voltage (MV) electric power distribution grids. The proposed algorithms are crucial components of some of the state-of-the art Fault Detection, Isolation, and service Restoration (FDIR) solutions described in [1]. Both scenarios rely on IEC 61850 Routable-Generic Object-Oriented Substation Events (R-GOOSE) peer-to-peer communications over 5G for Intelligent Electronic Device (IED) coordination.

Regardless of being integrated in self-healing solutions or other distribution automation applications, power system protection and control IEDs must be accessible for remote monitoring, control, diagnostic, and engineering operations. Therefore, although this is not the focus of the use case, the following non-time-critical communications are also present throughout both scenarios:

- IEC 61850 Manufacturing Message Specification (MMS), for monitoring and control;
- Access to the IEDs' embedded web server for diagnostic (HTTP);
- Engineering operations and remote diagnostic using the Efacec Automation Studio engineering tool (proprietary protocols).

## 2.1 Analysis of scenarios

The use case considers a power distribution grid open ring topology which includes two MV feeders connected by a Normally Open (N.O.) point, as represented in Figure 1. The considered system includes two substations, each with a protection relay[1] controlling a circuit breaker, and three field devices[2], each controlling a recloser[3]. One of the latter devices will be setup as a N.O. point, all others as Normally Closed (N.C.) points.

The protection and control IEDs considered for the use case are able to detect power system faults (*i.e.*, short-circuits) in a few milliseconds by analysing power system quantities, such as line current and voltage levels. These quantities are measured by current and voltage sensors connected to the power lines. The IEDs also control switchgear capable of interrupting very high levels of current (*e.g.*, circuit breakers or reclosers). Depending on their position in the topology and on the location of a fault, IEDs may issue a circuit breaker/recloser open command when a fault is detected, in order to de-energize part of the power grid and clear the fault.

[1] A protection relay is a type of IED. In real-world applications, these IEDs are installed inside substations.

[2] The referred field devices are protection and control IEDs, which, in real-world applications, are installed in cabinets attached to electricity poles, typically in remote rural areas.

[3] A recloser is a type of circuit-breaker, optimized for high-speed reclosing operations. It is typically pole-mounted.

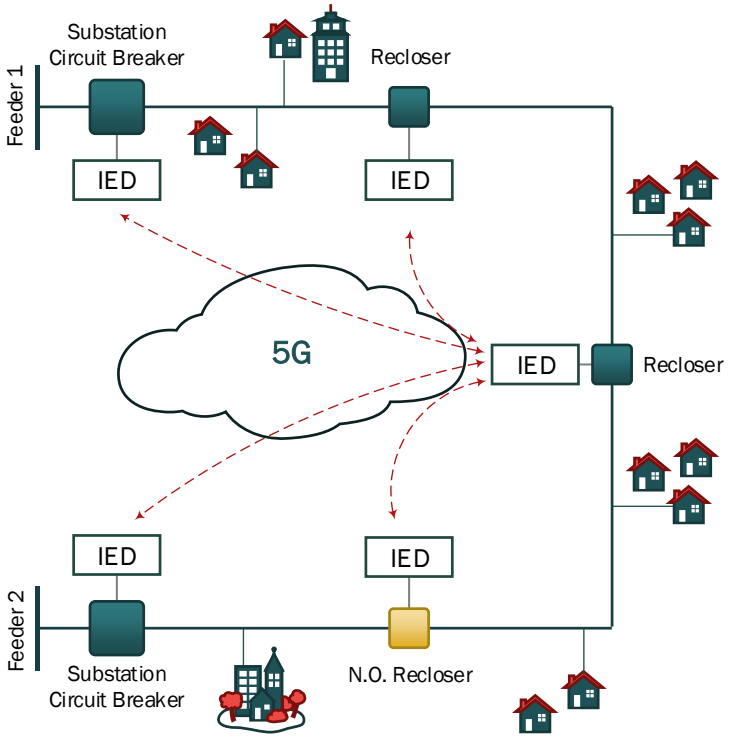



**Figure 1. Power grid topology considered for the use case scenarios.**

Although the use case tests and validation will take place in a laboratory environment, it is relevant to take into consideration that in real-world applications, the referred protection and control IEDs, are typically installed miles apart from one another, often in remote rural areas in which communication network coverage is currently sub-optimal.

## Scenario **1: High-speed selective blocking**

> *This scenario rests on a very critical aspect of power system protection, which is selectivity. The purpose of selectivity is to ensure that, when a fault occurs, only the minimum possible section of the power grid is de-energized. This requires some form of coordination between protection devices, since faults may be detected by all upstream devices, and selectivity dictates that a fault must be cleared by the closest device (i.e., the IED immediately upstream from the fault).*

Scenario 1 consists of a high-speed protection coordination solution based on communication-based selective blocking. This algorithm requires that, in the event or a power system fault, all devices that detect that fault immediately send blocking messages to all upstream devices. This ensures that only the most downstream of these devices remains unblocked and therefore only this IED will issue an open command to the corresponding switching device and consequently clear the fault.

Of course, high-speed fault clearance requires high-speed coordination, which means that the blocking signals must reach their destination in very short times, ideally in few milliseconds.

Blocking signals are transmitted between IEDs using the IEC 61850 R-GOOSE protocol, which is a routable version of IEC 61850 GOOSE. GOOSE is a layer 2 horizontal communication protocol widely used within substations (a detailed overview on the protocol is available in section 10).

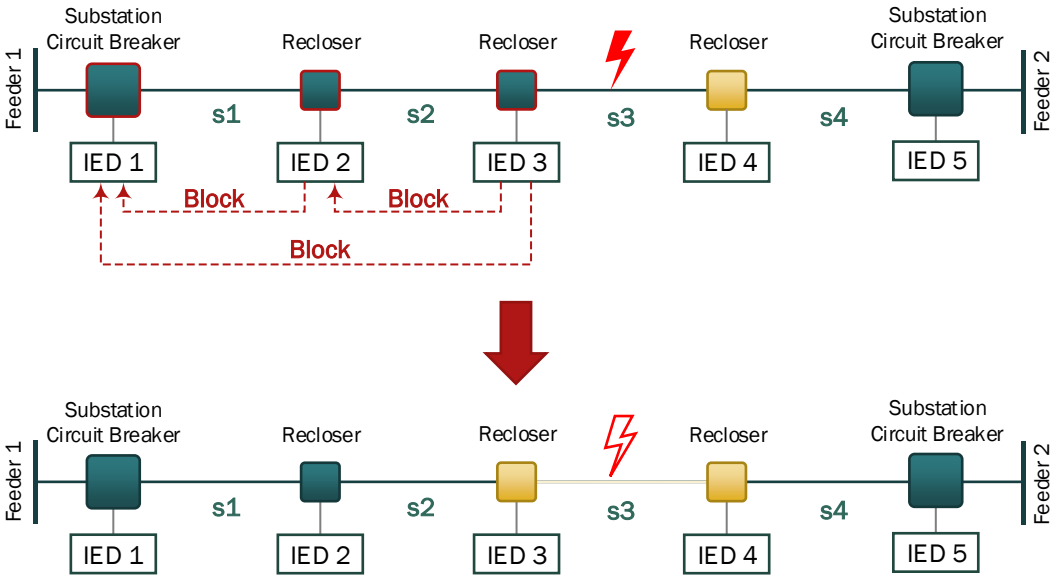



**Figure 2. Example of communication-based selective blocking.**

Figure 2 represents an example of the proposed algorithm when a fault is detected in line section s3, between the second recloser (N.C. point controlled by IED 3) and the third recloser (N.O. point controlled by IED 4). In this case, the line section in which the fault occurs is being powered by feeder 1, implying that the fault is downstream from IED 3, which is downstream from IED 2, which in turn is downstream from IED 1, and, consequently, that all referred IEDs will detect the fault. The goal of high-speed selective blocking is to ensure that the fault is cleared solely by the device immediately downstream of the fault (the recloser controlled by IED 3), thus leaving all other customers energized. For this purpose, all IEDs that detect the fault send blocking messages to all upstream devices using R-GOOSE messages, ensuring that only the most downstream device (IED 3) remains unblocked and therefore is the only one able to open the recloser and clear the fault.

## Use Case n Scenario 2: Distributed self-healing

Scenario 2 consists of a high-speed fully distributed power grid self-healing application that also uses IEC 61850 R-GOOSE horizontal communications for IED coordination.

Power grid self-healing algorithms implement part of the FDIR strategies previously described, namely the isolation of the faulty line section and subsequent service restoration on healthy line sections. Self-healing solutions aim at improving the Quality of Service (QoS) for energy distribution utility customers and reducing or even eliminating possible penalties related to minimal QoS requirements enforced to utilities by energy sector regulators.

Although there are solutions based solely on evaluating line voltage levels over relatively long periods of time, it is possible to implement high-speed solutions as long as there is a reliable communication infrastructure that complies with the latency and bandwidth requirements for these applications. Scenario 2 implements a high-speed application in which the IEDs that integrate the self-healing scheme exchange R-GOOSE messages in order to rapidly isolate the line section that includes the faulty section and to restore power to as many consumers as possible until the faulty section is repaired.

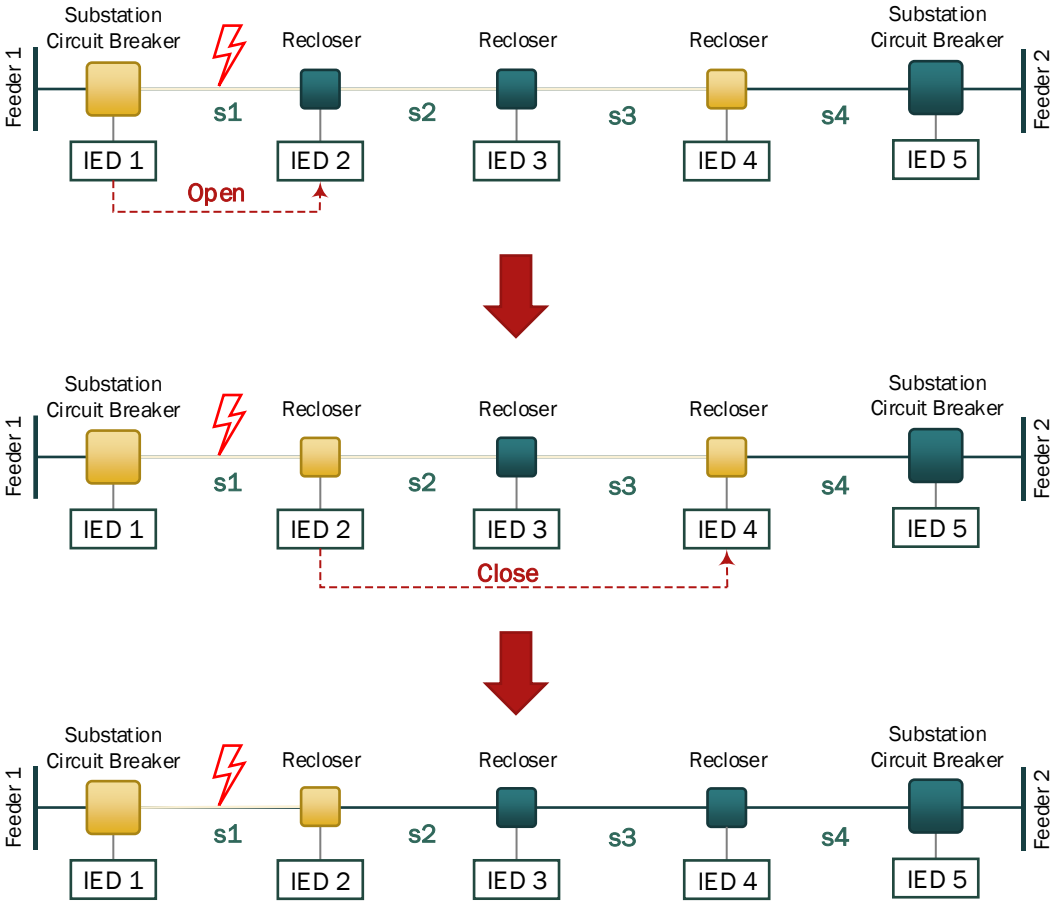



**Figure 3. Example of a self-healing sequence.**

Figure 3 illustrates an example of a self-healing sequence, initiated after a fault has been detected and cleared in line section s1. As a consequence, healthy line sections s2 and s3 have been de-energized as well.

As soon as the substation circuit breaker opens, IED 1 sends an open command to IED 2, which will open the recloser. When the recloser opens, IED 2 sends a close command to IED 4, which will close the N.O. point, re-energizing sections s2 and s3. Line sections s2 and s3 will be powered by feeder 2 until the faulty section is repaired, after which the system will return to its original configuration.

# 3 Task 3.2.3

# *T3.2.3 Requirements specification for real-time distributed protection systems for medium voltage energy networks using 5G communication technology*

This task is led by EFACEC Energia

## 3.1 Analysis of scenarios

*The main goal of the PPS3 is to map the usage of critical M2M applications on a 5G communication network. In this chapter we will present the main use cases and requirements for the use of a 5G communication network to support distributed automation and protection schemes*

### Horizontal communications (peer-to-peer – p2p)

*It is necessary to support horizontal communication between all the devices participating in the distributed algorithm. This means that it should be possible to communicate between peers (p2p communication). The distributed protection and automation algorithms depend on the exchange of information between the devices in real-time, so the horizontal communications are the most critical for these algorithms. Since the same information is necessary to several peers, a multicast approach should be used but, if technically it isn't possible to have multicast support, the sender should repeat the message to each of the receivers, this will cause more load on the sender and on the network, and this extra load should be particularly considered, since the latency is critical for the algorithm. Related to usage of a public communication infrastructure, security is of special concern. In the case of horizontal communication and the associated critical latency, security should be focused on the Integrity and Authentication, the Confidentiality concern might be less important.*

*The protocol used for the horizontal communication is IEC61850 (R-GOOSE).*

### Vertical communications

*In order to configure and to monitor each device and also to have a global view of the system operation, it is necessary for each device to be addressed by central components. The configuration software, a central gateway or even a central SCADA system could act as such central components. This type of communication is less critical than the horizontal one, but it is necessary in order to be possible to interact remotely with each device, for configuration or operation, so the only parameter that is more relaxed when comparing with the horizontal communication is the latency.*

*The protocols usually used for the vertical communication are IEC61850 (MMS), SSH, FTP(S) and HTTP(S)*

## 3.2 List and description of requirements

The following table illustrates the requirements associated to this use case:

| ID | Description | NotesVerification/Validation |
|---|---|---|
| GEN1 | It should be possible to assign static IP addresses to every device on the network | Configure static IP addresses on different devices and verify the communication between them (using ICMP PING) |
| GEN2 | The devices participating in the distributed algorithm will be geographically aggregated, nevertheless they can be connected to different network cells | Verify the fulfillment of the latency requirements between devices connected to different network cells (if this is possible in the scope of the pilot project). See ID HC4 |
| GEN3 | The network availability should be equal or better than 99.95% | Monitor the R-GOOSE communications over extended periods of time. R-GOOSE subscribers provide GOOSE failure indication when more than two consecutive messages are not received in the expected time. Packets received out-of-order are also registered. |
| HC1 | It should be possible to have peer-to-peer communication between each device on the network | With the devices configured, test the communication between them (ICMP PING) |
| HC2 | The horizontal communication should use R-GOOSE protocol over UDP/IP | Verify that all devices are receiving all configured R-GOOSE packets and no GOOSE failures are reported. |
| HC3 | The horizontal communication should have multicast support. If it is not technically possible to have multicast communication, the transmission time (end-to-end) of one message from one sender to up to 10 receivers should be according the latency requirements | A sender publishing an event to 10 receivers, all the receivers should signal the message reception for validation, and with a latency below 10ms (see ID HC4) |
| HC4 | The maximum latency for one message sent from one sender to multiple receivers should be below 10ms | The latency test should consider that a message is sent to 10 receivers, in multicast (if available) or in 10 unicast messages. In any of these situations, the latency should be below 10ms. |
| VC1 | It should be possible to have direct communication between the central systems (at the substation level) and each device on the network | Establish a session with each IED using a browser on the central systems |
| VC2 | The vertical communication will use IEC61850 (MMS), SSH, FTP(S), HTTP(S), all protocols over TCP/IP | Establish connections using all the mentioned protocols between the central systems and a IED |
| VC3 | The maximum latency for an MMS message between a device and a substation central system should be less than 300ms | MMS is mapped on TCP/IP, the latency can be evaluated dividing a measured TCP/IP RTT by 2 |

**Table 1: Requirements associated to Energy scenarios**

Notes:

- IP addressing is IPV4
- GENx: Generic requirements
- HCx: Horizontal Communication
- VCx: Vertical communications

# 4 Task 3.2.4

## *T3.2.4 Specification of the cybersecurity requirements for real-time protection systems for Medium Voltage power grids*

This task is led by EFACEC Energia

Key aspects for the functional requirements for energy networks using 5G communications include, but not limited to, the need of validating peer identity and ensuring peer to peer communication integrity and security.

In both cases, reliance on 5G service-based network functions for providing the necessary infra-structure services that allow secure identity assertion and communication establishment to be instantiated are used. Some of the necessary services for this project are outcomes of previous work, such as Mobile Edge Computing (MEC), Fog nodes, QoS and security and network services such as AAA, DNS and IDPS.

Specifically, for real time protection of Medium Voltage power grids, low response time and latency are key aspects to be accomplished whereas ensuring resilience to some cyber-attacks, namely:

- Impersonation attacks;
- Replay attacks;
- Man-in-the-Middle attacks;
- Denial of Service attacks.

Adding security might hinder response times – this could happen due to either the additional complexity of the communication layer by overlaying some of the existing protocols or the inability of peer capabilities for executing complex cryptographic functions, which normally have a significative high computational cost. Taking these facts into account, the first approach to ensure cybersecurity consists on having secure controlled network access and secure communications.

**Establishing Identity Validation:**

In a M2M (Machine to Machine) communication scenario such as this one, identification is a key stepping stone for enabling cybersecurity. Whereas current Medium Voltage power grids implementations use private communication networks, migration to 5G networking moves the communication to a domain in which there are several other partners and stakeholders involved. As such, one of the possible attacks against power grids might be done through the insertion of a rogue/fake peer/device on the electric power communication network. Then, if successful, the malicious device might inject fake commands or execute DoS (Denial of Service) attacks. Slicing 5G networks and the use of dedicated virtual networks are just some of the first measures that should be taken for implementing cybersecurity on a 5G based solution. Additional elements such as AAA (Authentication, Authorization and Accountability), policy firewall and the IDPS, among other modules, are also the necessary building blocks for having a secure communication. Therefore, validation of peer identity is a key security requirement for ensuring that only known (and non-malicious) network entities can establish communication channels and exchange data among themselves.

