

Deliverable 2.1

Vertical Sector Requirements Analysis and Use Case Definition

Editor:	Ana Cristina Aleixo, Efacec
Deliverable nature:	Report (R)
Dissemination level: (Confidentiality)	Public (PU)
Contractual delivery date:	31-10-2017
Actual delivery date:	20-11-2017
Suggested readers:	Telecommunication Operators, Service Providers, Power System Operators
Version:	1.0
Total number of pages:	179
Keywords:	5G Communications, Vertical Sector Requirements, Use Cases, Smart Grid, eHealth, Smart City

Abstract

This deliverable documents the definitions of use cases and the analysis of their requirements in the SLICENET project. The report presents three vertical sector use cases, each with their specific set of communication requirements. The use cases covered by this report are: Smart Grid Self-Healing, eHealth Smart/Connected Ambulance, and Smart City. Following a market analysis, the vertical sector high-level business requirements for 5G communications are further detailed and will be translated into technical specifications, which will in turn provide fundamental inputs for the SLICENET system architecture definition. The relation to 5G requirements and visions is also depicted for each use case, as well as the relation to the 5G-PPP KPIs and the expected business impact in the sector.

Disclaimer

This document contains material, which is the copyright of certain SLICENET consortium parties, and may not be reproduced or copied without permission.

All SLICENET consortium parties have agreed to full publication of this document.

The commercial use of any information contained in this document may require a license from the proprietor of that information.

Neither the SLICENET consortium as a whole, nor a certain part of the SLICENET consortium, warrant that the information contained in this document is capable of use, nor that use of the information is free from risk, accepting no liability for loss or damage suffered by any person using this information.

The EC flag in this document is owned by the European Commission and the 5G PPP logo is owned by the 5G PPP initiative. The use of the flag and the 5G PPP logo reflects that SLICENET receives funding from the European Commission, integrated in its 5G PPP initiative. Apart from this, the European Commission or the 5G PPP initiative have no responsibility for the content.

The research leading to these results has received funding from the European Union Horizon 2020 Programme under grant agreement number H2020-ICT-2014-2/671672.

Impressum

Full project title: End-to-End Cognitive Network Slicing and Slice Management Framework in Virtualised Multi-Domain, Multi-Tenant 5G Networks

Short project title: SLICENET

Work-package 2: SLICENET System Definition

Task 2.1: Vertical Sector Requirements Analysis and Use Case Definition

Document title: Vertical Sector Requirements Analysis and Use Case Definition

Editor: Ana Cristina Aleixo, EFACEC Energia

Work-package leader: Marius Iordache, Orange Romania

[Estimation of PM spent on the Deliverable]

Copyright notice

© 2017 Participants in SLICENET project

Executive summary

The SLICENET project expects to support a range of use cases of diverging requirements for vertical businesses by maximizing the potential of 5G infrastructures through end-to-end network slicing and slice management based on advanced software networking and cognitive network management.

This deliverable provides the analysis of the diverse requirements from the vertical sectors and the definition of the selected use cases, led by the vertical sector partners in the project. Specifically, the following achievements are reported in this deliverable:

- Three representative use cases including Smart Grid Self-Healing, eHealth Smart/Connected Ambulance and Smart City are defined with specific scenarios presented in detailed operation steps;
- For each use case, the implementation and evaluation considerations are described, and their potential technical, business and societal impacts are envisioned;
- For each use case, the functional, operational and interface requirements are assessed and specified based on a set of requirements analysis performed jointly by the vertical sector partners and the technical task leaders following a “verticals in the loop” co-design approach;
- A survey of 5G stakeholders is also performed as an additional source and methodology to inform the formulation of the use case definitions and requirements analysis.

The technical specifications of the reported use cases and requirements analysis supporting the vertical services will impact directly in the subsequent definition of the overall SLICENET system’s architecture.

List of authors

Company	Author	Contribution
EFACEC	Ana Cristina Aleixo	Smart Grid Use Case; Introduction; Conclusion;
EFACEC	Eduardo Rodrigues	Smart Grid Use Case; Introduction; Conclusion;
EFACEC	Alberto Rodrigues	Smart Grid Use Case; Introduction; Conclusion;
EFACEC	Rogério Dias Paulo	Smart Grid Use Case; Introduction; Conclusion;
EFACEC	Rui Dias Jorge	Smart Grid Use Case; Introduction; Conclusion;
EFACEC	Nuno Rodrigues	Smart Grid Use Case; Introduction; Conclusion;
EFACEC	Luis Martins	Smart Grid Use Case; Introduction; Conclusion;
EFACEC	Sara Costa	Smart Grid Use Case; Introduction; Conclusion;
EFACEC	Ricardo Santos	Smart Grid Use Case; Introduction; Conclusion;
EFACEC	João Peres	Smart Grid Use Case; Introduction; Conclusion;
CIT INFINITE	Paul Walsh	eHealth Use Case;
ORANGE ROMANIA	Marius Iordache	Smart City Use Case;
ORANGE ROMANIA	Madalina Oproiu	Smart City Use Case;
ORANGE ROMANIA	Horia Stefanescu	Smart City Use Case;
ORANGE ROMANIA	Cristian Patachia	Smart City Use Case;
ORANGE ROMANIA	Costea Catalin	Smart City Use Case;
ALTICE LABS	Pedro Miguel Neves	Introduction; Technical Requirements;

ALTICE LABS	Rui Calé	Introduction; Technical Requirements;
HELLENIC TELECOMUNICATIONS ORGANISATION S.A	George Agapiou	5G Communication Requirements; Technical Requirements;
HELLENIC TELECOMUNICATIONS ORGANISATION S.A	Stamatis Perdikouris	5G Communication Requirements; Technical Requirements;
DELL EMC	Zdravko Bozakov	5G Communication Requirements; Technical Requirements;
NEXTWORKS S.R.L.	Giacomo Bernini	Technical Requirements;
NEXTWORKS S.R.L.	Pietro G. Giardina	Technical Requirements;
UNIVERSITAT POLITÈCNICA DE CATALUNYA	Albert Pagès	Technical Requirements;
UNIVERSITAT POLITÈCNICA DE CATALUNYA	Fernando Agraz	Technical Requirements;
UNIVERSITAT POLITÈCNICA DE CATALUNYA	Salvatore Spadaro	Technical Requirements;
CREATIVE SYSTEMS ENGINEERING (CSE) LTD.	Konstantinos Koutsopoulos	Technical Requirements;
ERICSSON TELECOMUNICAZIONI SPA	Ciriaco Angelo	Technical Requirements;
ERICSSON TELECOMUNICAZIONI SPA	Raffaele De Santis	Technical Requirements;
ERICSSON TELECOMUNICAZIONI SPA	Carmine Galotto	Technical Requirements;
EURECOM	Navid Nikaein	Technical Requirements;
UNIVERSITY OF THE WEST OF SCOTLAND	Qi Wang	Technical Requirements;
UNIVERSITY OF THE WEST OF SCOTLAND	Jose Alcaraz-Calero	Technical Requirements;

Table of Contents

Executive summary	3
List of authors.....	4
Table of Contents	6
List of figures	9
List of tables	10
Abbreviations	11
Definitions	15
1 Introduction.....	16
1.1 Objectives	16
1.2 Approach and Methodology.....	17
1.3 Document Structure	17
2 5G Communication Requirements.....	19
2.1 5G Requirements and Vision	19
2.2 5G Security Challenges	20
2.3 Expected SLICENET Impact on 5G.....	22
3 Vertical Sector Use Cases	23
3.1 Smart Grid Self-Healing Use Case Overview	23
3.2 eHealth Smart/ Connected Ambulance Use Case Overview.....	26
3.2.1 5G Market.....	29
3.2.2 5G for Health	29
3.3 Smart City Use Case Overview.....	31
4 Smart Grid Self-Healing Use Case	35
4.1 General Background	36
4.2 Relation to 5G Requirements and Visions.....	36
4.3 Goals	37
4.4 General Assumptions.....	37
4.5 Actors.....	39
4.6 Use Case Scenario 1: Protection Coordination.....	39
4.6.1 Overview	39
4.6.2 Detailed Steps.....	40
4.6.3 Performance Requirements	44
4.7 Use Case Scenario 2: Automatic Reconfiguration	44

4.7.1	Overview	44
4.7.2	Detailed Steps.....	45
4.7.3	Performance Requirements	49
4.8	Use Case Scenario 3: Differential Protection	50
4.8.1	Overview	50
4.8.2	Detailed Steps.....	51
4.8.3	Performance Requirements	54
4.9	Technical Requirements	55
4.9.1	Requirements on Cognition (Intelligence)	55
4.9.2	Requirements on the One-Stop API	55
4.9.3	Requirements on Slicing/Slice	56
4.9.4	Requirements on Multi-domain Operations.....	56
4.9.5	Requirements on RAN	57
4.9.6	Requirements on MEC	57
4.9.7	Requirements on Core	58
4.9.8	Requirements on Enterprise Network	58
4.9.9	Non-functional Requirements.....	58
4.9.10	Coverage of Service Life-cycle Phases.....	59
4.10	Implementation, Evaluation and Impact.....	59
4.10.1	Prototyping/Testbed	59
4.10.2	Benchmarking and Validation	60
4.10.3	Relevant Standards	60
4.10.4	Relation to 5G-PPP KPIs.....	61
4.10.5	Technical Innovation in the Field	61
4.10.6	Business Impact in the Sector	62
4.10.7	End User Benefits	62
5	eHealth Smart/ Connected Ambulance Use Case	63
5.1	General Background	63
5.2	Use Case Scenario: Ultra-High Definition Video and IoT for Connected Ambulance	65
5.2.1	Overview	65
5.2.2	Detailed Steps.....	71
5.2.3	Technical Requirements.....	74
5.2.4	Implementation, Evaluation and Impact	78
6	Smart City Use Case.....	81