Establishing an identity validation requires the following:

- Communication peer identity defined by either manually provisioning or by other automated means (onboard software ID, either on firmware, chip (TPM – Trusted Platform Module) or smartcard). The identity is defined, for example, by either an ID/password pair, or other form of unique identification such as pre-shared key or PKI based credentials;
- The instantiated AAA service needs to recon the defined/stored peer identity's as valid, allowing the creation of communication session that allows the future secure establishment of peer to peer communications.

After the identity as been authenticated, the peers can check if the associated communication session is valid and authorized.

The use case scenario for secure identity is described as follows:

A VNF is instantiated for AAA as part of the solution SDN for supporting the Energy Distributed Protection solution. Previously a responsible user/administrator defined in the Identity Access Manager (IAM), defines the identities of the communication peers that will be part of the solution, by registering them on the IAM and provisioning, if necessary, the registered identity on the peers themselves or the attached CPE. The following picture presents an overview of the process of identity validation.

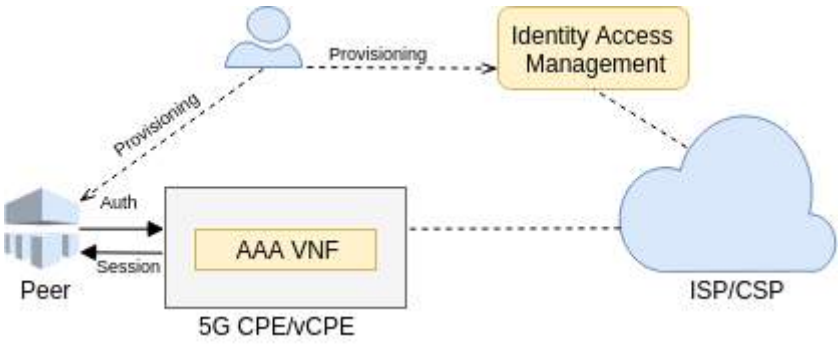



**Figure 4 – Process of identity validation.**

After successfully having the identity established and validated, the peer can request a session from the AAA VNF to be used for communication, or the AAA VNF, on behalf of the peer can behave as secure gateway, based on the peer identity to establish the peer to peer communication session.

With the session established, access to the SDN resources is granted which allows to the peer to either communicate with central core services or other peers. A Firewall VNF checks if the device establishing a communication has a valid session (hence a valid identity), and if so, allows the communication flow. The following picture presents an overview when communication is already established.

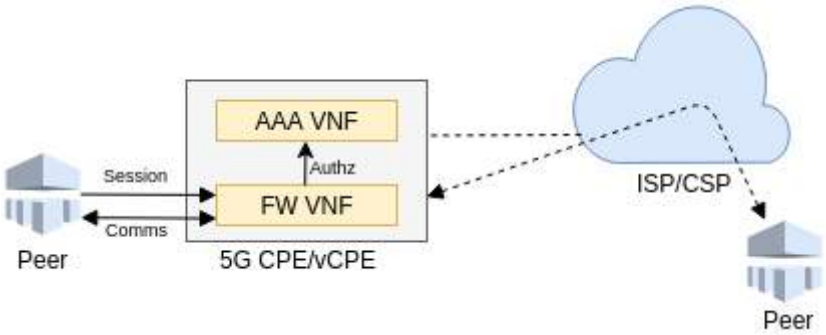



**Figure 5 – Communication established among peers.**

Regarding identity establishment and management, and complementarily to the approaches previously discussed, possible solutions can be based on 5G networking slicing with VPN, Firmware-based identification mechanisms, mechanisms employing TPM chips or solutions based on PSK (pre-shared keys). Such approaches are presented and discussed in greater detail in T3.2.11.

**Establishing Secure communications:**

Secure end to end communications can only be established between previously identified parties. Establishing a secure communication channel can require either pre-shared keys or, if using asymmetric encryption, the establishment of PKI infrastructure and secure peer provisioning with the necessary certificates and associated private keys. An additional use for the PKI infrastructure is that it also helps the assurance of the identification of the participating peers by the use of client certificates. Therefore, the AAA VNF can be expanded and/or configured to accept authentication through user (in this case device) certificates.

As previously described, Power Grid devices compliant with IEC 61850 Generic Object-Oriented Substation Events (GOOSE) usually have constrained and limited computational resources (such devices are commonly called IEDs – Intelligent Electronic Devices). Making changes on the standardized protocol layer could either break the protocol or even add too much computational overhead. Proposed schemes to add security to the IEC 61850, namely those defined on IEC 62351 to add Transport Layer Security (TLS) already exist, but other proposes consist on adding a Message authentication codes (MAC) to GOOSE packets without encrypting them, just to ensure the validity and integrity of the GOOSE packets without the encryption overhead.

A possible solution to allow the establishment of secure SSL/TLS communications between communicating peers, without modifying the GOOSE protocol or adding a TLS extension, is the possibility through the offloading of cryptographic communications functionality to the CPE, making the CPE behave as a front-end SSL/TLS proxy that secures communications on the shared 5G medium for the GOOSE communication. In this case while still leaving open to communication interception the local peer-CPE level, if offers protection on the 5G realm.

## 4.1 List and description of requirements

As extensions to what already 5G offers, for these specific security threats the following requirements must be met and dealt:

| ID | Description | Notes |
|---|---|---|
| CYBER1 | Impersonation attacks: Dealt with device provisioning and strong authentication; | |
| CYBER2 | Replay attacks: Dealt with the establishment of strong communication channel protection | |
| CYBER3 | Man-in-the-Middle attacks: Dealt with the establishment of strong communication channel protection | |
| CYBER4 | Denial of Service attacks: Dealt with 5G available countermeasures. | |

**Table 2: Cybersecurity requirements**

Mainly for the scenarios for protection of distributed energy solutions, the newer 5G capabilities offerings can lead to a new approach to security at the communication level among devices. As such a gap analysis needs to be performed between the possible new 5G security capabilities and the scenarios security requirements. Such gap analysis is performed further down on this document, where specific scenario requirements and 5G capabilities are analyzed.

The establishment of secure P2P communications depends on, other than the secure identification of the devices involved in the communications, the proper authentication and authorization of such devices. As discussed in greater detail in T3.2.11, a promising approach is the design of a group-based device authentication and authorization solution using a secret sharing algorithm, or the employment of a private blockchain platform with a zero-knowledge algorithm for privacy. The employment of a KDC-based solution can also be approached, using digital certificates with simplified enrolment of group-based authentication protocols.

# 5 Task 3.2.5

# T3.2.5 Safety requirements for signalling railways operations supported by 5G communications

This task is led by EFACEC Engenharia

The purpose of this task analysis regards the use of 5G communications to support railway signalling operations, in particular to meet railway level crossing (Figure 6 and 21) communication requirements (M2M), namely for safety critical communications from approaching train detectors (Strike In detectors) to the level crossing controllers (D2D/D2N2D) and safety critical communications from the approaching train to the level crossing controllers (V2X/V2N). Therefore, the analysis is emphasized in the use of wireless 5G communication instead of copper wire cables (D2D) and wireless 5G communication for V2X purposes

## 5.1 Analysis of scenarios

The scenarios involve safety critical communication and two use cases regarding the train approaching event. The use cases will demonstrate the use of 5G communications in railway safety critical communications, between the level crossing train detector activation points and the LX (Level Crossing) controller (Figure 6) and alternatively between the train (onboard computer) and the LX (Figure 21) controller. In the first use case, the traditional copper wire cables will be replaced by wireless 5G communications technology and safety communications protocols will be used to comply with railway signalling safety communications standards EN50159. The X-SAFE by EFACEC is the solution provided by EFACEC to Level crossing systems and it is already certified in compliance with all railway standards (RAMS Reliability, Availability, Maintenance and Safety – EN 50126, Functional safety - EN 50128 and Railway applications -Communication, signalling and processing systems - EN50159). However, being this system supported by cable, it is considered as a Close Transmission system. In the scope of this task the safety requirements concern the use of 5G technologies in Railways applications in compliance of Safety-related communication in transmission systems (EN50159), focused in the 5G as an Open transmission system.

In the scope of this safety critical scenarios it is mandatory to use a simulation or a real half barrier level crossing control system in a railroad crossing environment (laboratory or real premises). The real system will include the train, LX controller cabinet equipped with SIL4 safety PLC, an axle counter train detection system, EMC protection devices, an uninterruptible power supply and a 5G CPE. Each approaching train detector will use a 5G CPE to communicate with the level crossing controller. Two half barrier drives, controlled by the LX controller, will protect the entry of cars in the rail crossing during the train approaching and passing. All the communications will be supported by safety-critical protocols (Safe Ethernet or RASTA), used under the scope of the project.

Concerning the second use case (V2X scenario), if the train doesn't detect or could not transmit the approaching event information, the level crossing must show the train driver a danger aspect signal at train braking distance, signalling the level crossing open state (shown in the proper rail side protection signal – Figure 21).

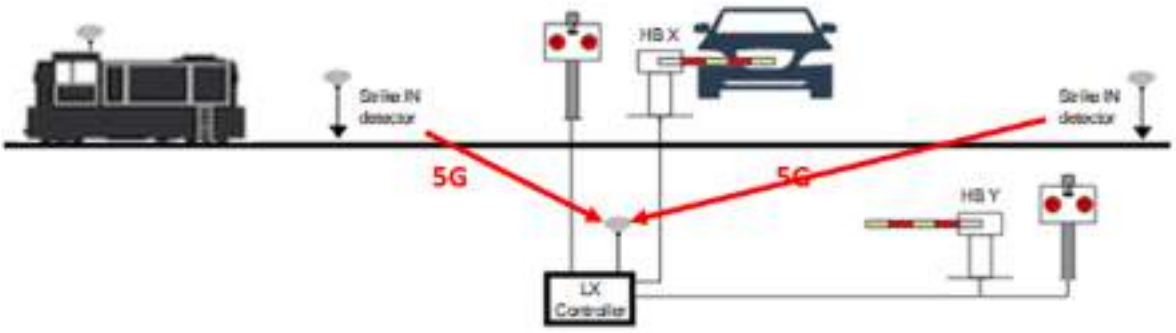



**Figure 6- Safety Critical scenario UC1 communication between the strike in points and the Level Cross controller**

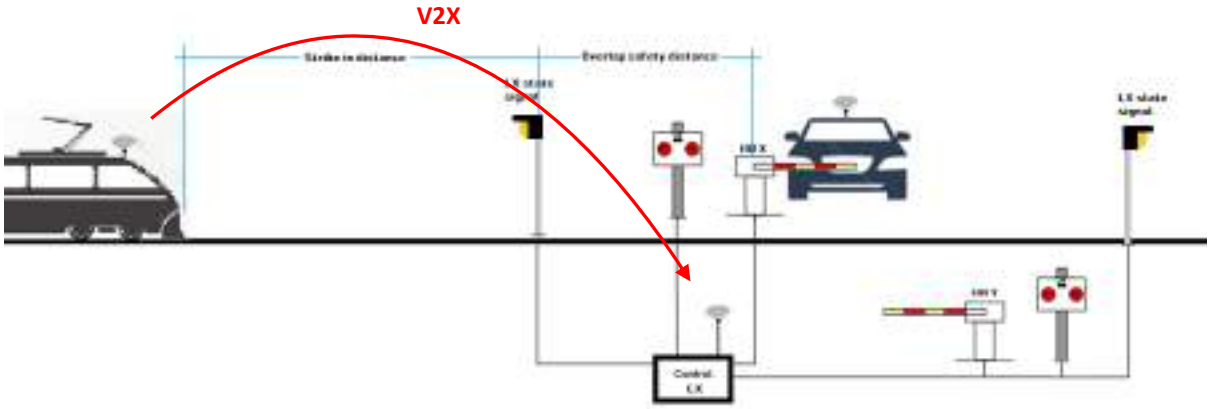



**Figure 21 – Safety Critical scenario – UC2: The train directly sends the information to the LX controller, whenever the train is approaching**

## 5.2 List of safety requirements for open transmission systems

The communications involved in this 5G use case is considered as an open transmission system and therefore can be affected by data corruption as well as unauthorized access.

According with the standard, an open transmission system is characterized as “a system with an unknown number of participants, having unknown, variable and no trusted properties, used for unknown telecommunication services ad for which the risk of unauthorized access shall be assessed”.

The following table identifies the requirements (SR) that should be addressed for this safety end-to-end 5G communication. The table outlines the Safety requirements Identifiers, for this use case (UC) and a brief description.

| SR-ID | Description | |
|---|---|---|
| SR-UC1-01 | Message authentication, a message in which the information is valid and known to have been originated from a stated source; | |
| SR-UC1-02 | Message integrity, a message in which the information is complete and not altered | |
| SR-UC1-03 | Message timeless, a message in which the information is available at the right time according to requirements; | |
| SR-UC1-04 | Message sequence, messages are received from the application in the same order in which they are transmitted. | |

**Table 3: Safety requirements**

These requirements will reduce the risk of the following threats (TH)

| TH-ID | Description | BR-ID |
|---|---|---|
| TH-UC1-01 | Repetition, when a message is received more than once | |
| TH-UC1-02 | Deletion, when a message is removed form a message stream | |
| TH-UC1-03 | Insertion, when a new message is implanted in the message stream | |
| TH-UC1-04 | Resequencing, when messages are received in an unexpected sequence | |
| TH-UC1-05 | Corruption, when the information contained in a message is changed, casually or not | |
| TH-UC1-06 | Delay , when messages are received at a time later than intended | |
| TH-UC1-07 | Masquerade, when a non-authentic message is designed thus to appear to be authentic (an authentic message means a valid message in which the information is certificated as originated from an authenticated data source). | |

**Table 4: list of safety threats**

# 6 Task 3.2.6

# T3.2.6 Requirements Specification for fix permanent train detection system (permanent strike-in) for Level Crossing supported by Radio communication

This task is led by EFACEC Engenharia

## 6.1 Analysis of scenarios

This is the safety critical scenario characterized as the use case 1 (UC1) and represented in the figure 20. This scenario gives the level crossing equipment capabilities to communicate the status of the equipment via Radio (4G/5G) technology. Each sensor and communication boards positioned in the trackline (detection system) has associated a CPE equipment that supports 4G/5G technology (Strike IN detector) and all of them are able to communicate their status, whenever requested by the LX controller that also has the same CPE equipment to support transmission by 4G/5G technology.

The LX controller with the information from all the sensors is able to assure the safety conditions to the level crossing, controlling the position of the barriers and the proper railway traffic lights information.

The communication between the sensors on the trackline and the LX controller shall comply with safety (Safe-Ethernet/RaSTA) and security requirements.

Regarding this use case, the business scenario flows can be summarized in the following steps:

1 – Train detection system detects the presence of an approaching train

2 – Train detection system sends information to the LX Controller (LX controller is permanently requesting and receiving equipment status and detection information)

3 – LX Controller starts safety actions managing all the peripheral devices (road and protection signals, bells, half-barriers) according to the track section occupancy status

4 – Train detection system detects that the level crossing train section is released (not occupied) and sends this information to the LX controller

5 – LX controller starts new safety actions managing the peripheral devices properly (Lx area is free for people and cars)

## 6.2 List and description of requirements

For a better requirements definition, for each use case, there were considered business, functional and technical requirements.

## 6.2.1Business Requirements

Table 5 shows the business requirements associated with the safety critical scenario (UC1) regarding the communication between the train detecting sensors and the Level Crossing controller.

| BR-ID | Description | Notes |
|---|---|---|
| BR-UC1-01 | A train detector system will be needed to detect trains approaching the Level Crossing | |
| BR-UC1-02 | A train detector system will be needed to detect if the train is occupying the Level Crossing section or to the detect the absence of the train in the section | |
| BR-UC1-03 | An information system will be needed to inform car driver's if the Level Crossing is free | |
| BR-UC1-04 | An information system will be needed to inform train drivers that the Level Crossing is free | |
| BR-UC1-05 | A dedicated and critical system will be needed to receive sensors and equipment information and to assure the LX actions (railways signalling operation) | |
| BR-UC1-06 | Communication technology need to be present to exchange information between the system components | |
| BR-UC1-07 | Wireless Communication, with the same level of safety and security need to be present to exchange information between the system components in order to reduce installation and maintenance costs | |

**Table 5: Business Requirements (UC1)**

### 6.2.2 Functional Requirements

Table 6 shows the functional requirements associated with the safety critical scenario (UC1) regarding the communication between the train detecting sensors and the Level Crossing controller. This table also provide the links between the functional requirements and the corresponding business requirements.

| FR-ID | Description | BR-ID |
|---|---|---|
| FR-UC1-01 | The communications between the components (track lines equipment's and LX controller) must use standard protocols both for safety and security | BR-UC1-06<br>BR-UC1-07 |
| FR-UC1-02 | A Strike-In detector/axel counter train detector system will be needed to detect trains approaching the Level Crossing | BR-UC1-01 |
| FR-UC1-03 | A Train detector/ axel counter train detector system will be needed to detect if the train is occupying the Level Crossing section or to the detect the absence of the train in the section | BR-UC1-02 |
| FR-UC1-04 | A LX controller will be needed to receive sensors and equipment information and to assure the LX actions (railways signalling operation) | BR-UC1-05<br>BR-UC1-06 |
| FR-UC1-05 | The communication between the Strike-in detectors and the LX controller must be supported over IP | BR-UC1-06 |
| FR-UC1-06 | In a presence of communication failures, the LX must be set to its safe mode (protection mode) | BR- UC1-06 |
| FR-UC1-07 | The communication between the axel counters and the LX controller must be 5G | BR- UC1-07 |
| FR-UC1-08 | Traffic lights will be needed to inform car driver's | BR- UC1-03 |
| FR-UC1-09 | Protection Lx Signals will be needed to inform train drivers that the Level Crossing is free | BR- UC1-04 |
| FR-UC1-10 | 5G CPE devices will be needed to assure the 5G connectivity of Lx devices to 5G network | BR-UC1-06<br>BR- UC1-07 |
| FR-UC1-11 | 5G CPE devices must support Ethernet interfaces | BR- UC1-07 |
| FR-UC1-12 | The same Level of safety and security must be assured by the 5G network | BR-UC1-06<br>BR- UC1-07 |
| FR- UC113 | The site pilot must be covered by a 5G network | BR- UC1-07 |

**Table 6: Functional Requirements (UC1)**

### 6.2.3 Technical Requirements

Table 7 shows the functional requirements associated with the safety critical scenario (UC1) regarding the communication between the train detecting sensors and the Level Crossing controller. This table

also provide the links between the technical requirements and the corresponding functional requirements.

| TR-ID | Description | Notes |
|---|---|---|
| TR-UC1-01 | Strike in detectors and the LX controller must connect to the 5G Network and use it as the communication channel | FR-UC1-01<br>FR- UC1-04<br>FR-UC1-10<br>FR- UC1-11<br>FR-UC1-10<br>FR- UC1-12<br>FR-UC1-10<br>FR-UC1-13 |
| TR-UC1-02 | The 5G New Radio component MUST radiate the coverage of the area where the selected railway devices are located | FR-UC1-13 |
| TR-UC1-03 | The gNB MUST have an outdoor reach of around 200-300m (1 macro-cell sector MUST be enough to cover the list of devices selected | FR-UC1-13 |
| TR-UC1-04 | The gNB MUST use the 3.6MHz band (100MHz bandwidth) assigned temporarily by the Portuguese regulator (ANACOM) for trial and research purposes | FR-UC1-13 |
| TR-UC1-05 | The 5G-Core MUST be deployed in a datacentre and connect to the gNB using a dedicated fiber (GPON) | FR-UC1-13 |
| TR-UC1-06 | The gNB and 5G-Core components MUST comply with 3GPP standards, namely with TS 23.501 and TS 23.502 | FR-UC1-13 |
| TR-UC1-08 | The 5G Network MUST support slicing mechanisms to cope with some requirements, such as bandwidth, latency (<10 ms) or reliability (99,99%), over a common 5G infrastructure | FR-UC1-12<br>FR-UC1-13 |
| TR-UC1-09 | The 5G Network MUST support a narrow bandwidth and reliable slices, with URLLC characteristics, to support machine-to-machine (M2M) communications (among level crossing components) | FR-UC1-11<br>FR-UC1-12 |
| TR-UC1-13 | 5G CPE must support router functions between Ethernet and 5G interface | FR-UC1-10<br>FR-UC1-11<br>FR-UC1-13 |
| TR-UC1-14 | The communications must be safe based on FSE (Safe Ethernet) or RaSTA (Rail Safe Transport Application – DIN VDE V 0831-200) protocol in accordance with CENELEC SIL4 and EN 50159 – for transmission system | FR-UC1-01<br>FR-UC1-05 |
| TR-UC1-15 | Security (cybersecurity) mechanisms shall be implemented for the LX crossing equipment's communications (over communication protocols) such as VPN with sage login and encryption | FR-UC1-01<br>FR-UC1-05 |
| TR-UC1-16 | The system must recover automatically from communications failures. The recovery time must be less than 500 ms | FR-UC1-01<br>FR-UC1-06 |

Table 7: Technical Requirements (P3UC1)

# 7 Task 3.2.7

# T3.2.7 Requirements Specification based on mobile virtual strike-in for Level Crossing supported by Radio communications using information from train positioning

This task is led by EFACEC Engenharia

## 7.1 Analysis of scenarios

This is the safety critical scenario characterized as the use case 2 (UC2) and represented in the figure 21. This is an alternative way to detect the approaching train using the onboard computer and GPS (mobile virtual system) to detect that the train is located in the Level crossing area. This scenario gives the Train vehicle, the capability to control the level crossing equipment remotely. The Train must have a GPS receiver and when approaching x meters (configurable on file centrally) of the sensor detector located on trackline it shall request a connection to the LX controller. After the connection has been establish and the train is in the GPS location that corresponds to the closest location of the sensor or y meters (configurable on file centrally), the train will send a message to the LX controller with the information that the TRAM is over the sensor (level crossing area)

The LX controller with the information from all the sensors is able to assure the safety conditions to the level crossing, controlling the position of the barriers and the proper railway traffic lights information.

The communication between the train and the LX controller shall comply with safety (Safe-Ethernet/RaSTA) and security requirements.

Regarding this use case, the business scenario flows can be summarized in the following steps:

1 – Train GPS system detects the presence of an approaching train in the level crossing area

2 – Train onboard computer sends information to the LX Controller

3 – LX Controller starts safety actions managing all the peripheral devices (road and protection signals, bells, half-barriers) according to the track section occupancy status

4 – Train GPS system detects that the level crossing train section is released (not occupied) and the onboard computer sends this information to the LX controller

5 – LX controller starts new safety actions managing the peripheral devices properly (Lx area is free for people and cars)

## 7.2 List and description of requirements

For a better requirements definition, for each use case, there were considered business, functional and technical requirements.

## 7.2.1Business Requirements

Table 5 shows the business requirements associated with the safety critical scenario (UC2) regarding the communication between the train and the Level Crossing controller.

| BR-ID | Description | Notes |
|---|---|---|
| BR-UC2-01 | A Location system will be needed to detect trains approaching the Level Crossing or leaving the level crossing area | |
| BR- UC2-02 | Train positioning must be assured | |
| BR- UC2-03 | An information system will be needed to inform car driver's if the Level Crossing is free | |
| BR- UC2-04 | Data communication must be available to the train | |
| BR- UC2-05 | An information system will be needed to inform train drivers that the Level Crossing is free | |
| BR- UC2-06 | A dedicated and critical system will be needed to receive sensors and equipment information and to assure the LX actions (railways signalling operation) | |
| BR- UC2-07 | Communication technology need to be present to exchange information between the system components | |
| BR- UC2-08 | Wireless Communication, with the same level of safety and security need to be present to exchange information between the system components in order to reduce installation and maintenance costs | |

**Table 8: Business Requirements (UC2)**

## 7.2.2 Functional Requirements

Table 6 shows the functional requirements associated with the safety critical scenario (UC2) regarding the communication between the train and the Level Crossing controller. This table also provides the links between the functional requirements and the corresponding business requirements.

| FR-ID | Description | BR-ID |
|---|---|---|
| FR-UC2-01 | The communications between the train (onboard computer) and LX controller must use standard protocols both for safety and security | BR-UC2-06<br>BR- UC2-07 |
| FR-UC2-02 | A GPS system will be needed to detect trains approaching the Level Crossing | BR- UC2-01<br>BR- UC2-02 |
| FR-UC2-03 | A GPS system will be needed to detect if the train is occupying or leaving the level crossing area | BR- UC2-01 |

| | | |
|---|---|---|
| FR-UC2-04 | A LX controller will be needed to receive sensors and equipment information and to assure the LX actions (railways signalling operation) | BR-UC2-05<br>BR- UC2-06 |
| FR-UC2-05 | The communication between the train and the LX controller must be supported over IP | BR- UC2-06 |
| FR-UC2-06 | In a presence of communication failures, the LX must be set to its safe mode (protection mode) | BR- UC2-06 |
| FR-UC2-07 | The communication between the train and the LX controller must be 4G/5G | BR- UC2-07 |
| FR-UC2-08 | Traffic lights will be needed to inform car driver's | BR- UC2-03 |
| FR-UC2-09 | Protection Lx Signals will be needed to inform train drivers that the Level Crossing is free | BR- UC2-05 |
| FR-UC210 | 5G CPE devices will be needed to assure the 5G connectivity of Lx devices to 5G network | BR-UC2-06<br>BR- UC2-07 |
| FR-UC2-11 | 5G CPE devices must support Ethernet interfaces | BR- UC2-07 |
| FR-UC2-12 | The same Level of safety and security must be assured by the 5G network | BR-UC2-06<br>BR- UC2-07 |
| FR-UC2-13 | The site pilot must be covered by a 5G network | BR- UC2-07 |
| FR-UC2-14 | If the train doesn't detect or could not transmit the approaching event information, the level crossing must show the train driver a danger aspect signal at train braking distance, signalling the level crossing open state (shown in the proper rail side protection signal) | BR- UC2-05 |

**Table 9: Functional Requirements (P3UC2)**

### 7.2.2.1 Technical Requirements

Table 7 shows the technical requirements associated with the safety critical scenario (UC2) regarding the communication between the and the Level Crossing controller. This table also provide the links between the technical requirements and the corresponding functional requirements.

| TR-ID | Description | Notes |
|---|---|---|
| TR-UC1-01 | The onboard computer and the LX controller must connect to the 5G Network and use it as the communication channel | FR-P3UC1-01<br>FR-P3UC1-04<br>FR-P3UC1-10<br>FR-P3UC1-11<br>FR-P3UC1-10<br>FR-P3UC1-12<br>FR-P3UC1-10<br>FR-P3UC1-13 |

| | | |
|---|---|---|
| TR-UC1-02 | The 5G New Radio component MUST radiate the coverage of the area where the selected railway devices are located | FR-P3UC1-13 |
| TR-UC1-03 | The gNB MUST have an outdoor reach of around 200-300m (1 macro-cell sector MUST be enough to cover the list of devices selected | FR-P3UC1-13 |
| TR-UC1-04 | The gNB MUST use the 3.6MHz band (100MHz bandwidth) assigned temporarily by the Portuguese regulator (ANACOM) for trial and research purposes | FR-P3UC1-13 |
| TR-UC1-05 | The 5G-Core MUST be deployed in a datacentre and connect to the gNB using a dedicated fiber (GPON) | FR-P3UC1-13 |
| TR-UC1-06 | The gNB and 5G-Core components MUST comply with 3GPP standards, namely with TS 23.501 and TS 23.502 | FR-P3UC1-13 |
| TR-UC1-08 | The 5G Network MUST support slicing mechanisms to cope with some requirements, such as bandwidth, latency (<10 ms) or reliability (99,99%), over a common 5G infrastructure | FR-P3UC1-12<br>FR-P3UC1-13 |
| TR-UC1-09 | The 5G Network MUST support a narrow bandwidth and reliable slices, with URLLC characteristics and eMBB (up to 160 Km/h), to support machine-to-machine (M2M) communications | FR-P3UC1-11<br>FR-P3UC1-12 |
| TR-UC1-13 | 5G CPE must support router functions between Ethernet and 5G interface | FR-P3UC1-10<br>FR-P3UC1-11<br>FR-P3UC1-13 |
| TR-UC1-14 | The communications must be safe based on FSE (Safe Ethernet) or RaSTA (Rail Safe Transport Application – DIN VDE V 0831-200) protocol in accordance with CENELEC SIL4 and EN 50159 – for transmission system | FR-P3UC1-01<br>FR-P3UC1-05 |
| TR-UC1-15 | Security (cybersecurity) mechanisms shall be implemented for the LX crossing equipment's communications (over communication protocols) such as VPN with sage login and encryption | FR-P3UC1-01<br>FR-P3UC1-05<br>FR-P3UC1-12 |
| TR-UC1-16 | The system must recover automatically from communications failures. The recovery time must be less than 500 ms | FR-P3UC1-01<br>FR-P3UC1-06 |
| TR-UC2-17 | The system must recover automatically from communications failures. The recovery time must be less than 500 ms | FR-P3UC1-01<br>FR-P3UC1-06 |

**Table 10: Technical Requirements (UC2)**

# 8 Task 3.2.8

# T3.2.8 Requirements specification for smart video systems supporting obstacle detection (X2V) in level crossing

This task is led by EFACEC Engenharia

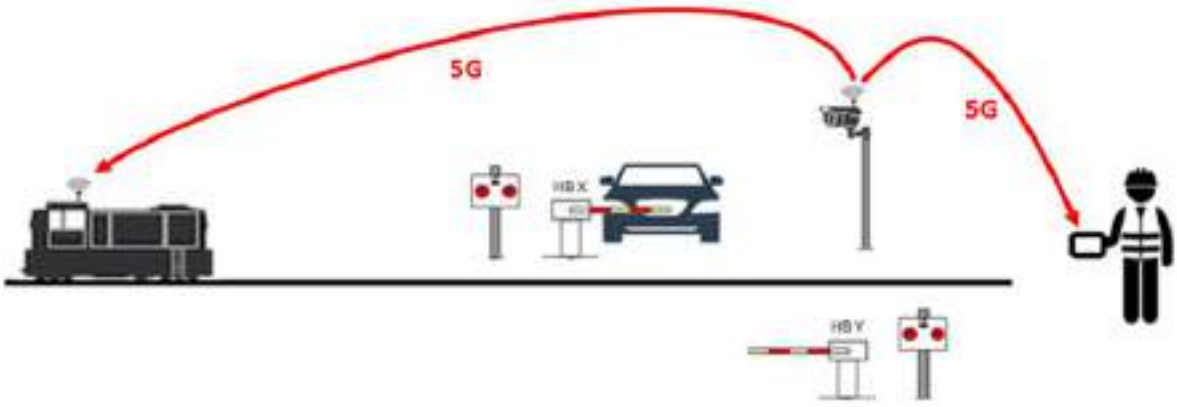
## 8.1 Analysis of scenarios

This nor critical scenario allows the driver or maintenance agents to watch the real-time video from the next level crossing video camera that is installed in the next level crossing passage (Figure xxx)

By means of GPS positioning, the train knows his location almost in real-time condition and when validating the GPS coordinates against the level crossing coordinates the train request a secure connection between the onboard equipment and the video camera in order to transmit the video streaming.

The main objectives of the use case is to transmit HD video images to the approaching train, allowing the driver to get images of the level crossing area, thus preventing accidents caused by cars trapped between the level crossing gates. In the scope of this UC it is also desired to transmit the same video images to maintenance agents/Command Centre, providing this way, mechanisms to reinforce the LX safety.

All the communications between the train and the video camera and also between the camera and the maintenance team are based on the 4G/5G technology.




Regarding use case, the scenario can be characterized as follows:

1. The GPS and the onboard train equipment detect that the train is located in the Level Crossing area.
2. Real-time video images (next LX area) start to be transmitted to Tablet Devices (train and maintenance agent).
3. The GPS and the onboard train equipment detect that the train passed the Level Crossing area.

4. The video images transmission to the Tablet Devices is interrupted.
5. Real-time video images are permanently transmitted to the command centre.

## 8.1 List and description of requirements

For a better requirements definition, for this use case, there were considered business, functional and technical requirements.

### 8.1.1Business Requirements

Table 5 shows the business requirements associated with the non-safety critical scenario (UC3)

| BR-ID | Description | Notes |
|---|---|---|
| BR-UC3-01 | Level Crossing (LX) area must be remotely monitored | |
| BR-UC3-02 | Train positioning must be assured | |
| BR-UC3-03 | Data communication must be available to the train | |
| BR-UC3-04 | Dedicated devices must be available to the train and to maintenance agents | |
| BR-UC3-05 | Communication technology (wireless) need to be present to exchange information between the system components | |
| BR-UC3-06 | A command centre will be needed to aggregate information | |
| BR-UC3-07 | Increase safety and security assuring more information to train drivers and maintenance agents | |

**Table 11: Business Requirements (UC3)**

### 8.1.2Functional Requirements

Table 6 shows the functional requirements associated with the non-safety critical scenario (UC3) .This table also provides the links between the functional requirements and the corresponding business requirements.

| FR-ID | Description | BR-ID |
|---|---|---|
| FR-UC3-01 | At least a HD camera must be installed in the LX area | BR- UC3-01 |
| FR- UC3-02 | Geolocation coordinates must be received by GPS | BR- UC3-02 |
| FR- UC3-03 | Tablet devices must support 5G communications | BR-UC3-03<br>BR- UC3-04 |

| | | |
|---|---|---|
| FR- UC3-04 | 5G communication must available to exchange information between the system components | BR- UC3-05 |
| FR- UC3-05 | Video Images must be visualized in Tablet Devices | BR-UC3-04<br>BR- UC3-07 |
| FR- UC3-06 | Video Camera must support IP protocols and interfaces | BR- UC3-01<br>BR- UC3-04<br>BR- UC3-06 |
| FR- UC3-07 | 5G CPE devices will be needed to assure the 5G connectivity of system devices to 5G network | BR- UC3-05 |
| FR- UC3-08 | A command centre will be needed to aggregate information (video images and to broadcast alarms) | BR- UC3-06 |
| FR- UC3-09 | An app for mobile devices (Tablet) must be supplied mainly to visualize video images regarding Level Crossing areas | BR- UC3-01<br>BR- UC3-04<br>BR- UC3-07 |
| FR- UC3-10 | The site pilot must be covered by a 5G network | BR-UC3-03<br>BR- UC3-05 |
| FR- UC3-11 | The driver shall have an option to see or not a GIS map with train location on that map and when the video streaming is displayed shall be over the GIS map. When the video streaming stops the driver with information about the distance to the next level crossing video exhibition. | BR-UC3-01<br>BR- UC3-02 |
| | | |

**Table 12: Functional Requirements (UC3)**

## 8.1.3Technical Requirements

Table 7 shows the technical requirements associated with the non-safety critical scenario (UC3). This table also provide the links between the technical requirements and the corresponding functional requirements.

| TR-ID | Description | FR-ID |
|---|---|---|
| TR-UC3-01 | All system components (Train, tablets, video camera) must connect to the 5G Network and use it as the communication channel | FR- UC3-03<br>FR- UC3-04<br>FR- UC3-07<br>FR- UC3-10 |

| | | |
|---|---|---|
| TR- UC3-02 | The 5G New Radio component MUST radiate the coverage of the area where the selected railway devices are located | FR- UC3-10 |
| TR- UC3-03 | The gNB MUST have an outdoor reach of around 200-300m (1 macro-cell sector MUST be enough to cover the list of devices selected) | FR- UC3-10 |
| TR- UC3-04 | The gNB MUST use the 3.6MHz band (100MHz bandwidth) assigned temporarily by the Portuguese regulator (ANACOM) for trial and research purposes | FR- UC3-10 |
| TR- UC3-05 | The 5G-Core MUST be deployed in a datacentre and connect to the gNB using a dedicated fiber (GPON) | FR- UC3-10 |
| TR- UC3-06 | The gNB and 5G-Core components MUST comply with 3GPP standards, namely with TS 23.501 and TS 23.502 | FR- UC3-10 |
| TR- UC3-07 | The 5G Network MUST support slicing mechanisms to cope with some requirements, such as bandwidth, latency (<10 ms) or reliability (99,99%), over a common 5G infrastructure | FR- UC3-10 |
| TR- UC3-08 | The 5G Network MUST support a narrow bandwidth and reliable slices, with URLLC characteristics, to support machine-to-machine (M2M) communications | FR- UC3-10 |
| TR- UC3-09 | 5G CPE must support router functions between Ethernet and 5G interface | FR- UC3-07<br>FR- UC3-10 |
| TR- UC3-10 | Security (cybersecurity) mechanisms shall be implemented for communications (over communication protocols) such as VPN with sage login and encryption | FR- UC3-04<br>FR- UC3-10 |
| TR- UC3-11 | The system must recover automatically from communications failures. The recovery time must be less than 500 ms. | FR- UC3-04 |
| TR- UC3-12 | The 5G Network MUST support a high bandwidth (at least 120 Mbps) slices, with eMBB (up to 160 Km/h) characteristics, for the delivery of high-quality video to trains, maintenance agents and command centre | FR- UC3-04<br>FR- UC3-10 |
| TR- UC3-13 | The 5G MUST support the video transmission system shall be in accordance with IEC 62676 – Video Surveillance Systems * | FR- UC3-04<br>FR- UC3-10 |
| TR- UC3-13 | The console/processing unit shall update the time/date of the equipment with an NTP server from the 5G service provider every 5minutes (this value shall be configurable). | FR- UC3-03 |

**Table 13: Technical Requirements (UC3)**

* transmission system shall be in accordance with IEC 62676 – Video Surveillance Systems for use in security application in terms of security, integrity, availability and latency like the following table from the standard shows:

| System feedback | | |
|---|---|---|
| Responding time | Performance | Operator |
| 0 s to 0,2 s | Optimal | Doesn't notice response time. |
| 0,2 s to 0,5 s | Delay | Feels the delay and tries to adapt. |
| 0,5 s to 2 s | Strong delay | Is disturbed by the delayed response.<br>System shall display "please wait..." |
| More than 2 s | Unacceptable | Loses response to manual actions.<br>system shall display reasons and/or prompt messages like "screen will be available in xx seconds, ..." |

**Table 14: vídeo response time requirements**

But because the latency of the images is a very important issue other values shall be used under communications with 5G technology:

| Latency | Performance | Information |
|---|---|---|
| 0 a 100 ms | Optimal | Doesn't notice response time.<br>The video shall be presented with a green border. |
| 100 a 200 ms | Delay | Feels the delay and tries to adapt. For instance decrease the Train speed. Another alternative to solve the issue can be to decrease the framerate and/or image resolution.<br>The video shall be presented with a yellow border. |
| 200 a 500 ms | Strong delay | Is disturbed by the delayed response.<br>System shall display "please wait for the updated video…".<br>The video shall be presented with a orange border. |
| 500 a 1000 ms | Unacceptable | Loses response to manual actions. The images shall be removed from the display and replaced by a red box.<br>System shall display reasons and/or prompt messages like "screen will be available in xx seconds…"<br>Driver shall be informed to decrease the speed of the Train and get in to the sight march mode situation. |

**Table 15: latency vs vídeo streaming information**

# 9 Task 3.2.9

# T3.2.9 Requirements specification for safety critical communications protocols applicable in railways signalling operation

This task is led by EFACEC Engenharia

## 9.1 List and description of functional requirements (communication protocols)

The communication protocols used for safety critical communications should provide the safe services described in the previous section in order to reduce the risk of threats outlined in the table 4.