- 6.1 General Background 81
- 6.2 Use Case Scenario: Smart Lighting (SmaLi-5G)..... 81
 - 6.2.1 Overview81
 - 6.2.2 Detailed Steps.....91
 - 6.2.3 Technical Requirements93
 - 6.2.4 Implementation, Evaluation and Impact97
- 7 Conclusions..... 99
- References..... 100
- Annex A Use Cases Requirements Tables 103
 - A.1 RAN 103
 - A.2 Control Plane 105
 - A.3 Data Plane..... 111
 - A.4 Enterprise 119
 - A.5 FCA 132
 - A.6 MEC..... 137
 - A.7 One Stop API 142
 - A.8 Security 152
 - A.9 Plug and Play..... 155
- Annex B 5G Technologies Business Requirements and Expectations Survey..... 160
 - B.1 Smart Grid Survey..... 160
 - B.1.1 Survey Template.....160
 - B.2 eHealth Survey..... 166
 - B.2.1 Survey Template.....166
 - B.2.2 Survey Analysis169
 - B.3 Smart City Survey..... 171
 - B.3.1 Survey Template.....171
 - B.3.2 Survey Analysis174

List of figures

Figure 1 Electric power grid architecture	23
Figure 2 Self-healing solution stratification	25
Figure 3 eHealth 5G key capabilities (Elayoubi, 2016)	27
Figure 4 In the context of 5G potential offerings please rate the importance of the following, considering: Strongly Disagree (1) Disagree (2) Neutral (3) Agree (4) Strongly Agree (5)	30
Figure 5 When thinking of your current and future business, which is the key enabler for migrating towards 5G solutions?	31
Figure 6 Please rate the relevance of the 5G technology for your next generation communication services approach	31
Figure 7 SmaLi-5G High Level Architecture	33
Figure 8 5G communications for smart grid self-healing applications.....	35
Figure 9 Importance of 5G high-level requirements for the use case scenarios.....	36
Figure 10 IEC 61850 GOOSE retransmission diagram [8].....	38
Figure 11 Protection coordination scenario activity flow.....	42
Figure 12 Automatic reconfiguration scenario activity flow.....	48
Figure 13 Synchrophasor measurement representation [19].....	51
Figure 14 Differential protection scenario activity flow.....	53
Figure 15 Smart Grid communication architecture, figuring the enterprise network.....	58
Figure 16 Example of a maximum topology.....	59
Figure 17 Scenarios likely to benefit from 5G SLICENET technology	64
Figure 18 High-level model of SLICENET roles	65
Figure 19 SLICENET overview of use case scenario	65
Figure 20 RedZinc BluEye system	67
Figure 21 This is a suggested initial slice to be built by RedZinc/CIT/DELL EMC	69
Figure 22 Stroke facial symptoms	72
Figure 23 UHD Video flow in SLICENET	73
Figure 24 End to end Provisioning.....	73
Figure 25 Relation to hospital enterprise network.....	76
Figure 26 Smart Lighting LoRaWAN based architecture.....	83
Figure 27 Smart Lighting LTE-M based architecture.....	83
Figure 28 Smart Lighting 5G based architecture.....	83
Figure 29 SmaLi-5G required network transformation	84
Figure 30 SmaLi-5G End-to-End slicing concept.....	84
Figure 31 Summarized LoRaWAN Classes and frames transmission	88
Figure 32 General LoRaWAN Architecture [30].....	88
Figure 33 LoRaWAN general summary capabilities.....	89
Figure 34 Migration Steps to Next Generation 5G Radio.....	90
Figure 35 SmaLi-5G Provisioning flow.....	92
Figure 36 Integration in SLICENET architecture	93
Figure 37 General services communication architecture	94
Figure 38 Telco end-to-end slicing concepts	95
Figure 39 SmaLi-5G Inter-domain slicing concepts	96
Figure 40 Key features and relevance for responders (% of responders selected the key features)	177
Figure 41 5G Key enabler - business model & cost efficiency statistics.....	177
Figure 42 5G Key enabler – enhanced business model & time to market.....	178
Figure 43 5G market trend relevance.....	178
Figure 44 New technology investments estimation	179

List of tables

<i>Table 1 Mapping of SLICENET use cases to the 5G requirements</i>	20
<i>Table 2 Comparative analysis of self-healing schemes</i>	25
<i>Table 3 eHealth Connected Ambulance KPIs for the eHealth Use Case</i>	29
<i>Table 4 User Experience KPI's and system performance requirements for all Smart City use case</i>	32
<i>Table 5 Performance requirements for peer-to-peer communications</i>	44
<i>Table 6 Performance requirements for peer-to-peer communications</i>	49
<i>Table 7 Requirements for IEC 61850 SV communications (for synchrophasor measurements)</i>	54
<i>Table 8 Requirements for IEC 61850 GOOSE peer-to-peer communications (for event-driven communication)</i> .	54
<i>Table 9 Performance requirements for communications with control centre/SCADA</i>	56
<i>Table 10 Uptime/ availability requirements for all communications</i>	57
<i>Table 11 Recovery delay requirements, per application</i>	57
<i>Table 12 Lamp technical specifications</i>	86
<i>Table 13 5G Survey Questionnaire and relevance</i>	174
<i>Table 14 Group of responders</i>	175
<i>Table 15 Questionnaire centralized responses</i>	176

Abbreviations

5G	Fifth Generation (mobile/cellular networks)
5G PPP	5G Infrastructure Public Private Partnership
AAA	Authentication, Authorization and Accounting
ADR	Adaptive Data Rate
API	Application Programming Interface
ASN.1	Abstract Syntax Notation One
BER	Bit Error Rate/ ASN.1 Basic Encoding Rules
BEREC	Body of European Regulators for Electronic Communications
CB	Circuit Breaker
CLI	Command-Line Interface
CSP	Communication Service Provider
CT	Computed Tomography
DA	Distribution Automation
DL	Download
DMS	Distribution Management System
DR	Data Rate
DSC	Digital Service Consumer
DSO	Distribution System Operator
DSP	Digital Service Provider
E2E	End-to-End
ECG	Electrocardiography
eMBB	enhanced Mobile Broadband
ETSI	European Telecommunications Standards Institute
EU	European Union
FCAPS	Fault, Configuration, Accounting, Performance and Security

FDIR	Fault Detection, Isolation and Restoration
FOV	Field-of-View
GDPR	General Data Protection Regulation
GOOSE	Generic Object Oriented Substation Events (IEC 61850)
HD	High Definition
HV	High Voltage
ICT	Information and Communications Technologies
IED	Intelligent Electronic Device
IoT	Internet of Things
IP	Internet Protocol
IR	Infrared
ITU-T	International Telecommunication Union Telecommunication Standardization Sector
KPI	Key Performance Indicator
LAN	Local Area Network
LED	Light-Emitting Diode
LI	Lawful Intercept
LoRaWAN	Low Power Wide Area Networking
LPWA	Low-Power Wide-Area
LTE	Long Term Evolution
LTE-M	Long Term Evolution for Machines
LV	Low Voltage
M2M	Machine-to-Machine
MAC	Media Access Control
MBB	Mobile Broadband
M2M	Machine to Machine

MEC	Mobile Edge Computing
MMS	Manufacturing Message Specification (IEC 61850)
mMTC	massive Machine-Type Communication
MTC	Machine-Type Communication
MV	Medium Voltage
MVNO	Mobile Virtual Network Operator
NB-IoT	Narrow Band Internet of Things
NFV	Network Function Virtualization
NIH	National Institutes of Health
NIHSS	NIH Stroke Scale
OMS	Outage Management System
OPEX	Operational Expenditure
OT	Operational Technology
PAC	Protection, Automation and Control
PC	Personal Computer
QoE	Quality of Experience
QoS	Quality of Service
QVGA	Quarter Video Graphics Array
R&D	Research and Development
RAN	Radio Access Network
RGB	Red, Green, Blue
RTU	Remote Terminal Unit
SCADA	Supervisory Control And Data Acquisition
SDN	Software Defined Networks
SIM	Subscriber Identification Module
SG	Smart Grid

SLA	Service Level Agreement
SLICENET	End-to-End Cognitive Network Slicing and Slice Management Framework in Virtualised Multi-Domain, Multi-Tenant 5G Networks
SSC	Smart Substation Controller
SV	Sampled Values (IEC 61850)
TCP	Transmission Control Protocol
THD	Total Harmonic Distortion
TRL	Technology Readiness Level
UDP	User Datagram Protocol
U-HDTV	Ultra-High Definition Television
UHD	Ultra-High Definition
UHDV	Ultra-High Definition Video
UHV	Ultra-High Voltage
UL	Upload
uMTC	ultra-reliable Machine-Type Communication
uRLLC	ultra Reliable Low Latency Communication
UTC	Coordinated Universal Time
VNF	Virtualized Network Function
WAN	Wide Area Network
WHO	World Health Organisation
WP	Work Package
xMBB	extreme Mobile Broadband

Definitions

This section presents the definitions of the most relevant terms used along the document, leading to a better understanding of the project's specific terminology.

- **Power system:** network of electrical components used to supply, transfer, store and use electrical power.
- **Substation:** part of the power system in which the voltage level is transformed.
- **Distribution Automation:** set of technologies capable of remotely operate in real-time to control the power grid, i.e., monitoring – voltages and currents – and commanding remote units, such as switches and transformers.
- **Intelligent Electronic Devices:** any device incorporating one or more processors with the capability of receiving or sending data/control from or to an external source (for example, electronic multifunction meters, digital relays, controllers).
- **Smart Grid:** advanced system, relying on the use of ICTs to manage power grids and their assets in an integrated and coordinated manner, improving electricity supply efficiency and reliability.
- **Synchrophasor:** Time-synchronized measurement of electrical quantities.