In order to comply the railway standards the communication protocols must implement the following defense techniques:

| | |
|---|---|
| Sequence Number | Every message has a data field containing a number changing in a predefined way from message to message |
| Time stamp | A temporal information (time stamp) is added at every message |
| Time-out | A timeout timer is used to control the timeliness of message |
| Feedback Messages | It's the confirmation of correct reception of the message sent by source |
| Source and destination identifier | An identifier is assigned to each entity.<br>This identifier can be a name, number or arbitrary bit pattern. Messages may contain a unique source identifier, or a unique destination identifier, or both. |
| Message identification procedure | Open transmission systems may receive messages from other (unknown) users confusing them with information originating from an intended source. The message identification procedure allows for the identification of received message |
| Safety Code | Can detect the eventual corruption of data. |
| Cryptographic Techniques | Redundant data based on cryptographic functions are included in messages to allow for detection of data corruptions and unauthorized access. |

**Table 16: Defense techniques Requirements**

Table 9 describes the matrix regarding the protection that each defense technique can provide against one or more possible threats

| Threats vs defenses | Sequence Number | Time stamp | Time-out | Source and destination identifiers | Feedback messages | Identification procedure | Safety Code | Cryptographic techniques |
|---|---|---|---|---|---|---|---|---|
| Repetition | ✓ | ✓ | | | | | | |
| Deletion | ✓ | | | | | | | |
| Insertion | ✓ | | | ✓ | ✓ | ✓ | | |
| Resequencing | ✓ | ✓ | | | | | | |
| Corruption | | | | | | | ✓ | ✓ |
| Delay | | ✓ | ✓ | | | | | |
| Masquerade | | | | ✓ | | ✓ | | ✓ |

**Table 17: threats vs defenses tecnhiques matrix**

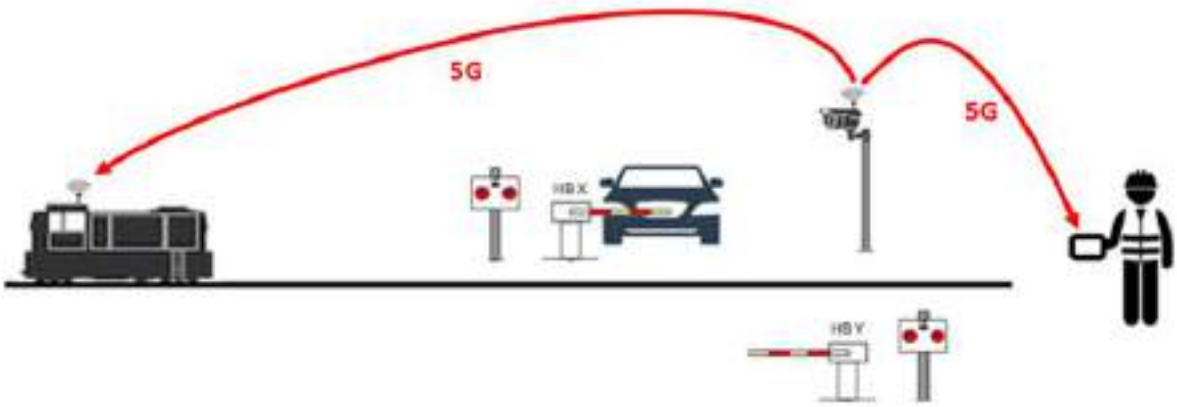
According with preliminary studies performed previously, several communication protocols have been studied and Rasta and FSE comply these requirements.

# 10 T3.2.10 Hardware requirements specification for 5G communications supporting railways signalling operations

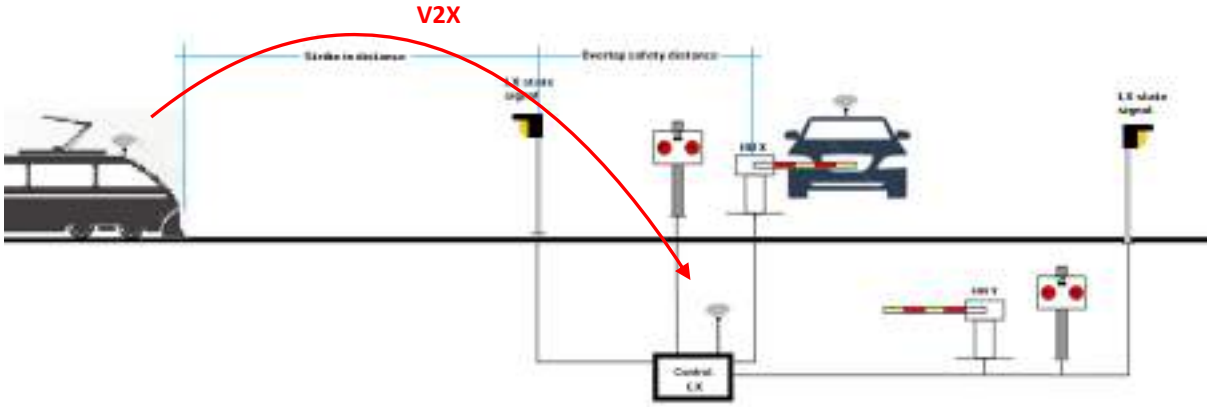
This task is led by EFACEC Engenharia

## 10.1 Analysis of scenarios

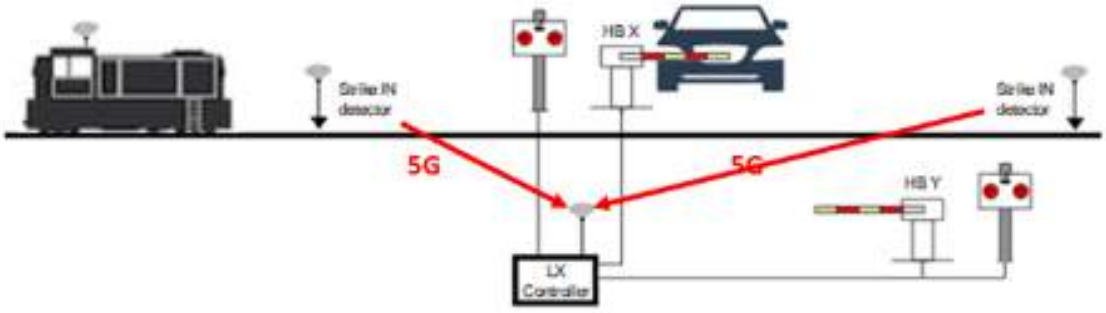
For the scenario defined in the T3.2.8 there is a need for a console/processing unit to be used inside a TRAM vehicle:




For the scenario defined in the T3.2.7 there is a need to access the LX controller in order to request the status change of the signal:




For the scenario defined in the T3.2.6 there is a need interface the strike IN detector equipment to the LX controller:



## 10.2 List and description of hardware requirements

a) Onboard console equipment

The following lists the requirements needed to implement the console/processing unit to be installed in the TRAM driver's cabin:

- Processor unit AMD or Intel Quad-core 64-bit platform clock speed >1.5GHz
- L2 cache 2MB minimum
- RAM 4GB minimum
- Flash 8GB minimum (eMMC, microSD card, on-board flash, CFast format or equivalent)
- TFT display with capacitive 8inch minimum
- Resolution 640x480 pixel minimum with dedicated GPU
- O.S. Linux Debian or equivalent
- GPS interface
- MiniPCI-e slot for 4G/5G interface with SIM holder
- Operating temperature -30ºC up to 70ºC minimum
- Railway usage EN50155 (onboard equipment)

The equipment that was selected was the SysLogic SDB/HB104PR8H19-EFA1, Railpanel (Build-In Version) 10.4" with E3845, M12 and Sierra Wireless MC7455 that only supports 4G technology.

To have 5G capabilities it is possible to use b) equipment.

b) CPE router 5G

The following lists the requirements needed to implement the interface between the strike IN detector and the LX controller:

- System on Module based computer – Quad Core Cortex A53 up to 1.8GHz minimum
- Memory > 4GB
- Storage 8GB eMMC
- Linux Operating System
- Temperature -45ºC to 85ºC
- USB3.0
- M.2 interface B keyed
- Gigabit Ethernet

The equipment that was selected was the Solid-Run – HummingBoard Pulse.

There is also a need for a 5G module with M.2 interface from Telit, Quectel or equivalent.

c) Sensor train presence

The following lists the requirements needed to implement the equipment to detect

- Board rack FRAUSCHER BGT08 42TE
- Sensor FRAUSCHER Radsensor RSR180/K-250
- Power Source FRAUSCHER PSC101
- Interface Communication FRAUSCHER COM-FSE101
- Axle Counter FRAUSHER AEB101

d) PN video camera

The following lists the requirements for the video camera present in the level crossing area:

- Video resolution 720p HD
- Rate 25 to 60 fps
- Decode video H.265; H.264; M- JPEG
- Latency processing <100ms
- Night vision
- Protocols RTP; RTSP; RTCP
- Light sensitivity < 0.07 lux
- Power-over-Ethernet
- Temperature range -40 °C a +70 °C
- Outdoor protection IP67

The equipment that was selected was the Bosch NBE-6502-AL

e) Maintenance tablet or phone

- Screen 1080p as minimum resolution
- Display size minimum 6in
- Android Operating system

Some equipment proposals, that fits the requirement, are:

Xiaomi Mi Mix 3 5G 6GB/128GB
Huawei MATE 20 X 5G
Samsung Galaxy Tab S6 5G

# 11 Task 3.2.11

# *T3.2.11 Gap analysis for safety and security regarding IoT and critical safety systems (MT and signalling)*

This task is led by FCTUC

## 11.1 Analysis of scenarios

Performance requirements such as low latency, high reliability, guaranteed delivery and low response time are essential and influence how security mechanisms should be implemented in critical systems. In a context of balancing safety and security of critical systems especially in critical communications such as alarms and fault detection, security mechanisms should not violate performance requirements.

Primarily, in critical systems the key requirements are integrity, high availability and timely delivery of critical messages. Integration of 5G medium has increased security risks and more actors and therefore data confidentiality has become one of the key security requirements in 5G to prevent unauthorised access and data theft. Careful consideration when adopting confidentiality in 5G is needed so as to adhere to the performance of safety scenarios of critical systems. For example, it is recommended to choose a suitable cipher suite when SSL/TLS is utilised with R-GOOSE or RaSTA to secure peer to peer communications in critical systems.

Technical security aspects of IEC 61850 standard for R-GOOSE communications are entrusted to the IEC 62351 standard. It addresses security concerns by providing Message Authentication Code (MAC) or digital certificates as means to achieve message integrity and authenticity. The standard recommends having confidentiality in applications that have more than 4ms response time. In 5G IoT networks, specific security considerations have to be made such as, adoption of secure tunnels when packets traverse public domains in order to prevent eavesdropping of data [1].

Alternatively, Layer 2 Tunnelling Protocol over IPSec can be used to create secure tunnels [2]. Another new approach is implementation of Key Distribution Centre (KDC) by using Group Domain of Interpretation Protocol (GDOP) and Simple Certificate Enrolment Protocol (SCEP) protocols so as to enable secure peer to peer R-GOOSE communications with Digital certificates [3]. This could be an effective solution because it is mentioned by the latest standard and works with R-GOOSE protocol.

In railways, the RaSTA protocol provides MD4 hashing algorithm for message integrity and authenticity, however stronger hashing algorithms should be considered to protect against collision attacks [4]. Furthermore, SSL/TLS with suitable ciphers are recommended for securing device to device communications in Railway signalling systems.

In BodyKit applications, Bluetooth Secure Secret Pairing with 6-digit alphanumeric code is used but it is vulnerable to Man in the middle attacks [5]. In Broker/client scenario SSL/TLS is utilized [6] but considered heavy and lightweight cipher such as MISTY and its successor KASUMI are recommended by 3GPP.

The following table provides more details of current security features supported by communication protocols used in Energy grids, Railway signalling and BodyKit systems.

| **Use case/Communication protocol** | **Current security mechanisms** | **Covered security requirement/Comment** |
|---|---|---|
| Energy grids: R-GOOSE | ❖ Message Authentication Code (MAC) without encryption to assure message validity. | ❖ For **data integrity** and **authenticity**. No data confidentiality. |
| | ❖ Transport Layer Security with suitable cipher suite in order to comply with both low latency requirements and timeliness and guaranteed delivery. | ❖ For securing P2P communications. In case of cipher suite selection, performance experiments are needed to test **latency** and **timeliness** requirements. |
| | ❖ Another approach is SSL/TLS Proxy to secure communication in 5G medium with crypto functionalities performed in CPE. | ❖ For securing P2P communications however this approach does not secure local R-GOOSE P2P communications. |
| | ❖ Alternatively, secure tunnels by using GOOSE with L2TP over IPsec. | ❖ For securing P2P communications by using lower layer protocol. |
| Railway signalling: RaSTA | ❖ MD4 Hashing | ❖ For **message integrity** and **authenticity**. |
| | ❖ Transport Layer Security with suitable choice of ciphers to stay in line with low latency and also timeliness and guaranteed delivery. | ❖ For Securing device to device communications. Experiments are needed to test different cipher suites. |
| | ❖ IPsec | ❖ Alternative for securing communications |
| BodyKit(Bluetooth & MQTT) | ❖ Secure Secret Pairing (SSP)with 6-digit alphanumeric code in Bluetooth communications. Public keys are used to share the mentioned code. | ❖ **Device to Device authentication** but vulnerable to man in the middle attacks. |
| | ❖ SSL/TLS with digital certificates in MQTT communications. | ❖ For securing client server connections but considered heavy weight for IoT. 3GPPP recommends lightweight algorithms such as KASUMI, elliptic light etc. |
| | ❖ Access Control Lists in Broker/client scenario. | ❖ For **authorization** of Broker resources i.e. access to MQTT topics. |

**Table 18: current security mechanisms in our use cases.**

## 11.2 Gap analysis

In previous section we have seen current security features that can be utilized with communication protocols used in our three scenarios. In this section we will explore specific security requirements left and their possible solutions that can be applied in our use cases.

Communication protocols in our three use cases have less specifications and no specific details on how security mechanisms should be implemented to provide security. A key security requirement to all three use cases is preventing illegal access of system. This is achieved by first, proper identification of communicating entities before usage of authentication and authorization processes. Usage of 5G network slicing and VPN will ensure only known devices are able to establish communication therefore acting as a first layer of defense against fake/rogue node DoS attacks. Network slicing will also enable closer monitoring of networks and easiness in security policy creation. Alternatively, firmware ID, TPM chip and Pre-shared keys may be adopted for identity establishment. After Identity establishment and management, device authentication becomes a main focus in our scenarios. Distributed architectures require effective mechanisms for device authentication. These mechanisms can be grouped mainly in two groups; mutual authentication and group authentication. The former can be implemented by using either username/password combination or use of digital certificates by setting up a Public Key Infrastructure. Furthermore, multifactor authentication can be used to enhance mutual authentication mechanisms. For instance, two mechanisms such as, use of digital certificates as well as testing device capability can be used together to enhance security [7]. In this case, the device to be authenticated and authorized is sent a puzzle and the perform an operation as a test and send back a response in order to validate its authenticity. Another approach is a simple scalable group authentication, by which devices are authenticated together once based on certain common characteristic such as location, device type, firmware version or functionality. This type of mechanism not only minimizes overheads introduced by simultaneous authentication requests of connected devices but also it provides effective control of device resources.

| Use case/Communication protocol | Security requirement | Security solutions |
|---|---|---|
| Energy grids: R-GOOSE | ❖ Identity establishment and management | ❖ 5G network slicing and VPNs<br>❖ Firmware ID<br>❖ Trusted Platform Module chip<br>❖ Pre-shared Keys |
| | ❖ Device authentication and authorization. | ❖ Group based device **authentication** and **authorization** mechanism using Secret Sharing algorithm [8].<br>❖ Private Blockchain platform with Zero knowledge algorithm for **Privacy** [9]. |
| | ❖ Secure P2P R-GOOSE communications (local and in 5G medium) | ❖ KDC with Digital certificates enabled by Simple Certificate Enrollment Protocol (SCEP) and Group Domain of Interpretation Protocol (GDOI).<br>❖ Private Blockchain platform. |
| Railway signalling: RaSTA | ❖ Identity establishment and management | ❖ 5G network slicing and VPNs<br>❖ Firmware ID<br>❖ Trusted Platform Module chip<br>❖ Pre-shared Keys |
| | ❖ Device to Device authentication | ❖ Group based device **authentication** and **authorization** mechanism using Secret Sharing algorithm. |
| | ❖ Message integrity and authenticity | ❖ Stronger up-to-date hashing algorithms i.e. Blake2b, SipHash-2-4, HMAC-256. |

| | | |
|---|---|---|
| | ❖ User authentication and authorisation i.e. maintenance agents | ❖ AAA VNF and Firewall VNF.<br>❖ VPN clients. |
| | ❖ Securing surveillance video transmission | ❖ SSL/TLS with suitable ciphers.<br>❖ IPsec |
| BodyKit application | ❖ Identity management of devices | ❖ Firmware ID<br>❖ Pre-shared keys |
| | ❖ Secure device to device communication in Bluetooth | ❖ SSL/TLS in application layer for E2E secure channel. |
| | ❖ User authentication in Bluetooth communications. | ❖ Zero knowledge mechanism to enhance **authentication privacy**. |

**Table 19: Specific security requirements and possible solutions**

For a Common Framework a general, step by step approach may include, first, devices in the network should have capability to form groups dynamically by using a certain similar characteristic such as location, firmware version or functionality. Next step is for AAA server to authenticate the formed group. Each group could have a group leader that communicate with AAA server to authenticate its group members. Alternatively, Secret Sharing Schemes (SSS) such as Shamir and Blakey algorithms can be considered [10] where by each member of group shares its part of shared secret key that is combined together with other group members. Instead of having a group leader each device takes active role during authentication and authorization. The proposed new mechanisms aim to overcome network overheads and preserve privacy. In terms of Privacy, zero knowledge mechanisms for authentication can be considered for authentication without exposing critical information of IoT devices.

# 12 Task 3.2.12

# *T3.2.12 Requirements specification of an Intelligent Video Surveillance System in Ultra-High Mobility, using MEC*

This task is led by Ubiwhere

## 12.1 Analysis of scenarios

As described in the previous deliverable, it is intended with this use case to implement a video surveillance system to assist the monitoring of railroad crossings in order to decrease the number of accidents that occur on those particularly hazardous areas. By exploiting Multi-access Edge Computing (MEC) capabilities, it is possible to design a cost efficient surveillance system capable of auto-detecting obstacles on railroad crossings while simultaneously providing a video live feed to the train conductor.

The architecture of the solution is represented in the next figure and is composed by four main elements, (I) camera, to provide live images of 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.

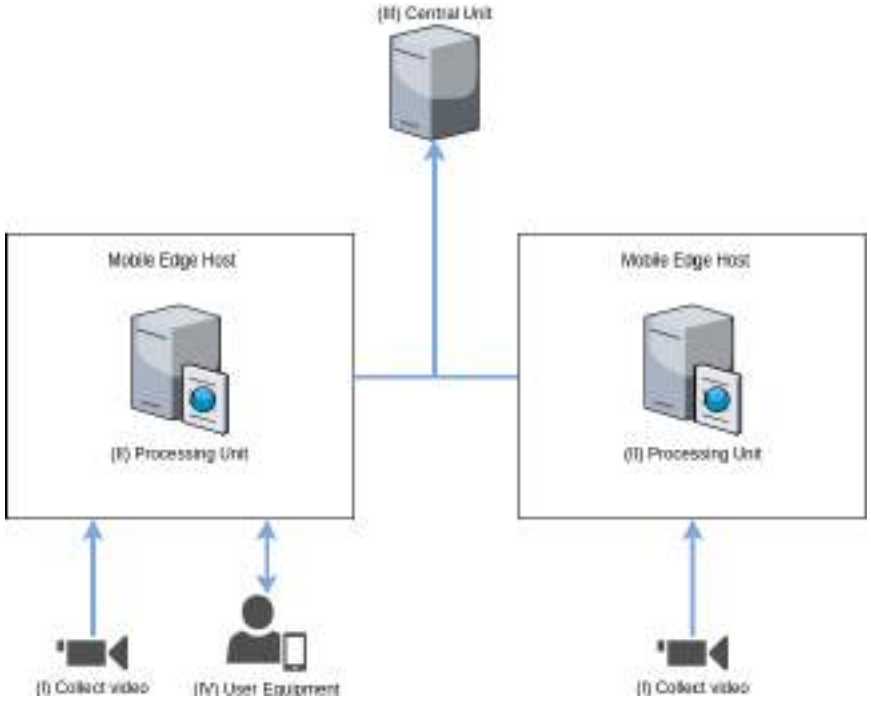



Figure 7. solution architecture

The system's behavior 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.

The following figure 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 suspicious 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.

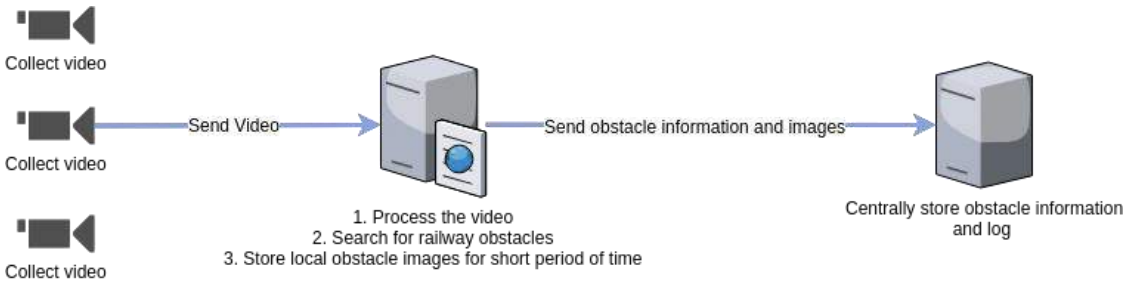



Figure 8. Video analysis

The notification stage only involves the user equipment and the processing unit, as depicted in the following figure. When a user equipment is registered in a mobile edge host it will receive (I) live feed of a given camera nearby 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.

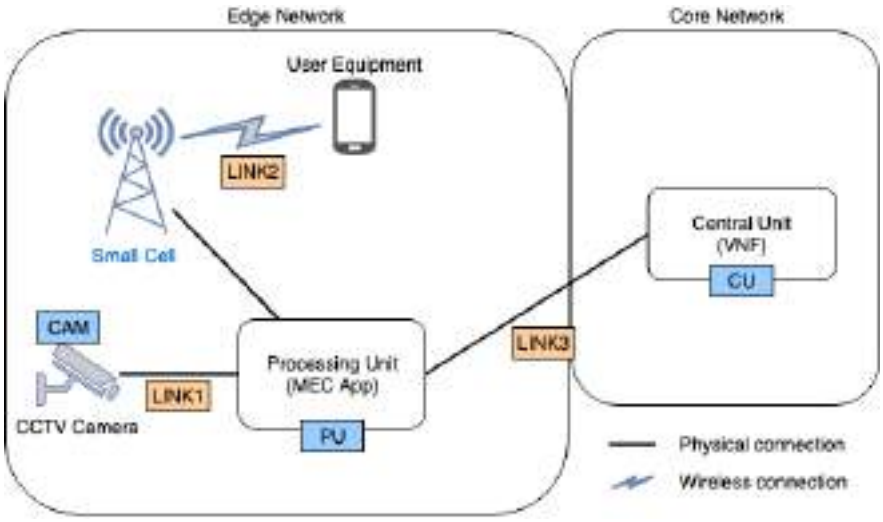

Figure 9. Notification stage

The upcoming 5G technology using MEC infrastructure with promised low latency service response is the key that enables the service, allowing fast video processing and live feed within the network's edge. Due to cost restraints the system is intended to use 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.

## 12.2 List and description of requirements

This section describes the hardware and functional requirements that are specific to the solution itself. It assumes that the MEC orchestrator is already provided, as well as the core network.

In order to provide a more comprehensive description of the requirements, the following figure shows all the actors involved in the scenario that are further described in this section.



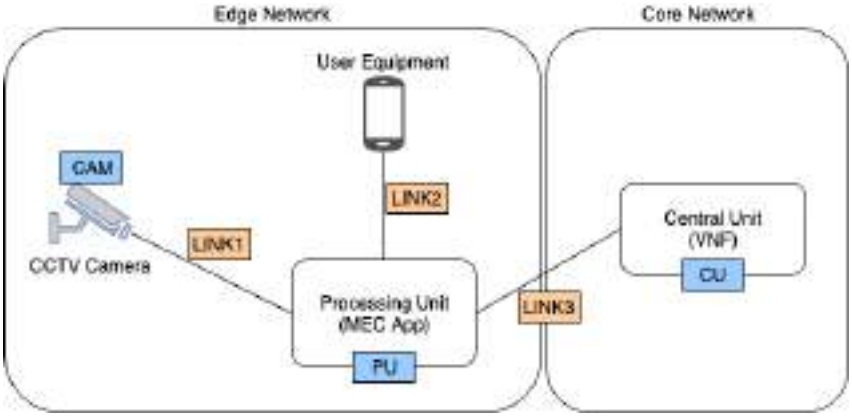



Figure 10. Use-case flow and actors

During the implementation and testing of the proposed solution, the following hardware, software and functional requirements were identified.

**Hardware Requirements**

The hardware requirements are specified in the following table. The video source should be obtained using a CCTV camera which will be physically linked to the Processing Unit virtual machine. The Processing Unit MEC application should have the processing power to detect and classify objects in the railroad crossing as well as the capability to broadcast the video live feed to user equipment that are in-range of the MEC antenna. The Central Unit VNF requirements were also specified regarding the amount of resources needed to aggregate and store the events generated by the Processing Unit.

| ID | Description |
|---|---|
| CAM | CCTV network camera:<br>- 4K resolution, 25fps<br>- 1/1.7 MOS sensor<br>- H.264 or H.265 encoding<br>- Water resistent IP66<br>- Position:<br>o Between 6 an 8 meters above site ground<br>Oriented to NW, N or NE tilted at a suitable angle to point towards and frame the railroad crossing |
| PU | Processing unit MEC app:<br>- 10 vCPUs<br>- 16 GB RAM<br>- 20 GB storage |
| CU | Central unit VNF:<br>- 8vCPUs<br>- 8 GB RAM<br>- 40 GB storage |

**Table 20: Hardware requirements**

**Functional requirements**

Regarding the links required for the correct functioning of the solution, the connection between the Camera and the Processing Unit should provide a suitable bandwidth to transmit 4K resolution videos at 25 fps with a low latency. Similarly, the link between the Processing Unit and the User Equipment should account for the transmission of 4K resolution video, at the same frame rate, plus the transmission of notifications and incident alerts. The availability of both these links is crucial for the real time analysis of the railroad crossing and broadcast of the live feed to the user equipment located inside the train. The link between the Processing Unit and the Central Unit can be more relaxed in terms of availability as it is not mission critical.

Another functional requirement is the support for video multicast. Upon being registered in the edge network, multiple End User Equipments should receive the video live feed from the railroad crossing area. In order to save bandwidth and processing resources, the video should be transmitted in multicast, instead of having multiple dedicated links streaming video.

| ID | Description |
|---|---|
| LINK1 | Link between Camera and Processing Unit:<br>- 25 Mbit/s<br>- Jitter less than 10 milliseconds<br>- Physical link (99,9% availability)<br>- |
| LINK2 | Link between Processing Unit and User Equipment:<br>- 30 Mbit/s<br>- Jitter less than 10 milliseconds<br>- Radio link (99,9% availability, once in range with the edge network small cell) |
| LINK3 | Link between Processing Unit and Central Unit (core network):<br>- 25 Mbit/s<br>- Best effort link |

| | |
|---|---|
| MULTI | Video should be broadcasted in multicast |
| | |

**Table 21: Functional requirements**

# 13 Architecture Definitions : Task 3.2.1

# T3.2.1 General architecture for real-time distributed protection systems for medium voltage energy networks

This task is led by EFACEC Energia

## 11.1 IEC 61850 GOOSE overview

GOOSE, is a time-critical network protocol specified on IEC 61850 to enable horizontal communication among IEDs in substations – It was designed to ensure fast and reliable communication for protection purposes. For example, if an IED detects a critical situation (such as a massive overcurrent) it must actuate the circuit breaker and trigger a message (GOOSE frame) for other devices to warn them.

Taking into consideration the OSI (Open Systems Interconnection) model, GOOSE is a layer 2 protocol. This fact leads to two important conclusions: there is no IP addressing and devices exchanging data through GOOSE must be in the same LAN (Local Area Network). GOOSE data is directly embedded into ethernet frames and it is based on a multicast publisher-subscriber mechanism. The following figure presents the structure of a typical ethernet frame, on which GOOSE is also based.

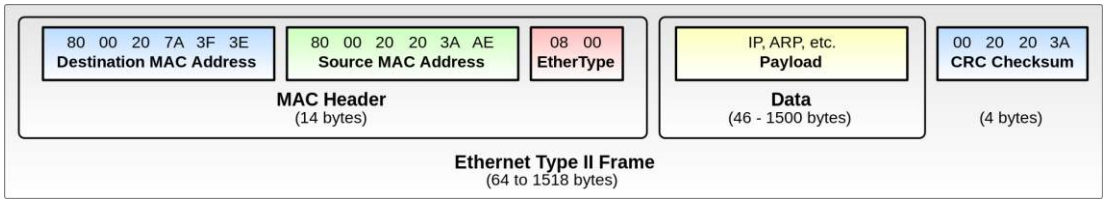



**Figure 11 - Structure of a typical ethernet frame**

The GOOSE protocol defines a multicast publisher-subscriber mechanism. This means that an IED might be publishing and/or subscribing GOOSE events:

- When publishing, the sender generates an ethernet frame whose destination MAC address is a multicast address – multicast addressing on layer 2 is achieved by having the least significant bit of the first octet set to '1'. Additionally, the source MAC address is its own physical MAC address, the field EtherType is 0x88B8 and VLAN and priority tagging (IEEE 802.1Q) is used to have a separated virtual network within the same physical network and to set higher priority. When a GOOSE frame reaches a network switch, it is transmitted via multicast to all ports, ensuring that all devices on the same network receive it (even if those devices are not subscribing them);

- When subscribing, the receiver keeps listening for GOOSE frames. If not configured to subscribe GOOSE frames, an IED discards them when they are received.

The GOOSE protocol specifies a retransmission curve and a heartbeat, as exemplified in the following figure:

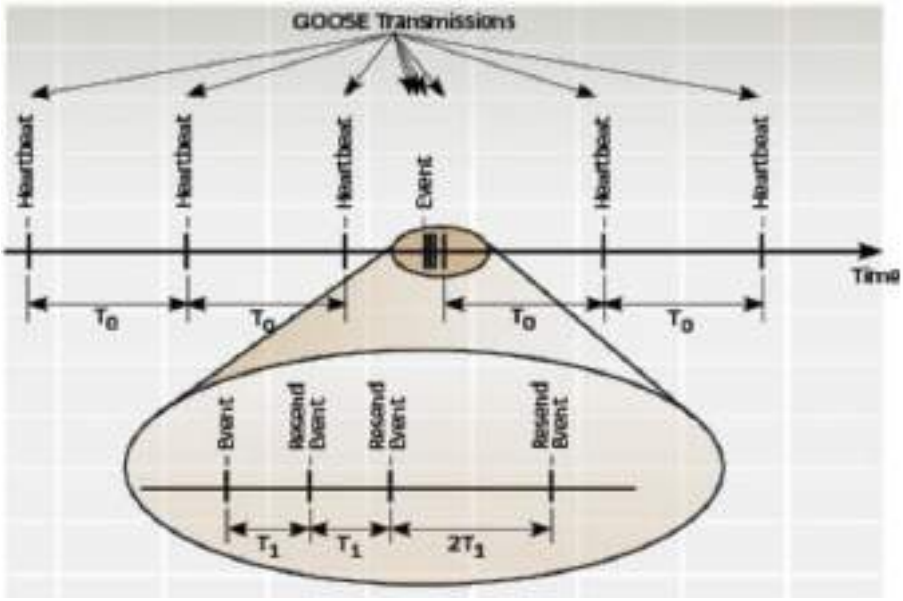



**Figure 12 - Heartbeat and retransmission curve when publishing**

If the network infrastructure fails, the subscribers are not going to receive the heartbeat. Therefore, the heartbeat is used by subscribers to realize that there is a communication issue. The retransmission curve is a very quick burst of GOOSE frames sent by publishers whenever the published data changes its state in order to ensure that subscribers are notified regarding the event.

### 13.1.1 Routable-GOOSE

As mentioned in section 10, one of the major characteristics of the GOOSE protocol is that it is mapped on the layer 2 of the OSI model – this fact constrains GOOSE communication to LANs. Over the recent years, the need for GOOSE communication over WAN (Wide Area Network) has come up. Therefore, an extension to the GOOSE protocol has been created – Routable-GOOSE (R-GOOSE). It is a communication protocol very similar to GOOSE (it encapsulates all the content available on a GOOSE frame) except the following aspects: transportation and security.

Regarding transportation, R-GOOSE uses the UDP/IP stack with multicast or unicast addressing. This enables communication over WAN based on the major characteristics of GOOSE: time-critical, high speed, high priority, multicast and publisher-subscriber mechanism. When multicast is used on R-GOOSE publication, the IP range is 224.0.0.1 to 239.255.255.255. Additionally, the ToS (Type of Service) of the IP header might be set to increase priority to the R-GOOSE packets. R-GOOSE might also be used for unicast environments – it is just necessary to use unicast IP addresses. The publisher sends R-GOOSE packets using an UDP client and the subscriber receives them on port 102 of an UDP server.

Regarding security, GOOSE protocol does not address it. In most cases, it has not been considered critical on access controlled LANs inside of a substation. On the other hand, when communication over WAN is used (it is the case of R-GOOSE protocol), it performs a critical role. Taking into account that the R-GOOSE protocol is used for protection purposes, it is very important to ensure integrity – someone who is malicious cannot change the content of a R-GOOSE packet. The standard IEC 62351-6 specifies measures for such insurance. One of the measures consists on generating and attaching an encrypted hash code to the packet that is published. Afterwards, when it is received, the subscriber uses the hash code to validate the R-GOOSE packet integrity.

The following figure presents the structure of a typical R-GOOSE packet, evidencing the fields related to the GOOSE data and the additional ones related to security and transportation.