1 Introduction

As enablers of the digitalisation of the European economy, fuelled by the power of mobile, cloud and broadband technologies, 5G infrastructures are gaining relevance, with several R&D initiatives being promoted recently under this topic. In particular, network slicing has emerged as a promising technology to address cost-efficiency and flexibility requirements, imposed by custom services of 5G based software-networking, among new use cases taking place in almost every enterprise and industry.

Under this context, the SLICENET project aims to design, prototype and demonstrate an innovative verticals-oriented 5G network slicing framework, focused on cognitive network management and control for end-to-end slicing operation services. The envisioned 5G network slicing solution will enable customisable control, cross-plane coordination and orchestration, slicing scalability, security, resource efficiency and interoperability across multiple domains.

This report establishes the vertical sector requirements analysis and the use cases definition, which will be prototyped, integrated and demonstrated in WPs 7 and 8. Furthermore, an updated market analysis over telecommunication markets for vertical services will be implemented. The partners polarizing the vertical use cases will be queried on this specific subject.

The requirements related to network and APIs support for the vertical services will be identified, including the business and technical requirements – functional, operational and interface conditions – imposed by each use case. These requirements will target the technical specifications of each of the vertical sectors and the respective KPIs addressed.

Additionally, security risk management and scalability considerations will also be addressed.

This report is a live document that will evolve throughout the several stages of the project.

1.1 Objectives

1. Describe the business Use Cases from the point of view of the verticals

Well described business Use Cases will help keep an end to end view throughout the project, focusing the architecture, avoiding scope drift, and providing an effective way to demonstrate and evaluate project results.

2. Identify what the verticals expect from 5G

The days of inflexible service offers from CSPs may soon be over, and what follows will be determined by their customers, not only in terms of sheer communications capabilities (bandwidth, delay, jitter, etc) but also with the need to control and manage the service.

3. Identify needs that challenge the traditional communications services models

Use the 5G approach promises together with the particular needs of verticals to foster the discussion about new services that suit customers' needs and differentiate SP offers.

4. Describe the verticals' preferences for an interaction model with service providers

The gap between the expectations of verticals and those of Service Providers.

1.2 Approach and Methodology

This document aims at identifying and describing the Use Cases that highlight specific needs that the verticals involved in the project consortium expect to be met by 5G in general, and by network slicing in particular. These needs will be converted to requirements that will help determine how the SLICENET framework will be designed.

The Use Cases hereby described will be analyzed in the scope of Task 2.2 (Architecture) and will be discussed to manage perfect alignment between the verticals' and the Service Providers expectations, to guarantee that the architecture fulfills the needs of these scenarios and that the Use Cases demonstrate the virtues of the Architecture.

Once this alignment exists, a set of "Technical Use Cases" will be defined as an instrument for the detailed design of the framework architecture (under the scope of T2.2).

The Use Cases that are hereby described, along with changes that may arise from architecture discussion, will be implemented using the resulting framework, under the conditions set up by each Use Case promoters, and that implementation will be used for validation and demonstration of the project results.

1.3 Document Structure

The structure of the document is as follows:

- In Section 1, the objectives, the approach and methodology followed, and the document structure will be presented. Includes:
 - Introduction – introduction to document's topics and context on the project's rollout plan;
 - Objectives – description of the specific objectives of the document within the project WPs structure;
 - Approach and Methodology – presentation of the approach and the methodology adopted to proceed to the vertical sector requirements analysis and use cases definition;
 - Document Structure – presentation of the document general organization.
- Section 2 addresses the 5G requirements and vision, the 5G security challenges, and the expected SLICENET impact on 5G. Includes:
 - 5G Requirements and Visions identification;
 - 5G Security Challenges – identification of the security challenges related to 5G communications;
 - Expected SLICENET impact on 5G – presentation of the expected impacts of project results on 5G.
- Section 3 focuses on the overview of the Smart Grid Self-Healing use case, the eHealth Smart / Connected Ambulance use case, and the Smart City use case. Includes:
 - Smart Grid Self-Healing Use Case Overview – general overview on the Smart Grid Self-Healing use case features;
 - eHealth Smart / Connected Ambulance Use Case Overview – general overview on the eHealth Smart / Connected Ambulance use case features;
 - Smart City Use Case Overview – general overview on the Smart City use case features.
- In Sections 4, 5 and 6, those use cases will be described in detail.

- The last Section – 7 – summarizes the conclusions of the report.

2 5G Communication Requirements

2.1 5G Requirements and Vision

As technology evolves, new services are offered and more sophisticated networks are needed. The increasing number of Internet users leads to a redesign of network architecture, forcing designers to take into account new parameters such as the need of global coverage combined with low latency, as well as a high reliability and security level. Additionally, new networking experiences are added, such as Internet-of-Things (IoT), which promise to offer new services and facilities to people's daily lives by creating "smart" homes and even "smart" cities. In this demanding environment, 5G technology is emerging, playing a decisive role in the implementation of new visions and promising to deliver solutions.

A major innovation introduced by 5G technology is the scalability. 5G architectures take into account the possible need of extending the capabilities of the network, both at the level of user traffic growth and at the level of new services input from providers. Slicing could be the ideal solution for such networks, offering scalability as well as flexibility in managing a giant network.

Additionally, there is a steady upward trend of wireless connectivity, which is projected to be continued in the future with exponentially increasing rate. This phenomenon poses a challenge for network designers: the integration of wireless and fixed services so that users can enjoy the same services regardless of how they are interconnected. 5G vision is to deal with this challenge by focusing in virtualized elements, which could be shared between wireless and fixed networks. The virtualization could also play an important role in scalability too, as it offers ease in expanding network capabilities without redesigning the hardware elements.

Finally, the advantages of scalability and unification would unlock the ability to add new services that will create new experiences for users. For instance, users would be able to enjoy broadband services on the go. 5G will ensure the uninterrupted interconnection of a user when, for example, he is steaming during his trip to work. This ability of uninterrupted interconnection could also be very important in services such as self-driving public transport vehicles or in the crucial case of remote healthcare provision.

At the design level of a 5G architecture, there are several parameters which the designer should take into account:

- **Low latency**
An important characteristic of network operation is the low latency. There are services such as live streaming, Voice over IP or over WiFi, gaming etc, which demands low latency in order to operate effectively. Otherwise there is a danger of significantly long-time interruption and even unexpected termination of the services. The combination of the requirement for low delays with the predicted increase of data traffic, make the insurance of low latency necessary.
- **Availability**
5G ensures the uninterrupted interconnection, as it promises new services and new customer experiences. Thus, it is important to offer high availability to users. That also leads to a design of the network in such a way as to ensure maximum

geographical coverage so that the user could be connected to the network continuously as he moves from place to place.

- **High traffic needs**

As even more users would be interconnected with multiple devices, the rapid increase of data traffic is predicted. The network must be designed to counter this increase, because it could lead, if not tackled in time, in low latency or even interruption of a service.

- **Low cost**

The extended network that 5G brings, with many services and new equipment would increase the total operating cost of the network. It is important to keep that cost as low as possible.

- **Energy efficiency**

As it is known, the 5G technologies will have to implement a large number of small base stations on traditional topologies in order to sustain both data volumes and capacity demands. Therefore, energy consumption in such networks increases proportionally with the number increase of small cells. Thus, improving energy efficiency becomes an important target for the implementation of 5G networks.

- **Scalability**

The architecture of 5G should be flexible and scalable in order to adapt to the diverse needs of users and services

- **Flexibility**

The resources of the infrastructure including spectrum resources in different bands should be flexible and include licensed and unlicensed, paired and unpaired spectrum, and low and high frequency bands.

- **Coverage**

The coverage of the small base stations is expected to be improved at the cell edges in order for the networks to sustain high bit rates especially at the edges.

The mapping of the requirements to the SLICENET use cases is shown in Table 1.

Table 1 Mapping of SLICENET use cases to the 5G requirements

Requirements	Smart Grid	eHealth	Smart City
Low latency	x	x	
Availability	x	x	x
High traffic needs		x	
Low cost	x	x	x
Energy efficiency	x	x	x
Scalability	x		x
Flexibility	x	x	x
Coverage	x	x	

2.2 5G Security Challenges

The 5G architecture faces a number of security risks and challenges. In order to successfully fulfil its envisioned goals these issues must be resolved: both conceptually, by clearly defining the functionality and scope of security and privacy features of the architecture, and technically, by utilizing the most suitable solutions in the architecture design.

A key challenge is preventing unauthorized access of assets in an infrastructure hosted and operated by multiple parties and accessed by numerous users with different levels of access. Hence, a strong and consistent Authentication, Authorization and Accounting (AAA) mechanisms which are interoperable across all parties comprising the 5G infrastructure are needed.

Further, given the wide range of verticals that are poised to see deployment, a strong isolation of the individual slices is crucial. It is expected that 5G infrastructure slices offered by the telecom operators will replace and augment critical infrastructures (e.g., e-health, emergency services, smart grids) previously operated on dedicated resources. Thus, slices must provide a level of availability, performance, and security that is at least equal to the infrastructure that they are supplanting. Specifically, the architecture must guarantee that the slice control and data planes cannot be disrupted by external parties or co-hosted slice elements, and must detect and mitigate attacks which may expose slice data to unauthorized parties. The problem is aggravated by high degree of virtualization and automation that 5G infrastructures are expected to employ. A strong consistency between the various levels of abstraction used is therefore essential. To this end, the architecture requires effective mechanisms for monitoring and managing the infrastructure components - end-to-end - across multiple administrative domains.