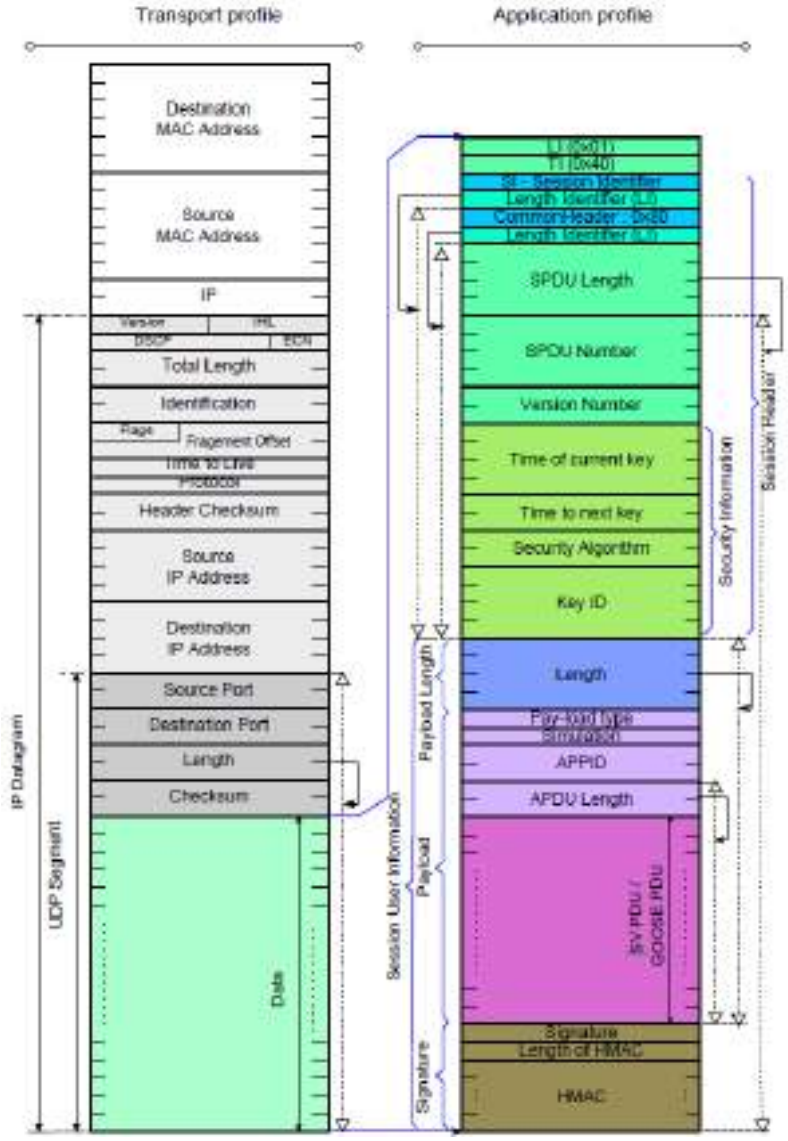



**Figure 13 - Structure of a R-GOOSE packet**

# 11.2 Architecture definition for medium voltage real time distributed protection systems

As described in section 2, the use case includes two substation IEDs, three field IEDs, and an engineering station running on a virtual machine. Each IED and the engineering station are connected to the 5G network via a dedicated user equipment (UE). This architecture is represented in Figure 14.

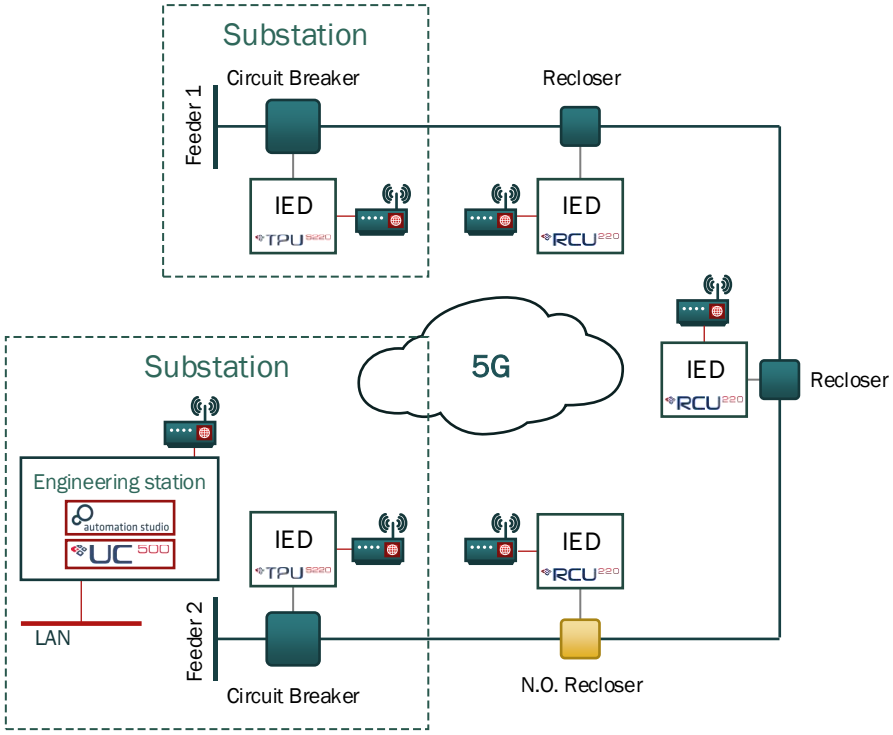



**Figure 14. Network architecture.**

The use case considers time-critical peer-to-peer R-GOOSE communication between power system protection and control IEDs. Communications between a substation engineering station and the IEDs will also be included.

The use case communication architecture is represented in Figure 15. The indicated R-GOOSE streams correspond to the message flows required for the defined smart grid topology, taking into consideration that IED 4 is a N.O. point and all possible alternative grid configurations caused by self-healing sequences. Non-time-critical communications between the engineering station and the IEDs are also represented.

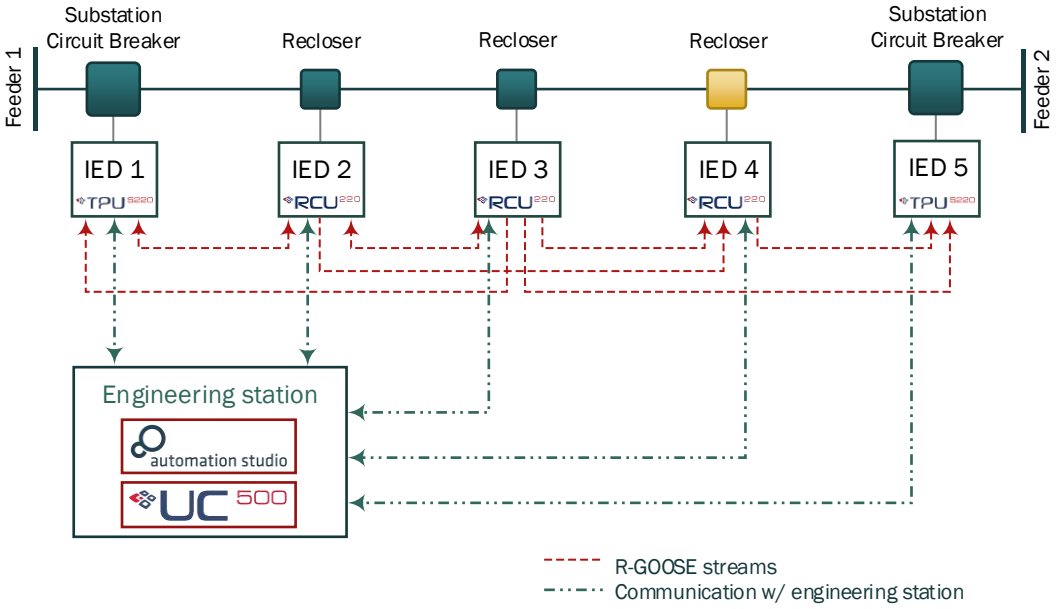



**Figure 15. Communication architecture.**

Peer-to-peer communication between IEDs is critical for the correct operation of the proposed algorithms and should be considered priority. The R-GOOSE messages are published as continuous streams that are constantly monitored by the subscribers – if one of these links fails or suffers a significant delay, it may compromise the entire system. Therefore, it is crucial that the 5G communication infrastructure guarantees the required levels of latency, bandwidth, reliability and availability, even in adverse conditions.

# 14 Architecture Definitions: Task 3.2.5

# Task 3.2.5 Architecture for railways signalling solution supported by 5G communications

This task is led by EFACEC Engenharia

## 14.1 General architecture definition for 5G railway signalling systems

Figure 16 depicts the logical architecture for the connected worker use case, including all the necessary components and labelled interfaces, which are further explained and justified in Table 1 and Table 2. In this case the operator provides and manages the Vertical service in a Slice as a Service model.

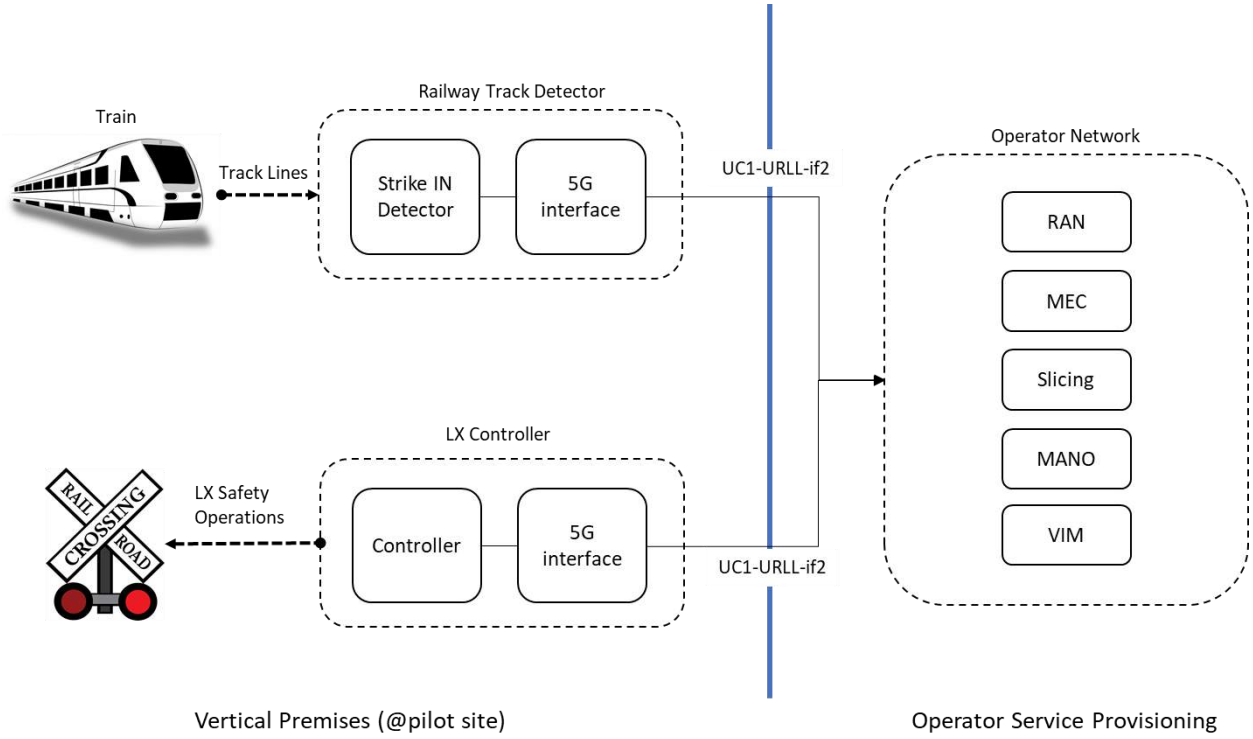



**Figure 16: Logical architecture EFACEC_S-UC1**

**Table 1: EFACEC_S UC1 Logical Architecture Components**

| Component | Description | Location |
|---|---|---|
| **Train** | The machine responsible to transport people or freight. | Aveiro Harbor |
| **Strike in detectors/axle counter train detector system** | Device (system) that can detect if a train is approaching the level crossing area. | Level Crossing area-Aveiro Harbor |
| **Train detectors/axle counter train detector system** | Device (system) that detects if the train is occupying the Level Crossing section or to the detect the absence of the train in that section | Level Crossing area-Aveiro Harbor |
| **Traffic lights** | Device that is installed in the Level Crossing area and is responsible to process traffic information | Level Crossing area-Aveiro Harbor |
| **Lx protection signals** | Device used to inform the train driver that he can proceed (level crossing is free), or if he must stop the train (level crossing is occupied, or its operation status is unknown). | Level Crossing area-Aveiro Harbor |
| **LX controller** | Shelter of devices that receive sensors and equipment information, process this information and assures the LX actions (railways signaling operation). | Level Crossing area-Aveiro Harbor |
| **Half Barriers** | The device that physically protects the Level Crossing against non-authorized entrances. | Level Crossing area-Aveiro Harbor |
| **5G Interface** | Mobile network interface able to connect to a 5G mobile network. | Strike IN Detector/LX Controller at the Railway track |
| **Operator Network** | 5G Mobile network covering the level crossing | Mobile Operator/Altice Labs/Aveiro Harbor |
| **RAN** | The RAN portion of the operator's mobile network | Mobile Operator/Altice Labs |
| **MEC** | The MEC portion of the mobile operator, allowing for lower latency service provisioning whenever needed. | Mobile Operator/Altice Labs |
| **Slicing** | Network slicing capability whenever needed | Mobile Operator/Altice Labs |

| | | |
|---|---|---|
| **MANO** | Mobile Network Management and Orchestration capability. | Mobile Operator/Altice Labs |
| **VIM** | Virtualized Infrastructure Management Capability | Mobile Operator/Altice Labs |

**Table 2: EFACEC_S UC1 Interfaces and Requirements.**

| Interface | Services | Requirements (KPIs) | Slice Type |
|---|---|---|---|
| UC1-URLLC-IF1, UC1-URLLC-IF2 | Train sensors to LX communications | 1.2Kbit/s, 10ms, 99.99%, - | URLLC |

Figure 17 depicts the logical architecture for the connected worker use case, including all the necessary components and labelled interfaces, which are further explained and justified in Table 3 and Table 4. In this case the operator provides and manages the Vertical service in a Slice as a Service model.

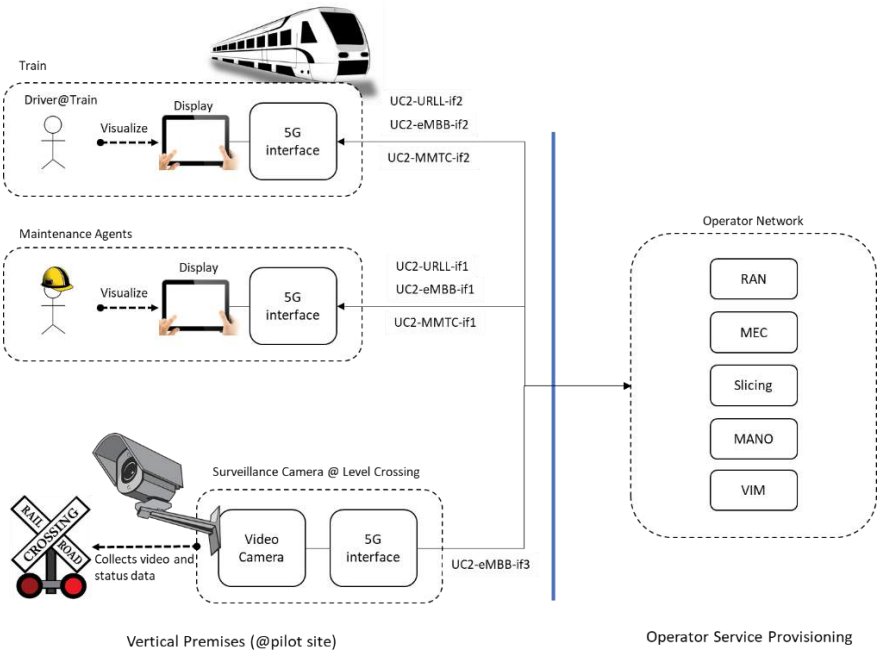



**Figure 17: Logical architecture EFACEC_S-UC2**

**Table 3: EFACEC_S UC2 Logical Architecture Components**

| Component | Description | Location |
|---|---|---|
| **Train** | The machine responsible to transport people or freight. | Aveiro Harbor |
| **Tablet/Mobile Devices:** | Devices to be installed in the train and to be used by maintenance agent to monitor the level crossing area (video) and to assure the proper installation operation | Train/Aveiro Harbor |
| **HD Video Camera:** | Device (video camera) that will be installed in the level crossing area and allows surveillance and image transmission to the train and to a command center. | Level Crossing area-Aveiro Harbor |
| **Command Centre:** | Technical and Operation rooms to support the monitor and control of the Level Crossing. | Level Crossing area-Aveiro Harbor |
| **LX controller** | Shelter of devices that receive sensors and equipment information, process this information and assures the LX actions (railways signaling operation). | Level Crossing area-Aveiro Harbor |
| **GPS position system** | Device to be installed in the train in order to report its geographical positioning. | Train-Aveiro Harbor |
| **5G Interface** | Mobile network interface able to connect to a 5G mobile network. | Train, Maintenance Crew Terminal, Surveillance Camera |
| **Video Camera** | HD video camera able to send video stream over a network link | Level Crossing-Aveiro Harbor |
| **Operator Network** | 5G Mobile network covering the level crossing | Mobile Operator/Altice Labs/Aveiro Harbor |
| **RAN** | The RAN portion of the operator's mobile network | Mobile Operator/Altice Labs/ |
| **MEC** | The MEC portion of the mobile operator, allowing for lower latency service provisioning whenever needed. | Mobile Operator/Altice Labs/ |
| **Slicing** | Network slicing capability whenever needed | Mobile Operator/Altice Labs/ |
| **MANO** | Mobile Network Management and Orchestration capability. | Mobile Operator/Altice Labs/ |

| | | | | | |
|---|---|---|---|---|---|
| **VIM** | Virtualized Capability | Infrastructure | Management | Mobile Labs/ | Operator/Altice |

**Table 4: EFACEC_S UC2 Interfaces and Requeirements**

| Interface | Services | Requirements (KPIs) | Slice Type |
|---|---|---|---|
| UC2-eMBB-IF1, UC2-eMBB-IF2, UC2-eMBB-IF3 | HD video on the train (near real-time), sent from the surveillance camera at the level crossing | 14Mbit/s, 5-100ms, 99.9%, 160Km/h | eMBB |
| UC2-URLLC-IF1, UC2-MMTC-IF1, UC2-URLLC-IF2, UC2-MMTC-IF2 | Real-time sensors data monitoring | 1.2Kbit/s, 10ms, 99.99% | URLLC |

# 15 Architecture Definitions : Task 3.2.13

## *T3.2.13 Definition of Bodykit architecture and interfaces with support for sensors and real-time video over 5G networks*

This task is led by OneSource

This section addresses an architecture for Bodykit, which enables a situational awareness platform for teams performing missions in the field.