In addition, the 5G architecture must provide solutions that resolve conflicting requirements with respect to privacy and manageability. Privacy is an essential prerequisite for many potential users of the architecture and an appropriate enforcement thereof will play a critical role for the acceptance of a sliced 5G architecture across a wide range of verticals. Hence, trust relationships between involved entities must be clearly expressed and potentially redefined to accommodate the heterogeneity and complexity of the architecture. What's more, privacy requirements are frequently at odds with mechanisms aiming to support monitoring of data in the shared infrastructure. Uses of monitoring range from analytics for traffic and resource optimization, attack and intrusion detection for threat mitigation as well as interfaces for lawful intercept (LI), e.g., as defined in the EU Data Retention Directive.

In addition to user and operator requirements, privacy and manageability aspects are further influenced by regulatory frameworks including, among others, the EU Directive on privacy and electronic communications, the General Data Protection Regulation (GDPR), BEREC Guidelines on the Implementation by National Regulators of European Net Neutrality Rules, Access Directive (2002/19/EC), etc.

As a primary strategy for addressing some of the challenges outlined above, SLICENET will focus on developing end-to-end (E2E) encryption approaches that provide a satisfactory level of in-slice privacy. Further, we will explore mechanisms necessary to enable granular and compliant access to data for the purposes of monitoring, analytics, logging, and LI. A number of associated encryption schemes, key management, and service assurance techniques must be implemented in a way which does not call into question the overall security and trust concepts of the architecture. Furthermore, in order to maintain an acceptable performance level, steps for minimizing the signalling overhead associated with establishing secure channels must be undertaken, and the efficiency of the encryption schemes must be considered.

Additional key challenges for enforcing E2E security, given the numerous virtualization and abstraction levels prevalent in the 5G architecture, are the placement and chaining of encryption functions, as well as the attestation of physical and virtual network elements. Furthermore, the instantiation of all security features must be synchronised with the orchestrator which provisions and enforces the allocation of the available infrastructure resources to ensure the isolation of the slices.

As a consequence of the above, the carried-out security efforts must be coordinated across multiple work packages.

2.3 Expected SLICENET Impact on 5G

SLICENET is a 5G-PPP Phase 2 project which targets in fully softwarisation of the network. For this purpose it adopts the network slicing, expecting a significant improvement in network performance, service quality, and overall reduction in operating cost through sharing the software elements.

In more details, SLICENET's scope is to ensure the network scalability by using software-based elements in the network. The ability to easily extend the network when it is necessary is very important because it affects two major factors: first, as an increase in traffic is observed, interventions can be implemented so that latency would be maintained in low levels and services operation would not be affected. Second, the high geographical coverage will be achieved since the network scalability would not present the difficulties of the legacy systems. By implementing the proposed SLICENET architecture, these two factors will ensure the availability of the network and contribute in maintaining low latency even when the data traffic is increasing.

Additionally, the introducing of software network architecture could help providers to include new services. This ability comes to make true the 5G vision of introducing new experiences to the users, such as IoT. Furthermore, the virtualization in combination with different technology unification (fixed and mobile access) would offer an amount of services which are not limited by the location of the users.

Finally, slicing is an excellent way to reduce network cost: firstly, it maximizes the sharing elements, leading to a more economical management of the available resources. Additionally, the management of the network will be more efficient, since SLICENET offers an integrated framework to manage infrastructures. This will facilitate interventions to deal with unexpected phenomena, ensuring the immediate restoration of the well-functioning of the network, while saving resources.

The impact of SLICENET will be better depicted when the use case scenarios will be implemented. Then the above benefits of the proposed architecture will be depicted in real, innovative applications.

3 Vertical Sector Use Cases

3.1 Smart Grid Self-Healing Use Case Overview

The Smart Grid use case aims to benefit from the ultra-high network reliability and ultra-low communication latency provided by the SLICENET framework to implement and demonstrate an advanced Self-Healing solution for electric power grids - Figure 1. This use case will exploit the 5G slicing framework developed within the project, highlighting its potential to leverage critical systems supported by 5G network infrastructures.

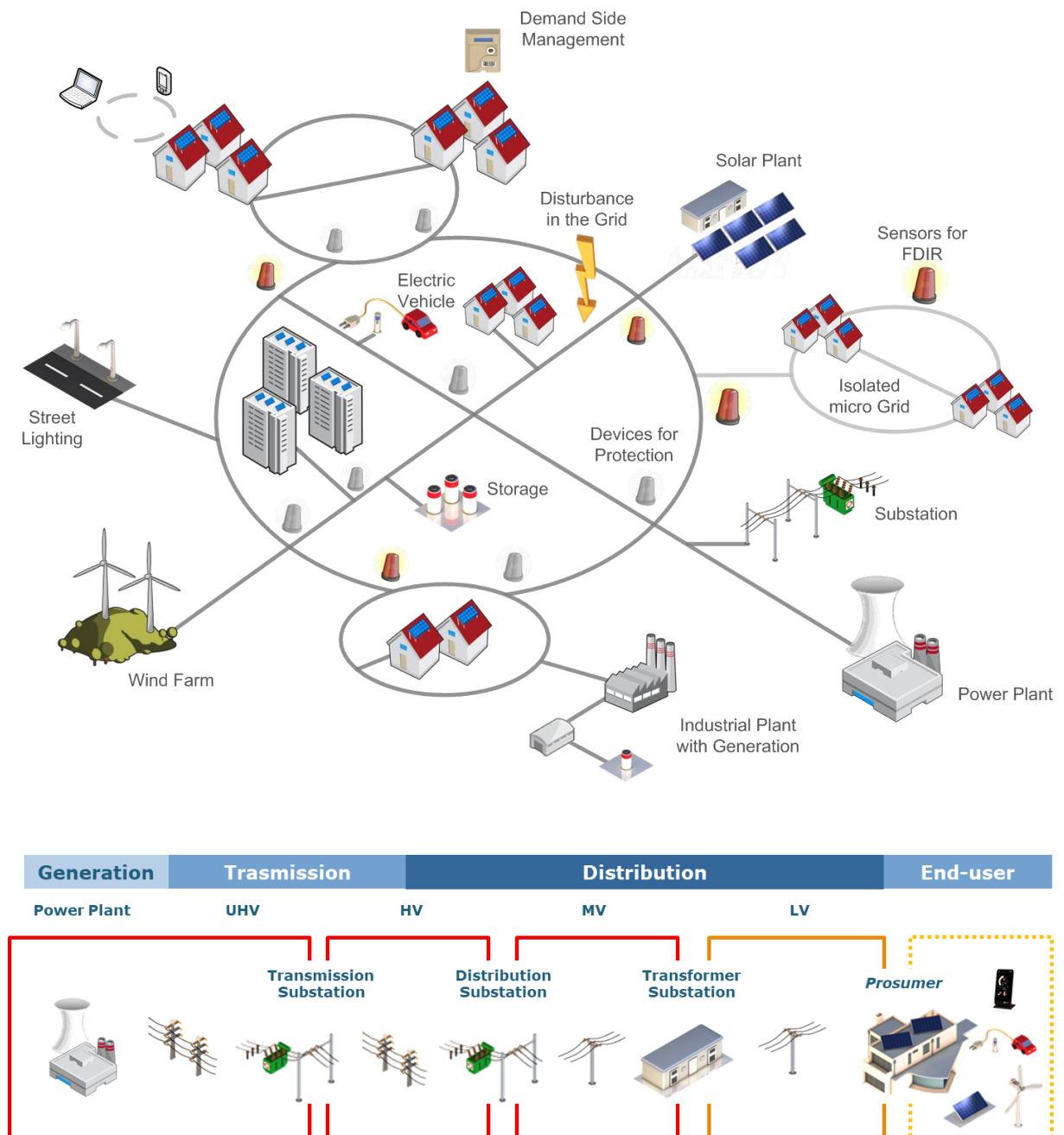


Figure 1 Electric power grid architecture

Within the Smart Grid use case, three major scenarios are envisioned to be exploited:

- Protection coordination – Scenario 1;
- Automatic reconfiguration – Scenario 2;
- Differential protection – Scenario 3.

Self-Healing in electric power grids, an overview:

Unplanned service interruptions represent a great concern to power system operators due to their significant impact in system's reliability, affecting technical quality of service and performance indicators related with the unavailability of supply to customers.

Regardless of the nature and magnitude of the damage caused by power failures, system operators are technically and economically responsible for it. As most of the interruptions are caused by faults in the electric power grid, an investment in Distribution Automation (DA) solutions must be foreseen in the reliability and planning studies, in order to ensure a continuous improvement of quality of service in electric energy supply. DA refers to a set of technologies capable of remote operation in real time, allowing advanced Self-Healing functionalities capable of immediately detect and isolate faults, and then proceed with an automatic reconfiguration and service restoration process.

Considering underlying goals of supplying the maximum load within a grid area affected by a fault, thus reducing the load restoration time to minimum, and under an increasingly prominent Smart Grid (SG) context, characterized by an increased use of Information and Communication Technologies (ICTs), an efficient Fault Detection, Isolation and Restoration (FDIR) functionality must provide fast automatic response to disturbances, detecting, locating and isolating faults based on real time metering and using suitably coordinated protection schemes.

Regarding the first two stages of the FDIR process, a fast and effective protection coordination is critical in order to ensure an efficient fault detection and isolation, as Intelligent Electronic Devices (IEDs) controlling the power switchgear devices deployed along the grid must communicate between them relying on high speed communications to ensure critical selectivity, *i.e.*, the closest device must clear the fault, ensuring a maximum load supply within the grid area affected by the fault, and reducing the service restoration time to minimum.

Differential protection provides an alternative protection scheme to the protection coordination. Despite providing greater accuracy and being able to deal with more complex grid topologies, the differential protection method is more demanding concerning the computational effort involved, as requires a wider metering range and the comparison of power system state estimation in different areas, imposing more severe communication requirements.

Self-Healing may be implemented based in different strategies concerning DA solutions for network remote operation in real time, through network high-speed communication empowering and hardware and software outfitting. Table 2 presents a comparison – considering the main features – between different approaches for Self-Healing implementation.

Table 2 Comparative analysis of self-healing schemes

Architecture	Centralized	Semi-Decentralized	Decentralized
Processing	Dispatch Centre DMS/OMS	SSC micro-DMS	IED peer-to-peer GOOSE
Hardware specificity	Any type of RTU	Any type of RTU	New generation IED capable of peer-to-peer communications
Scalability	High wide area scalability	Medium wide area scalability	Local wide area scalability
Time response	Slower response time	Average response time	Faster response time
Control specificity	Any type of remote control	Any type of remote control	Distributed intelligence

Apart from the implemented architecture Self-Healing solutions comprise a component layer, composed by the physical infrastructure, a bidirectional and integrated information layer, supporting high-speed communications, and an application layer, which includes different processes – monitoring, warning analysis, decision-making and control action - Figure 2.

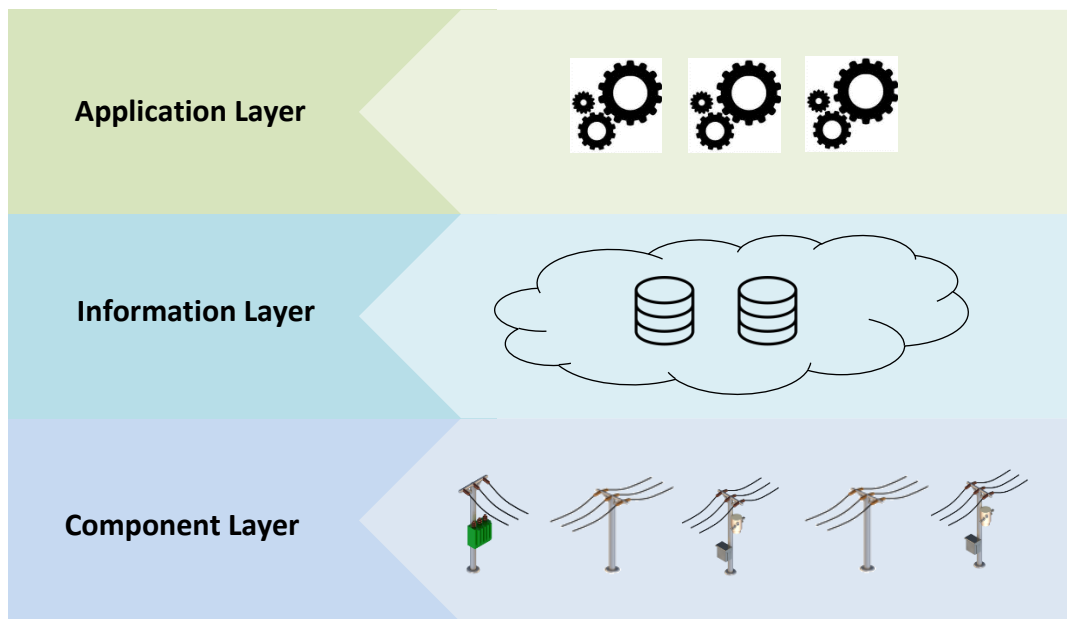


Figure 2 Self-healing solution stratification

Three different scenarios are defined for the use case, all three are based on a decentralized scheme leading to: a distributed application layer implementation; and a bidirectional access to the information layer in all the IEDs.

Scenario 1 – Protection Coordination:

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

Scenario 2 – Automatic Reconfiguration:

The Self-Healing scheme which will be exploited within the 2nd scenario proposed for the Smart Grid use case, related with the effective implementation of Self-Healing through

power grid's automatic reconfiguration, will follow a decentralized architecture, supported by IED peer-to-peer GOOSE communications.

Scenario 3 – Differential Protection:

For the implementation of the differential protection scenario, the capable IEDs must be supported by a high-speed communication infrastructure, allowing a real-time reaction to disturbances through an efficient fault detection and isolation procedure.

Next, in section 4, the Smart Grid use case is to be expose in detail. The main technical requirements will be defined, providing specific details to design and implement a proper framework to perform the use case and to showcase the capabilities and innovative characteristics of the SLICENET system.

3.2 eHealth Smart/ Connected Ambulance Use Case Overview

eHealth is defined by the World Health Organization (WHO) as the use of information and communication technologies (ICT) for health (WHO, 2017). It provides benefits in terms of better, decision making, enhanced diagnosis and more efficient, convenient and potentially more cost-effective delivery of care (IIA, 2017). Moreover, it reduces time to treatment and supports real-time treatment by first responders by wireless devices and video technology (IIA, 2017). With this in mind, SLICENET aims to provide such eHealth support to medical emergency first responders by developing a platform that can rapidly provision dedicated end-to-end broadband 5G slices that can support first responder eHealth scenarios to play an enabling role in the transformation of the delivery of healthcare through the design of better-connected, integrated and coordinated services. To that end we have engaged with stakeholders to develop a “Connected Ambulance” concept to advance the emergency ambulance services as they develop new collaborative models with their healthcare participants to help create improved experiences and outcomes for patients in their care. In scenarios such as a medical emergency response, an ambulance to hospital based eHealth system is a good example of how 5G technology can save lives as it enables remote diagnosis, provides on-scene care and reduces response time (Constandinos Mavromoustakis, 2016).

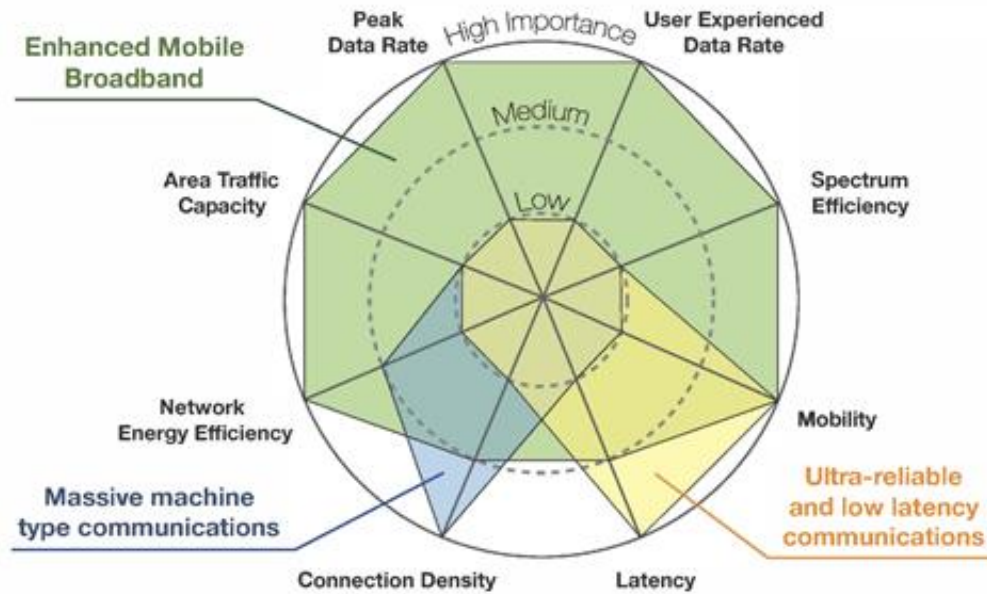


Figure 3 eHealth 5G key capabilities (Elayoubi, 2016)

In SLICENET the Connected Ambulance will act as a connection hub for the emergency medical equipment and wearables, enabling storing and real-time streaming of video data to the awaiting emergency department team at the destination hospital. It will use 5G eHealth, enhanced MBB (eMBB) (Elayoubi, 2016), requiring both extremely high data rates and low-latency communication in some areas, and reliable broadband access over large coverage areas. According to (Elayoubi, 2016), ultra-reliable and low-latency capabilities are key for eHealth applications due to patient safety factors, see Figure 3.

The continuous collection and streaming of patient data will begin when the emergency ambulance paramedics arrive at the incident scene right up until the delivery of the patient to the emergency department at the destination hospital. Video sensors will enable the provision of enhanced patient insights and the goal is for all paramedics to have wearable clothing that can provide real-time high-definition video feeds as well as other sensor related data pertaining to the immediate environment. The availability of patient related real-time video stream to the awaiting emergency department will enable more intelligent decision support for the paramedics attending the patient. Real-time streaming video will enable the awaiting emergency department professionals to remotely monitor the patient for conditions that are not easily sensed such as skin pallor and patient demeanour. In other scenarios, medical devices and equipment could be 5G enabled to report health status to clinical and incident control staff.

Quality of Experience (QoE) and quality of service (QoS) metrics will be used as KPIs in assessing 5G technology in the connected ambulance scenario. The International Telecommunication Union Telecommunication Standardization Sector ITU-T P.10/G.100 defines the QoE as “level of user’s acceptance towards application and services is referred as QoE” (Brooks, 2010). QoS is analyzed on technical measures like peak data rate, spectral efficiency, packet loss, delay, jitter and other parameters which can present the negative or positive QoS (Herzog, 2016).

In order to achieve acceptable QoE and QoS in a 5G eHealth scenario the following Ultra-high reliability & Ultra-low latency data rates are recommended (Google, 2017), (Lighterra, 2012):

- Recommended video bitrates for Standard DR uploads: 1080p: 8 Mbps
- Recommended video bitrates for High DR uploads: 1080p: 10Mbps
- Bitrates required for H.264 video encoding is 5.12 Mbps (4992 kbps for video + 128 kbps for Audio).