## 15.1 General architecture

Is compliant with an IoT architecture, to enable the collection of information from several devices in a scalable way. This information from sensors enables an enhanced situational awareness at Command Control Centres (CCC), for instance, operators and commanders can have a view in real time of the PPDR forces that are in the field, as well as the type and assets that are operating in the field (e.g. terrestrial, aerial assets, etc.).

The Bodykit architecture includes two channels: the control to allow the management devices, to perform actions and the data channel that is intended to allow the collection, visualization of information. The data channel includes the information flows and includes also alerts/alarms that can be triggered according to define thresholds.

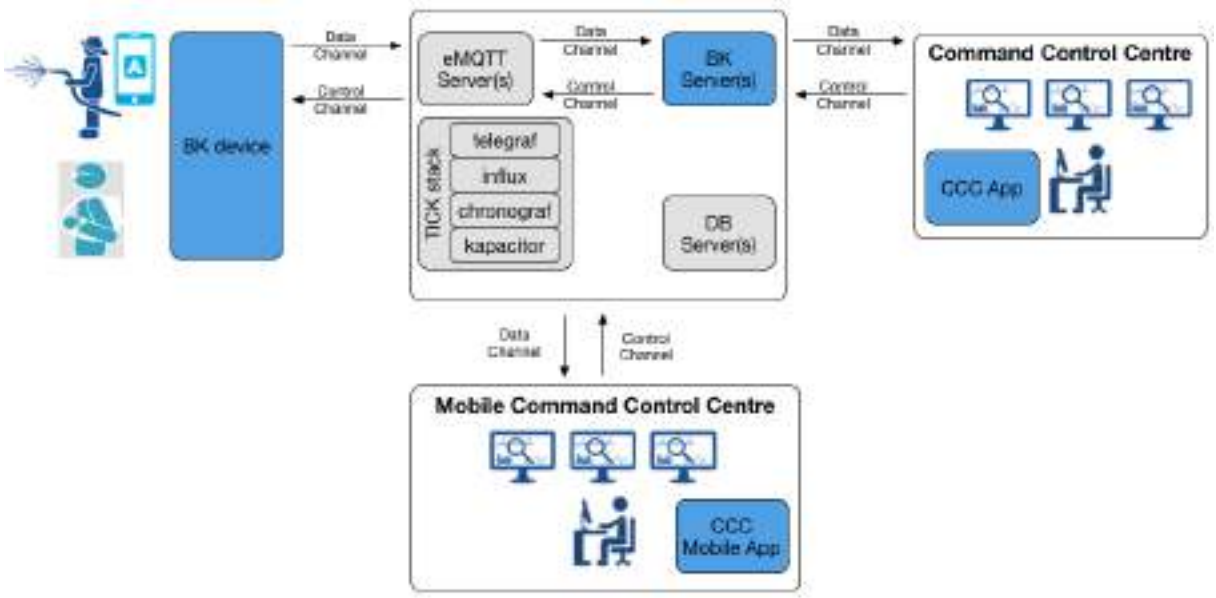



**Figure 18 - Bodykit Architecture**

The Bodykit architecture, as depicted in Figure 18, includes three major components:

- The Bodykit device, which can run on mobile devices or can be a dedicated device, which functionality is the collection of sensor data and respective aggregation for transmission to the Bodykit Server(s).
- The Bodykit Server(s) that perform the analysis of data to support situational awareness. The BK server interacts with other elements like the TICK stack from Influxdata that 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 CCC application which is crucial for the situational awareness, and can run on multiscreen devices (very common in Control rooms) or in mobile devices (e.g. tablets).

The MQTT server (based on eMQTT) requires authentication and employs an ACL plugin to authenticate users and to manage the access control to topics.

## 13.2 Bodykit Components

### 15.2.1 Bodykit Device

There are two types do Bodykit Devices:

- The Bodykit Device that is a wearable platform with biosensors and environmental sensors.
- An application running in a mobile phone and collecting information from sensors via Bluetooth.

The BodyKit Device is a wearable equipment that collect information from sensors and transmit such information to the BodyKit Server.

The Bodykit Device supports the following sensors:

- Biosensors, sensors that are employed to collect biophysical parameters of PPDR users. Such sensors can include:
    - Electrocardiogram (ECG)
    - Respiration Rate (RR)

    - Blood Volume Pressure
    - Heart Rate
    - Temperature
- Environmental sensors collect information from environment and can include:
    - Gas detection including CH4, CO, Benzine
    - Smoke detection
    - Humidity
    - Environment temperature
    - Location based on GPS

The Bokdykit Device also supports bidirectional audio and HD video, which can be customized according to the network settings. The transmission of information can be performed using public or private mobile networks (e.g. LTE, 5G) or via WiFi. Within safety concerns the Bodykit Device includes an emergency button to enable an agent in the field to request assistance in emergency situations (e.g. Man Down).

### 15.2.2 BK Server(s)

The BodyKit Server (BKS) manages all the communication between the components of the service, as well as all other operations that are computationally heavy. For instance, the BKS runs algorithms that process the information from sensors to detect hazards such as Man Down, or stress conditions (e.g. high levels of fatigue due to prolonged mission service).

A key role of BKS includes the authentication and authorization procedures for all the communications, and the request to configure the QoS settings in the network for information flows. The information flows managed by the BKS are summarized in the next Table.

| Information flow | Description | 5G parameters configuration (configured according **to** ETSI TS 23501) |
|---|---|---|
| Priority flow | Flow for emergency events, like detection of man Down, emergency button | Resource Type = Guarantee Bit Rate (GBR), delay critical GBR<br>Priority level = Highest level (11)<br>Packet Delay Budget (PDB) = 20 ms<br>Packet Error Rate (PER) = 10-6<br>Averaging Window = N/A<br>Maximum Data Burst Volume = 320 B |
| Video and audio flows | Flow for real-time HD video and bidirectional audio | Resource Type = Guarantee Bit Rate (GBR),<br>Priority level = Medium (40)<br>Packet Delay Budget (PDB) = 150 ms |

| | | |
|---|---|---|
| | | Packet Error Rate (PER) = 10-3<br>Averaging Window = N/A<br>Maximum Data Burst Volume = N/A |
| Sensors data flow | Flow with collected data from biosensors and environmental sensors | Resource Type = Non-GBR<br>Priority level = Medium (55)<br>Packet Delay Budget (PDB) = 200 ms<br>Packet Error Rate (PER) = 10-6<br>Averaging Window = N/A<br>Maximum Data Burst Volume = N/A |
| Regular data | Flow for exchange of data, like mission details | Best effort (default classes) |

**Table 5: Information flows managed by Bodykit Server**

The BKS also performs the configuration of devices (BKD) and manage the real-time communications with the devices.

In summary, with the received data, the BKS performs three tasks:

- Data Aggregation: data is aggregated per user and forward to registered CCC (according to their authorization);
- Data Inspection: data is inspected to detect alert situations (e.g. location, vital signs);
- Data Store: data is stored in a database for off-line processing and history visualization.

The internal architecture of the BKS includes other components, are described in the next sections.

### 15.2.3 MQTT Server(s)

The MQTT Server(s) employ a eMQTT solution. 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.

Some of the used topics are summarized in the following table.

| Topic Name | Description |
|---|---|
| tenantid/deviceid/data/<SENSOR_ID> | Topic for a specific/event |
| tenantid/deviceid/control/device | Topic to manage a device:<br>CRUD Topics |

| | |
|---|---|
| tenantid/deviceid/control/server | Authentication /Permission<br>Device Management (Confs, Status of device)<br>Control Actions: WIPE, LOCK, MESSAGES, ACTIVATE GPS<br>Manage Apps: List, retrieve apk, install/uninstall<br>Alerts for CCC |

**Table 6: Examples of data and control topics in MQTT**

### 15.2.4 TICK Stack

A TICK stack relies on the Open Source solution of InfluxData. Real-time series database is employed to allow a scalable and efficient analysis of the information collected from sensors. The time series is assured by the InfluxDB, while the telegraf component retrieves the information sent to the topics in the MQTT and forwards the data to the influxdb to enable the analysis by BKS. The kronograf component enables an alarm system, namely for thresholds configuration: value is above a certain limit, values are inside a range, among other sets.

The chronograf component is not strictly required but allows to verify, in a simple way that the overall system is working without problems (i.e. BKD is sending data).

### 15.2.5 DB Server(s)

Persistent storage systems are employed to allow the storage of configurations regarding devices and security policies. Additionally, all the sets for missions are also stored in the Database servers, which rely on PostgreSQL.

### 15.2.6 CCC Application

The 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 Ionic framework to allow the development of applications in multiple Operating Systems.

| ID | Functionality Description |
|---|---|
| 1 | Login according user role (username, password and operator or administrator roles) |
| 2 | Show list of devices |
| 3 | Show list of devices pending registration |
| 4 | Show list of users |
| 5 | Support CRUD of users |
| 6 | Support WIPE action on a device |

| | |
|---|---|
| 7 | Support LOCK action on a device |
| 8 | Support install/uninstall of actions on a device |
| 9 | Support sending alert/messages to a device |
| 10 | Allow to modify the default configuration of the collection mechanism in the mobile service (MS) - update frequency, events information, allowed applications and other settings |
| 11 | Support history of events per device |
| 12 | Support history of location (in google maps) |
| 13 | Display current location of device (in google maps) |
| 14 | Display details of device |
| 15 | Change user allowed authentication methods (password, IDGO, NXP) and respective information for login |
| 16 | Support history of devices per user |
| 17 | Support timeline of events with filtering of events, alerts types, date, location... |
| 18 | Support statistics of alerts per type (information, warning, severe/Critical) |
| 19 | Support situation awareness in map (plot unregistered devices and users' devices) |
| 20 | Support search of devices |
| 21 | Support search of users |
| 22 | Handle all the communication through MQTT/TLS |
| 23 | Manage operators (and administrators permission) |
| 24 | Support send files to Mobile Device |

| | |
|---|---|
| 25 | Support Activation of GPS in Mobile Device |

**Table 7: CCC Application functionalities**

The CCC Application must support two approaches:

- Manager – which manages the configuration of PPDR infrastructure, devices that can be registered, users in the system
- Operator – which manages the missions, teams and other operational processes (e.g. perform LOCK action).

# 16 Architecture Definitions : Task 3.2.14

## *T3.2.14 Data mobility reliable architecture specification, using 5G flexible mechanisms, for application in railway signalling systems*

This section addresses a 5G mechanisms-enabled architecture for supporting and enhancing services that have reliable and critical data requirements in machine-to-machine scenarios.

This task is led by IT

## 16.1 General architecture

Our scenario considers a critical and reliable communications environment where an Internet Service Provider (ISP) and/or Cloud Service Provider (CSP) hosts the Network Functions NFs on behalf of an industrial corporation. The ISP/CSP needs to ensure not only the placement of the NF (or VNF) near to the end-users, but also reliable communications with a near zero downtime between version updates and/or failures for those NFs. Due to the critical nature of these VNFs, they are managed as black boxes in order to prevent tampering, which means that the CSP cannot modify in any way the operation of the VNFs. In this line, for our proof-of-concept framework, a virtual firewall (vFW) will be used as an example VNF. The use-case scenario is depicted in Figure 19.

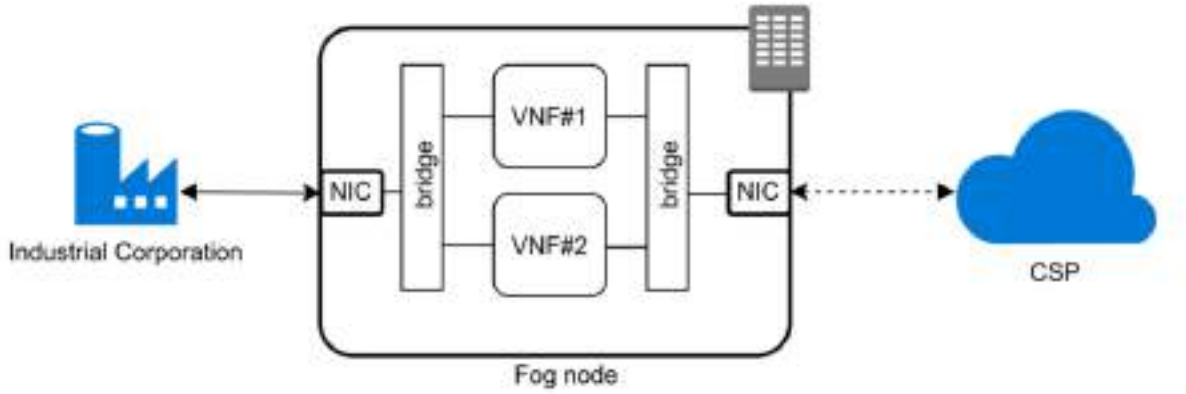



**Figure 19 - Use Case Scenario**

As stated, to cope with the reliability and latency requirements imposed by the industrial corporation, the CSP needs to instantiate the VNFs close to the corporation. For this, the CSP may explore fog computing, however due to hardware resource limitations the probability of failure increases. To overcome such failure events, the CSP requires enhanced failure detection and recovery mechanisms to obtain near zero downtime of VNFs failure and/or updates.

## 16.1.1 Building Blocks

The fog node architecture is composed by the following items:

- Fog Node: The fog node is a computing system that plays the part of a mini-cloud, located at the edge of the network.
- Source Node: The source node constitutes an industrial critical communication process.
- Database: The source node simulates an industrial critical communication.
- Sink Node: This entity is the node that consumes the information provided by the Source Node.
- VNF: The VNF represents the service request by the corporation and hosted by the ISP and/or CSP. The CSP provides secure 3rd party interfaces to the corporation, allowing the latter to provide new versions of its VNFs, without the former tampering with them. However, such interfaces are out-of-scope from this work.
- Open vSwitch bridges: the network bridges ensure the communication between services, while seamlessly redirecting the traffic to the required VNF.
- SDN Controller The SDN controller manages and controls OvS bridges using the OF, by implementing therein flow- based rules. This allows the controller to dynamically redirect the network traffic from one VNF to another in a failure or update event.

## 16.1.2 Recovery Mechanisms

Our framework is supported by a recovery mechanism in order to reduce downtime. In this line, our recovery mechanism can be divided into 3 steps: 1) failure detection; 2) VNF re-instantiation; and 3) data-path update. While Figure 20 depicts the failure detection and re-instantiation mechanisms, Figure 21 shows the sequence messages of the datapath update.

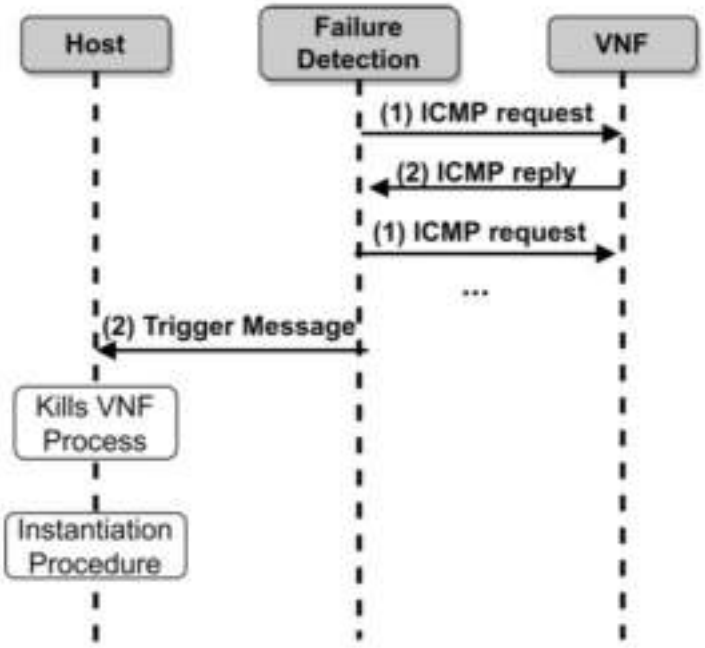



**Figure 20 - Failure Detection and Re-Instantiation Sequence Messages**

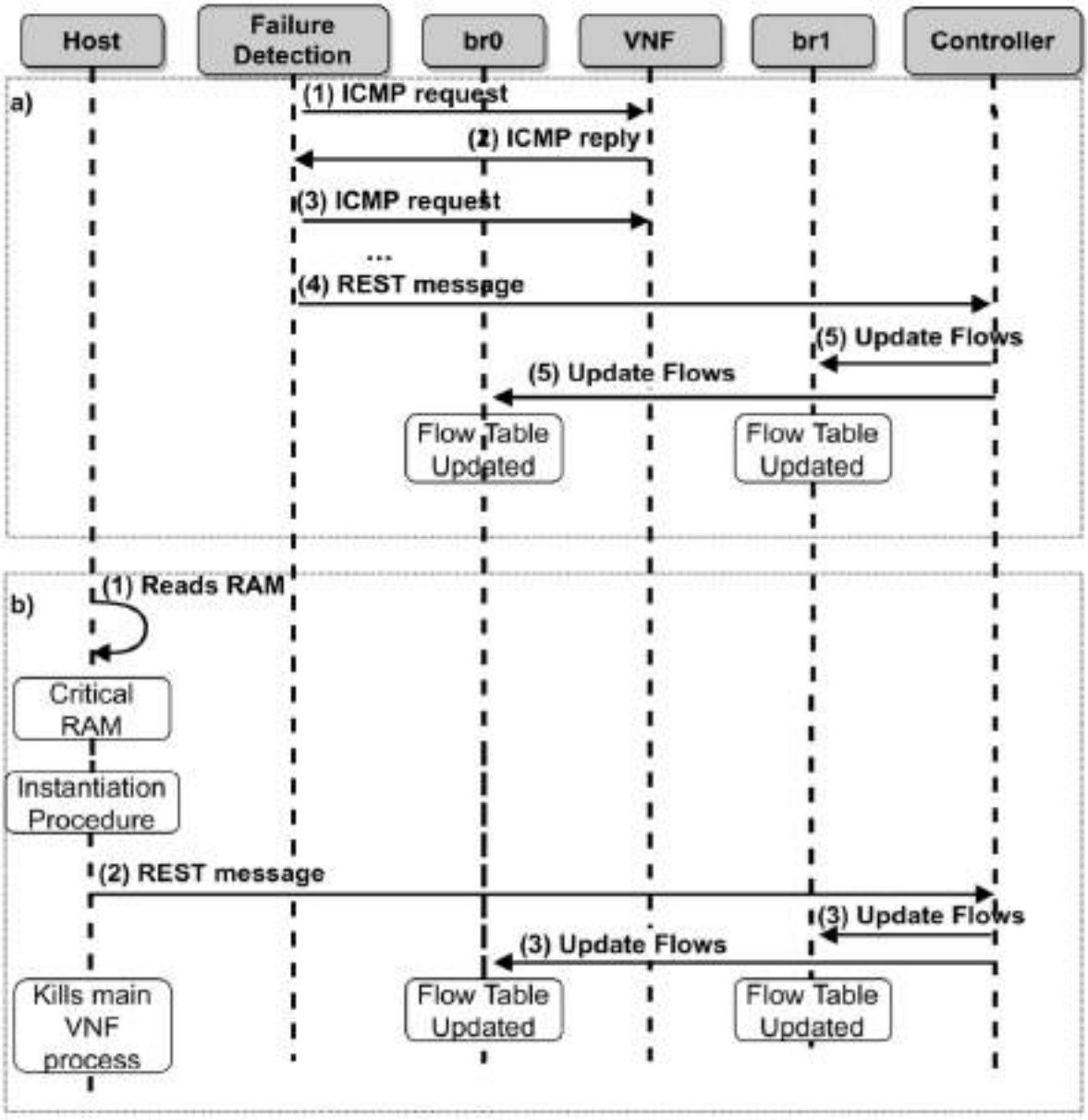



**Figure 21 - Failure Detection and Recovery Mechanism**

### 16.1.2.1 Failure Detection and VNF Re-instantiation

As the ISP and/or CSP need to cope with the possibility of software failures, a failure detection mechanism was developed for verifying the status of operation of the NF, in this case the firewall. This mechanism is based on the heartbeat software developed by the Linux-HA (High-Availability Linux).