In terms of latency (time to travel the network from the sensor to the end user), jitter and packet loss rate:

- 30 to 100ms latency end-to-end
- 10ms peak-to-peak jitter
- 0.03 to 0.05% random packet loss
- Reliability 99.999% (Accedian, 2017).

These KPIs are summarized in Table 3.

Table 3 eHealth Connected Ambulance KPIs for the eHealth Use Case

eHealth / Connected Ambulance	Experienced user throughput	Standard DR: 1080p: 8 Mbps High DR: 1080p: 10Mbps
	Traffic volume density	Low
	Connection density	Low
	Jitter	10ms peak-to-peak
	Latency	30 to 100ms ¹
	Packet Loss	0.03 to 0.05%
	Reliability	99.999%
	Mobility	on demand: 0-500 km/h

In another scenario 5G enabled Internet of Things devices (IoT) can provide major benefits for healthcare (Z. Pang, 2013), and it has the potential to correctly identify optimum times for replenishing supplies for various devices for their smooth and continuous operation (Islam, 2015). In the connected ambulance scenario, it is envisaged that oxygen tank levels would be continuously monitored by a 5G IoT device using a Critical machine-type mode of communication (uMTC) that allows immediate feedback with high reliability, although the focus in this project will be eMBB for ultra-high definition video.

In addition to the above requirements, attention must also be given to patient privacy and the end-to-end solution must meet the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679), which is a regulation by which the European Parliament, the Council of the European Union and the European Commission intend to strengthen and unify data protection for all individuals within the European Union (EU).

3.2.1 5G Market

Various reports and forecasts predict significant growth of 5G in the market place. Juniper Research forecasts 1.4 billion 5G connections by 2025, from a base of 1 million in 2019, which represents an average annual growth of 232% (Juniper, 2017). Some industry sources recommend that communication service providers (CSPs) must transform into digital service providers (DSPs) in order to remain competitive, or be relegated to the providers of internet plumbing (O'Brien, 2017).

3.2.2 5G for Health

eHealth is a vision of care delivery that is distributed, mobile and patient-centered, so the emergence of 5G will allow for a new generation of services built on MEC, SDN, NFV (Politis,

¹ Ideally the application delay would be of the order of 100ms based on suggestions of ITU for conversational video.

2016). Technologies such as ultra-high-definition video (UHDV) and Internet of Things (IoT) are gaining recognition among the health stakeholders as powerful enabling technologies. For example, it takes about eight minutes to download a feature movie using 4G, whereas with 5G technologies this will be possible in less than five seconds (Scott, 2016). UHDV and IoT enabled wearable sensors can be used to track vital signs, motion, speech pallor and demeanour, to provide real-time diagnosis of people’s health problems (Looney, 2016). Demand for these services are growing, with a survey of 12,000 adults across eight nations showing that 70% of respondents are receptive to video and IoT technology for medical consultations (Intel, 2016), (West, 2017). 5G technology will encompass data centres and cloud services and storage to provide “computing at the edge,” allowing computations to be performed near the mobile location (Politis, 2016).

A recent survey of health stakeholders for the SLICENET 5G project (<https://goo.gl/s9iVF7>) found a preference for “Self-Management w/o need to communicate to service provider”, while “improved cost efficiency” and “increase reliability” were less of a priority², see Figure 4. Figure 5 shows relative importance of key business enablers, while Figure 6 shows that only 20% of those surveyed so far do not see any relevance of the 5G technology to their next generation communication services approach.

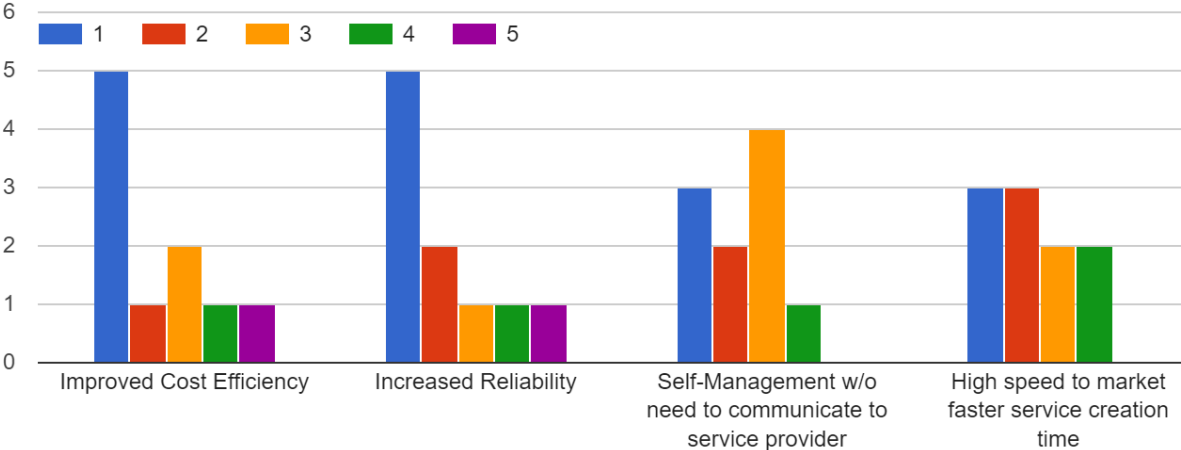


Figure 4 In the context of 5G potential offerings please rate the importance of the following, considering: Strongly Disagree (1) Disagree (2) Neutral (3) Agree (4) Strongly Agree (5)

² There are preliminary results and will need to be validated in a wider study.

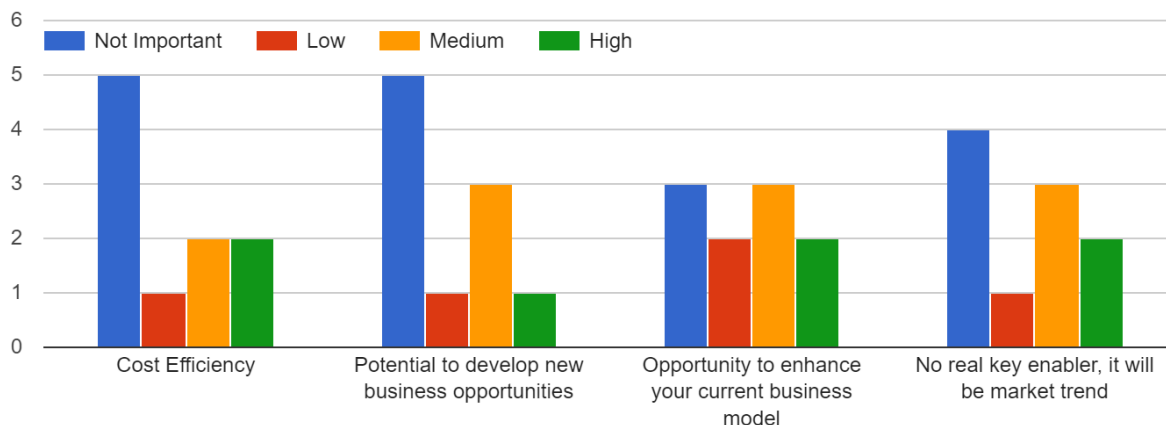


Figure 5 When thinking of your current and future business, which is the key enabler for migrating towards 5G solutions?

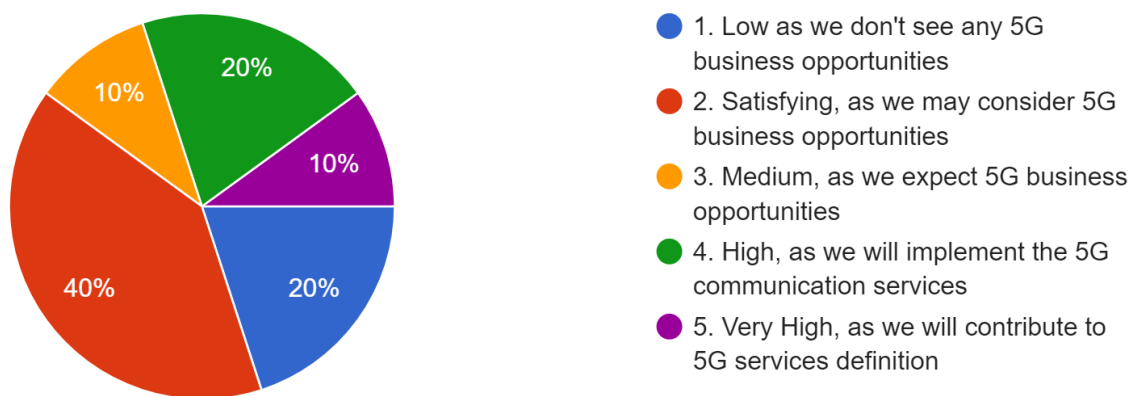


Figure 6 Please rate the relevance of the 5G technology for your next generation communication services approach

3.3 Smart City Use Case Overview

A use case is a software and system engineering term that describes how a user uses a system to accomplish a particular goal. A use case acts as a software modeling technique that defines the features to be implemented and the resolution of any errors that may be encountered [2].

The most important vertical industries in Europe are: Factories of The Future, Automotive, Health, Energy and Media & Entertainment. It is expecting that 5G will integrate different telecommunication technologies (e.g. mobile, fixed, satellite and optical), spectrum-regulatory frameworks (e.g. licensed and unlicensed) and enabling capabilities (e.g. IoT) for the benefit of these vertical industries. 5G architecture will accommodate a wide range of use cases with advanced requirements in terms of latency, resilience, coverage, and bandwidth. These use cases originating from verticals industries should be considered as drivers of 5G requirements.

In the perspective of future 5G networks, there are three main categories of use cases:

- Massive broadband (xMBB) that delivers gigabytes of bandwidth on demand;
- Massive machine-type communication (mMTC) that connects billions of sensors and machines;
- Critical machine-type communication (uMTC) that allows immediate feedback with high reliability and enables for example remote control over robots and autonomous driving.

These three main categories could be further divided in some families, each of them including some of use cases. From Orange Romania point of view the **Internet of Things** family including the Smart City Use case presents interest.

The **Internet of Things** family include devices (sensors, actuators) with a wide range of characteristics and demands for which the 5G must perform a massive deployment. A sensor is a device that detects and responds to inputs from physical environment. An actuator is responsible for moving or controlling a mechanism or a system. Sensors feel the measured characteristic and basis of that action can be performed by the actuators. The IoT family includes both low-cost/long-range/low-power machine type communication as well as broadband MTC.

Services of a **Smart City** consist in metering solution (gas, energy, water), remote monitoring of city infrastructure (pollution, temperature, humidity, noise), real-time traffic information and control, city or building lights management and public safety alerts for improved emergency response times, besides aggregation of these services with very different characteristics (which have to be combined in a common communication and interworking framework). In Table 4, we can observe the main KPIs applicable for all smart city services enumerated above.

Table 4 User Experience KPI's and system performance requirements for all Smart City use case

Smart city	Experienced user throughput	300 Mbps in DL, and 60 Mbps in UL
	Traffic volume density	700 Gbps/km ²
	Connection density	200 000 users per km ²
	Latency	Seconds to hours
	Mobility	on demand: 0-500 km/h

Smart City is an important worldwide initiative, and in EU only the annual smart city benefits from 5G is estimated to reach 8.1 billion Euros in 2025 [EU-5G].

Over the last decade, the evolution of information technologies and communications networks, sensors, actuators, cloud infrastructure, big data and products/services based on these enablers has changed the way people live in a city. Access to information, services and communication is now provided anywhere and anytime by smartphones and modern people have adapted to this new way of living. Meanwhile, various actors that create "smart city technologies" are trying to convince the governments and the public administrations that these technologies can help cities improve the efficiency, availability, quality and cost of

providing city services. At the same time, governments make transition to online services, but they must ensure that no one is left behind, not even those without access to this technology.

In this use case, we will observe how Alba Iulia, a small to middle size city in Romania with about 70k inhabitants, is moving forwards as a smart city by adopting the latest ICT technologies including LoRaWAN, LTE-M and finally 5G enablers. Alba Iulia was the first smart city from Romania, develop by Orange and is a key driver for the other cities or operators that want to develop such a solution. For the smart city use cases Orange proposes an open data strategy and open architecture that give access to further development of new applications by monetizing datasets from the city itself. The high-level architecture is constructed on three levels: data collection and transport layer, open IoT middleware layer and application layer. The data collection and transport layer will provide LoRaWAN, LTE-M and 5G specific connectivity for all sensors, actuators and consequently raw datasets that will be generated from the smart city solutions. These datasets will be sent to the open middleware platform to be stored, processed and secured. The open middleware can work also with other datasets that are not real time accessible through sensors or actuators. Alba Iulia has been selected by Orange to demonstrate the capabilities of the targeted smart city high level architecture in dealing with critical smart lighting infrastructure under the **SmaLi-5G** SLICENET and **water metering** use case.

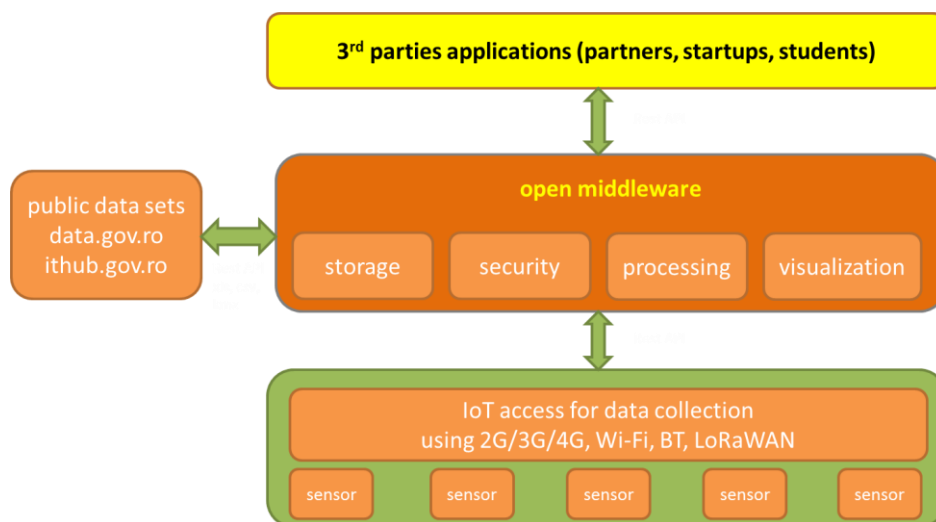


Figure 7 SmaLi-5G High Level Architecture

SmaLi-5G use case will be considered in the scope of the 5G Massive machine-type communication category where the challenge is to accommodate the massive number of connected actuators/controllers without impacting the QoS and QoE. Another service requirement to be met by the SmaLi-5G use case is to assure ultra-high network reliability and availability, while low-power, context awareness and location awareness requirements for managing the connected actuators/controllers over the access and transport layers can further improve the solution cost efficiency. This will be especially important during the daytime when the smart streets lighting poles infrastructure is supposed to remain powered to facilitate other city services (e.g. public safety surveillance, air quality monitoring, public Wi-Fi hotspots, advertising).

The second use case proposed by Orange is **water metering**. This enables the water provider to remotely read the indexes from the water meters and to be alerted in case of water

leakage, reverse flow, empty pipe or magnetic tampering. This solution helps the water provider to localize more easily any problem that can appear, leading to a shorter time of resolution and fewer wasted money.

In conclusion, the both use cases proposed by Orange will be considered in the scope of the 5G Massive machine-type communication category and will utilize the same infrastructure depicted below in chapter 6.

4 Smart Grid Self-Healing Use Case

The main purpose of the smart grid self-healing use case is to demonstrate that 5G mobile networks provide an adequate framework for power system protection and control device peer-to-peer communications.

The use case presupposes the use of a communication infrastructure like the one represented in Figure 8, in which the field devices (i.e., the remote Intelligent Electronic Devices (IEDs)) that integrate the self-healing schemes rely on a 5G Wide-Area Network (WAN) both for horizontal and vertical communication.

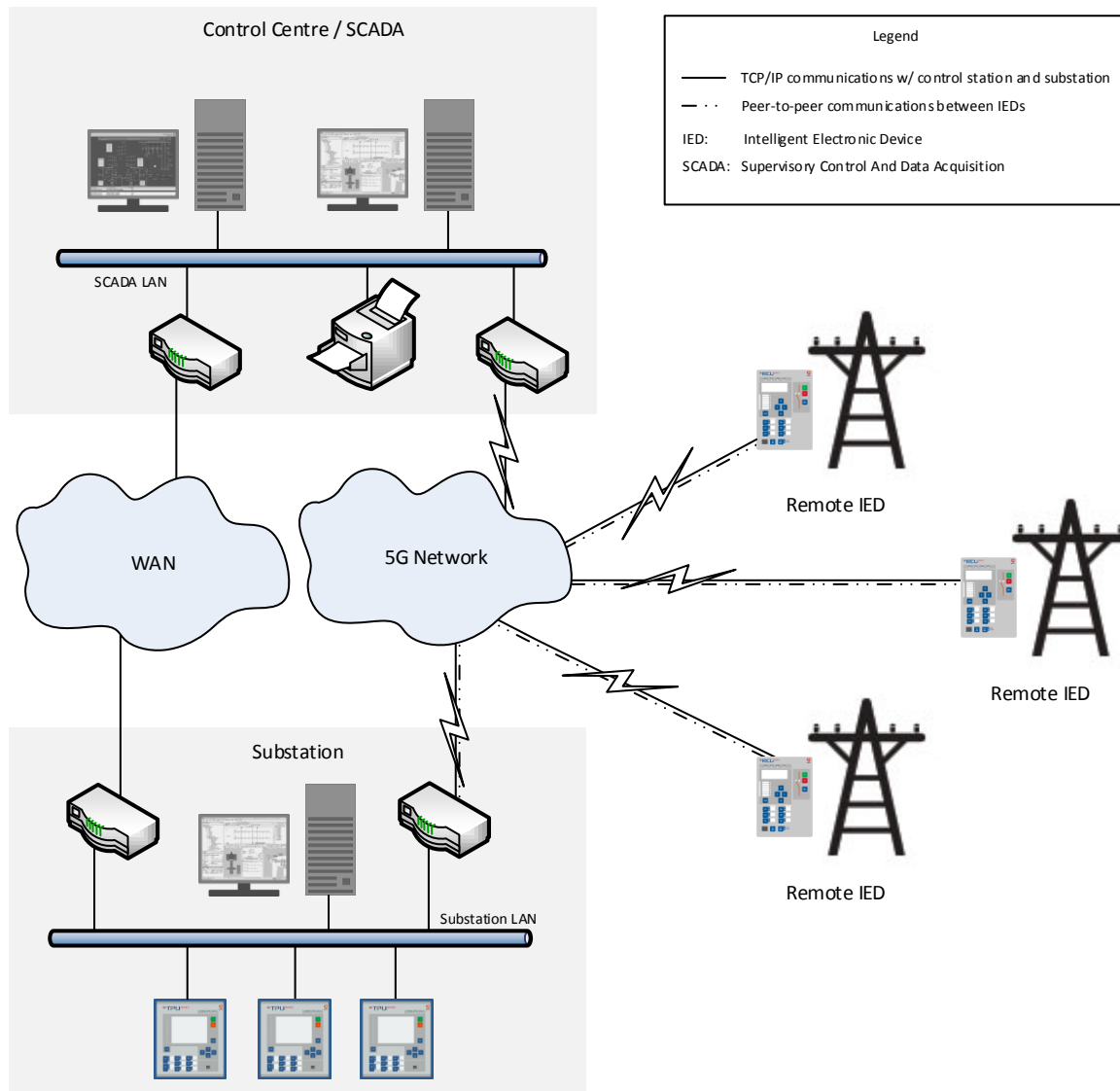


Figure 8 5G communications for smart grid self-healing applications

The present use case comprises three scenarios: protection coordination (defined in section 4.6), automatic reconfiguration (defined in section 4.7), and differential protection (defined in section 4.8).