Figure 20 illustrates the failure detection procedure, which is described as follows. The failure mechanism periodically sends ICMP requests (1) (every 100ms), and if the VNF responds by sending an ICMP reply (2), the failure mechanism does nothing and proceeds to keep sending ICMP requests (3). When the VNF fails to respond within a 50ms time-frame, a trigger is sent to the host (4). Note that both the ICMP request periodicity and the time-frame for response were chosen for proof-of-concept evaluations and different values can be used in order to optimise the mechanism. After receiving the trigger, the host kills the processes of the VNF to enforce the re- instantiation procedure. The

virtualization technology (i.e., unikernel or container) in which the VNF (i.e, vFW) is going to be re-instantiated is sent in the trigger message. This failure mechanism is an illustrative approach with the sole purpose of triggering dynamic re-adjustments of the system. Other more refined solutions can be used, including monitoring and operation assessment mechanisms more tailored towards commercial environments.

### 16.1.2.2 Datapath Update

To minimize and achieve a near zero downtime of the service, SDN was used for data-path update on-the-fly. As such, our failure detection mechanism informs the SDN controller of failure and requests a flow redirection to the new VNF. To prevent a disconnection between the source and sink nodes during a VNF fail detection event, one of two cases is required: *case a)* a backup VNF for resilience is already running from the beginning; or *case b)* a new VNF is dynamically and pre-emptively instantiated upon trigger of a monitoring mechanism. For this last case, the monitor mechanism can explore KPIs, such as memory usage, which when reaches the memory limit increases the probability of failure. Figure 21 depicts the high-level sequence message for a data-path update upon a failure detection.

**Case a) VNF already instantiated as backup:**

1. The failure detection mechanism sends ICMP requests to the firewall;
2. The VNF replies to those requests;
3. Another ICMP request is sent;
4. Since the firewall does not respond to the CMP request, meaning that an error occurred, a REST message is sent to the SDN controller;
5. After receiving the trigger message, the controller updates the flow tables of both OvS bridges, offloading the traffic to the backup VNF.

**Case b) VNF dynamically instantiated:**

1. The host reads the RAM consumption of the main VNF; When the RAM consumption reaches critical values (80% of total RAM allocated to the VNF, although other values can be configured), the instantiation procedure of the backup VNF begins;
2. When the backup VNF is fully operational, a REST message is sent to the SDN controller;
3. After receiving the trigger message, the controller updates the flow tables of both OvS bridges, offloading the traffic to the backup VNF.

Finally, note that once the OvS bridges update their flow tables, the packets that were previously being sent to the main VNF, are now forwarded to the backup VNF, ensuring the reliability of the service.

## 16.1.3 IEC 61850 Data Transfer over Public Networks

Parallel to the previously explained architecture (which composes the base system contribution of this task), some analysis regarding the usage of the IEC 61850 protocol for transferring data between remote substations was considered, taking advantage of public network links. The base concept is to validate the differences between different kinds of access technologies and their impact for using this protocol in a remote way.

In order to assess the performance of GOOSE messages, three scenarios were devised. The first scenario focuses on the usage of the protocol in the same LAN, using Ethernet and Wi-Fi, illustrated in Figure 22. Raspberry Pi devices were used to implement the Server/Gateway Sender, the Client and the Gateway Receiver. The router is a Linksys WRT1200AC flashed with DD-WRT. PC's were used to access the Raspberry Pis via SSH or VNC (for GUI).

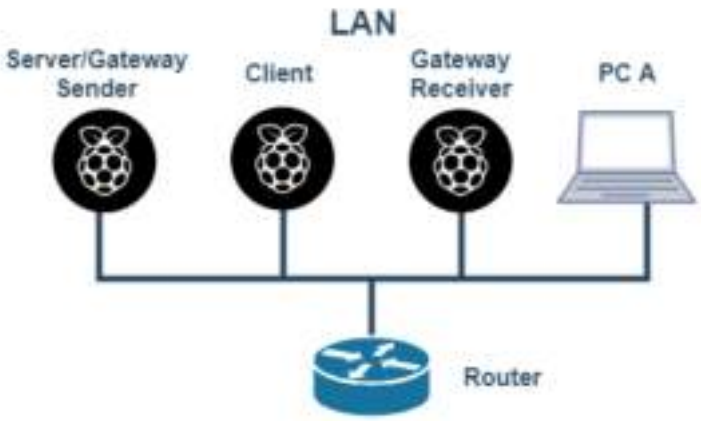



**Figure 22 - Different Entities in the same LAN**

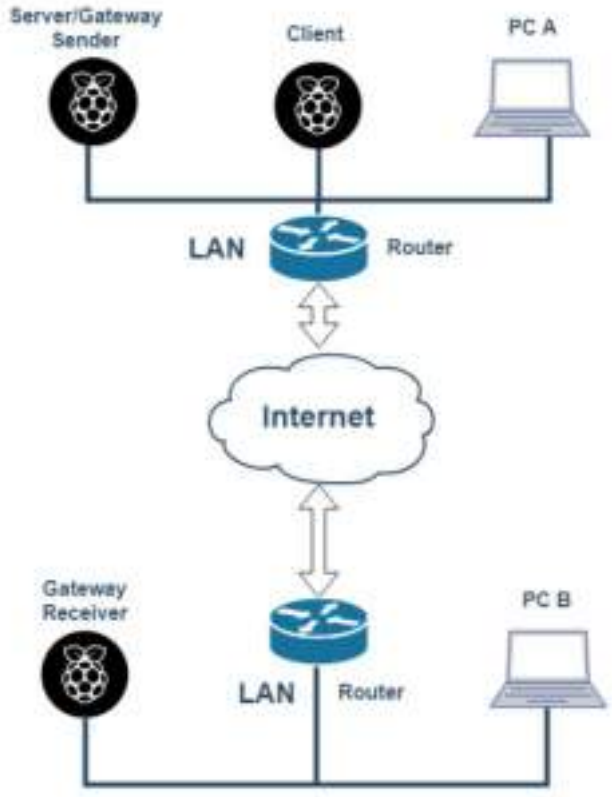



**Figure 23 - Topology using the IP approach**

The second scenario considers the intercommunication of devices existing in two distinct LANs, interconnected via a WAN which can be accessed via 4G, ADSL or Optical Fiber routers, as depicted Figure 23. Three distinct Portuguese ISPs were used, namely MEO, Vodafone and NOWO. This scenario considers a direct IP link between the Server/Gateway Sender and Gateway Receiver. In order to have the correct flow of the messages, it is required that the messages leave their LANs, being routed to the destiny public IP and being forwarded by the router using NAT to the device that is listening and waiting for the message, more concretely the Gateway Receiver. The first column refers to the study case and the second one refers to the ISP and technology in the Server/Gateway Sender. In the third column, the ISP and technology to the Client or Gateway Receiver is displayed.

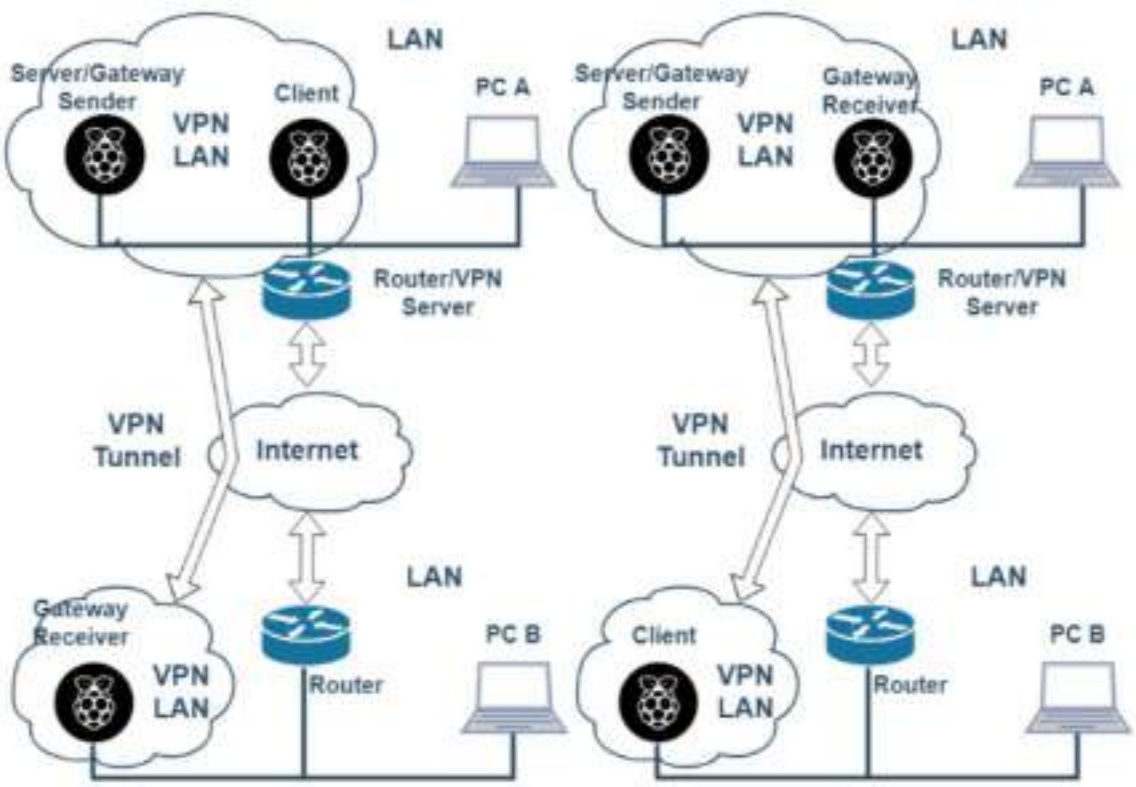



**Figure 24 - VPN Approach using UDP (left) and GOOSE (right)**

Finally, the third scenario illustrates the data transfer using the tunneling approach, as shown in Figure 24. Resorting to a VPN Server, installed on the Linksys routers, a VLAN is created allowing the messages to be sent over a Layer 2 protocol like GOOSE. The VPN Server and Server/Gateway Sender are placed in the same LAN, allowing messages to travel only once through the Internet, which would not happen if the VPN Server would be placed in an independent LAN. Since we want to compare both approaches, it would not make sense to force the messages to pass twice through the Internet and increase transmission delay.

## 16.2 Architecture definition for railway signalling systems

Considering the scope of the addressable system, the architecture definition for railway signalling systems consists of a direct instantiation deployment of the system depicted in Figure 19. Concretely, the “Industrial Corporation” would be a “Railway Corporation”, the VNF’s would compose virtualized network functions that intervene in critical data from machine-to-machine communications (e.g., a network firewall), and the Cloud Service Provider would be a 5G-enabled network telecommunications operator. In order for the critical communications benefit from lower latency, it is important that the VNF’s have the ability to be instantiated in a virtualised infrastructure closer to the “Railway Corporation”. In this way, the “Fog Node” can correspond to a virtualized infrastructure instantiation that can either belong to the 5G-enabled network telecommunications operator, or to the “Railway Corporation” itself.

This work will focus on the capability of instantiating critical VNF's in the fog node close to the "Rrailway Corporation", as verified in Figure 25.

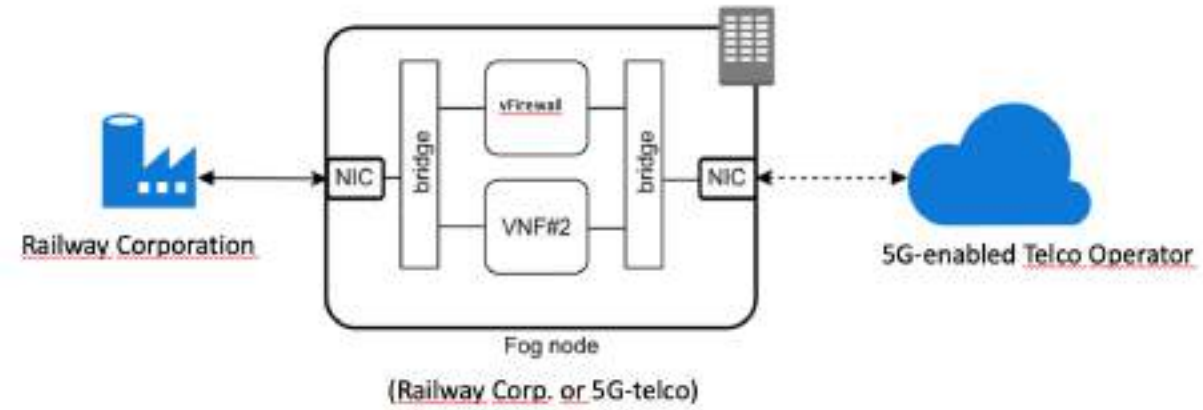



**Figure 25 - Virtualized Network Function Instantiation for Critical Communications Architecture in Railway Signalling Scenarios**

# 17 Conclusions

## 17.1 Main Conclusions

This version describes all the achieved results in the scope of the Technical Specification Activity, which includes the task T3.2.1 to T3.1.14. This activity was postponed to 30/06/2019, mainly to consolidate and finish some complex task that have been concluded at 30/06/2019. Therefore, this version of the report, consider that all tasks of the activity are concluded (30/06/2109). As previously described, this activity, was very important for the success of the further activities and this key activity was reported in this Deliverable. It is important to mention that, during the execution of the next activities, mainly regarding research and development activity, new progress may lead to minor revisions to the Technical specification, meaning that new versions of this reported will be performed.

# References


[1] O. Khaled, A. Marín, F. Almenares, P. Arias e D. Díaz, “Analysis of secure TCP/IP profile in 61850 based substation automation system for smart grids,” *International Journal of Distributed Sensor Networks,* p. 5793183, 2016.

[2] P. Jafary, O. Raipala, S. Repo, M. Salmenperä, J. Seppälä, H. Koivisto, S. Horsmanheimo, H. Kokkoniemi-Tarkkanen, L. Tuomimäki, A. Alvarez, F. Ramos, A. Dede e D. D. Giustina, “Secure layer 2 tunneling over IP for GOOSE-based logic selectivity,” em *2017 IEEE International Conference on Industrial Technology (ICIT)*, Toronto, ON, Canada , 2017.

[3] M. Kanabar, A. Cioraca e A. Johnson, “Wide Area Protection \& Control using High-Speed and Secured Routable GOOSE Mechanism,” em *2016 69th Annual Conference for Protective Relay Engineers (CPRE)*, College Station, TX, USA , 2016.

[4] M. Heinrich, J. Vieten, T. Arul e S. Katzenbeisser, “Security Analysis of the RaSTA Safety Protocol,” em *2018 IEEE International Conference on Intelligence and Security Informatics (ISI)*, Miami, FL, USA , 2018.

[5] G. Samta, S. Karmakar, M. Sharma e S. Sharma, “Bluetooth Secure Simple Pairing with enhanced security level,” *Journal of Information Security and Applications,* vol. 44, pp. 170-183, 2019.

[6] A. Oak e R. Daruwala, “Assessment of Message Queue Telemetry and Transport (MQTT) protocol with Symmetric Encryption,” em *2018 First International Conference on Secure Cyber Computing and Communication (ICSCCC)*, Jalandhar, India, 2018.

[7] Z. A. Alizai, N. F. Tareen e I. Jadoon, “Improved IoT Device Authentication Scheme Using Device Capability and Digital Signatures,” em *2018 International Conference on Applied and Engineering Mathematics (ICAEM)*, Taxila, Pakistan, 2018.

[8] B. A. Alohali, V. G. Vassilakis, I. D. Moscholios e M. D. Logothetis, “A Secure Scheme for Group Communication of Wireless IoT Devices,” em *2018 11th International Symposium on Communication Systems, Networks & Digital Signal Processing (CSNDSP)*, Budapest, Hungary, 2018.

[9] C. H. Lee e K.-H. Kim, “Implementation of IoT system using block chain with authentication and data protection,” em *2018 International Conference on Information Networking (ICOIN)*, Chiang Mai, Thailand, 2018.

[10] R. S. Satpute e A. N. Thakare, “Secret Sharing Schemes: A Review,” em *International Conference on Industrial Automation And Computing (ICIAC)*, 2014.

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

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

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

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

[15] 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].

[16] 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].

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

[18] 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].

[19] 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].

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

[21] 3GPP, “3GPP TS23.501, "System Architecture for the 5G System",” [Online]. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3144.

[22] “Deliverable 2.1 - Use cases and requirements for solutions targeting 5G network core,” 2018. [Online]. Available: https://wikis.ptinovacao.pt/download/attachments/44648131/Deliverable_21_final.pdf?api=v2.

[23] “3GPP 5G System Architecture,” [Online]. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3144.

# 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 |
| **FCTUC** | Jorge Granjal, João Vilela, Munkenyi Mukhandi |
| **IT** | Daniel Corujo, João Barraca Filipe, Asad Rehman |
| | |
| | |

# Versions history

| Version | Date | Description |
|---|---|---|
| **1.0** | 28-06-2019 | First version including all partners' contributions. |
| **2.0** | 06-12-2019 | Revised version |
| | | |
| | | |