4.1 General Background

The increasing demand for power supply Quality of Service (QoS) has motivated utilities to spread out beyond the substation environment, to increase the number of monitoring and protection-capable devices deployed along the energy distribution networks and to use these devices to implement self-healing schemes. The lack of a high-performance, reliable, and cost-effective wireless network with the required geographical coverage has been one of the major drawbacks for high-speed protection and automation schemes implemented outside contained substation environments. Although the latest advances in mobile communications have propelled the implementation of communication-based self-healing schemes, fourth generation technologies are still unable to fully comply with the demanding peer-to-peer communication needs, especially in geographical areas where signal strength and/or quality is not optimal. The need for an ultra-reliable, fault-tolerant, cybersecure communication infrastructure gains relevance for communication-based fully decentralized self-healing schemes, where a single point failure jeopardizes the entire system.

4.2 Relation to 5G Requirements and Visions

5G-PPP states that 5G will be focused on providing high Quality of Experience (QoE) not only for consumers, but also for industrial stakeholders with specific needs regarding wide area wireless communications. The 5G communication infrastructure will be designed with native support for mission-critical services with high-demanding needs such as very high reliability, very low latency, or global coverage.

Communication-based applications for smart grid self-healing require an ultra-reliable communication infrastructure with ambitious specifications that, at present, cannot be fully obtained from public wireless networks. Furthermore, bringing power system communications outside the substation isolated LANs and extending them to WANs will likely compromise power system security and make critical assets more vulnerable to cyber-attacks. Cybersecurity issues will be thoroughly addressed by the 5G infrastructure, which aims to guarantee system integrity and to assure operational security.

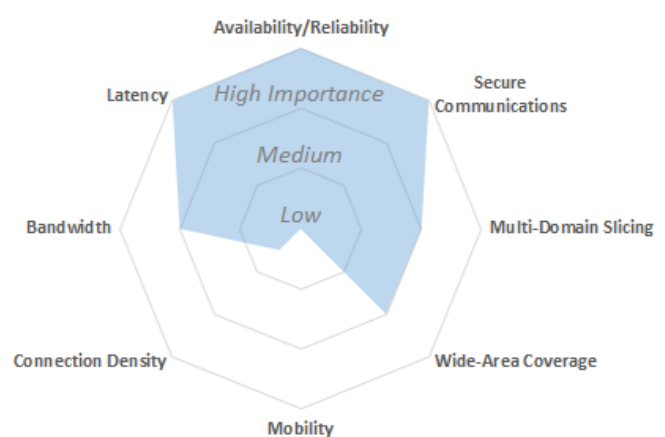


Figure 9 Importance of 5G high-level requirements for the use case scenarios

Figure 9 presents a radar diagram that characterizes the level of importance for the 5G high-level requirements of the use case scenarios.

4.3 Goals

The main goals for the smart grid self-healing use case are:

- To provide an ultra-reliable communication infrastructure for smart grid devices;
- To exchange messages between remote devices at very high speed;
- To provide deterministic communications;
- To provide secure communications between smart grid devices, focusing on the Operational Technology (OT) cybersecurity principles that favour availability and data integrity over confidentiality (1st: availability; 2nd: integrity; 3rd: confidentiality);
- To guarantee QoS and QoE under all network conditions.

4.4 General Assumptions

The smart grid self-healing use case scenarios, presented in section 4.6, section 4.7, and section 4.7.1.1, will rely on IEC 61850 peer-to-peer communication for IED coordination.

Remote IEDs are continuously monitored from the Supervisory Control And Data Acquisition (SCADA) systems and automatic and manual operations (e.g., record retrieval, remote control of switchgear, configuration and firmware deployment) can be performed from the control center at any time. Control center communications must coexist with the time-critical peer-to-peer communications that are the main focus of the present use case scenario and cannot compromise their determinism or availability under any circumstances.

General features:

- This use case will rely on IEC 61850 Generic Object Oriented Substation Events (GOOSE) [8][12] for event-driven peer-to-peer communication between power system IEDs;
- Any device integrating a self-healing scheme exchanges IEC 61850 GOOSE messages with every other device in that scheme;
- IEC 61850 Manufacturing Message Specification (MMS) [8] will be used for communications between the control center and the IEDs (acquire data from the IEDs, issue remote commands to the IEDs, perform online diagnostic);
- Engineering operations and record retrieval operations will be performed using Efacec engineering and/or system management tool(s) [18].
- Files or sets of files sent from the control center to the IEDs (firmware files, configuration files, operational settings files, etc):
 - The size of a single file is typically lower than 30 MB;
 - The size of a set of files is typically lower than 40 MB.
- Files or sets of files retrieved from the IEDs by the control center (disturbance records, event logs, etc):
 - The size of a single file is typically lower than 10 MB;
 - The size of a set of files is typically lower than 12 MB.
- The IEDs are stationary;
- The IEDs are permanently connected to the 5G network;
- IED density is typically lower than 0.5 devices/km²;
- Power system switching devices (e.g., reclosers) and consequently the IEDs that are used for controlling these devices can be located virtually anywhere (a wide geographical coverage is required);

- Typical distances between two adjacent points may range from 500 meters to 25 km (average values for Portuguese medium voltage power grid are approximately 12 km)³;
- Maximum distances between two IEDs operating in the same power system network (i.e., IEDs that may integrate the same self-healing scheme) are typically lower than 50 km³;
- During power outages, the IEDs must be able to operate and communicate on battery power for extended time periods (low power consumption is valued);
- Faults can be unpredictable and can occur at any time (high availability is required);
- Power system faults must be cleared as fast as possible (time requirements for communication-independent instantaneous fault detection can be lower than 50 ms)⁴;
- A single point failure will compromise the entire system (communications must be up for all devices at all times).

Relevant IEC 61850 GOOSE characteristics:

- User Datagram Protocol (UDP) with multicast addressing;
- Continuous stream of cyclic heartbeat messages (heartbeat rhythm is configurable and is typically set within 500 ms to 2 s);
- Messages are temporarily retransmitted at a faster rate after an event (see Figure 10);
- Messages have an incremental sequence number, reset after each event;
- Messages have an incremental state change counter (incremented after each event);
- The receiver will consider a maximum time between two consecutive messages and will assume communications are lost if that time is exceeded.

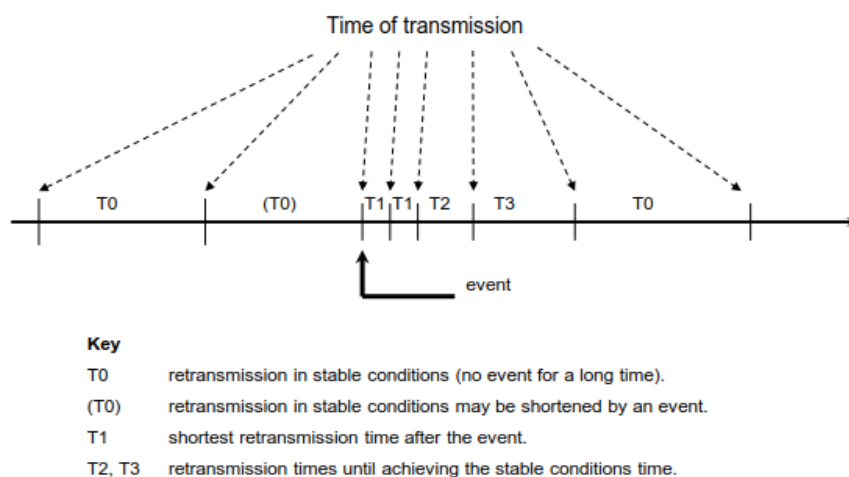


Figure 10 IEC 61850 GOOSE retransmission diagram [8]

³ The presented values are representative. Distances may vary with geography, network topology, voltage levels, and other factors.

⁴ The fault detection time corresponds to the time measured from the fault occurrence to the initiation of the trip command (it includes the protection function operating time and the output relay operating time, but it does not include the recloser or circuit breaker operating time).

Relevant IEC 61850 MMS characteristics:

- Client/server communications;
- TCP/IP;
- Uses ASN.1 basic encoding rules [16].

4.5 Actors

The actors for the use case scenario are:

- Power system protection and control IEDs;
 - Remote IEDs;
 - Substation IEDs;
- SCADA system;
- Station servers;
- Engineering stations;
- Communication services provider;
- 5G communication network;
- External subject that causes the fault in the power system.

4.6 Use Case Scenario 1: Protection Coordination**4.6.1 Overview****4.6.1.1 Storyline**

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

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

For this scenario, a single feeder protection coordination will be implemented based on a communication infrastructure allowing for information to be exchanged between all IEDs involved in the feeder Protection Automation and Control (PAC) system. All smart grid self-healing scenarios will be based on laboratory simulations in which real-world power system conditions will be replicated. For the protection coordination scenario, faults will be induced in several locations in the simulated power system network, which will cause the real-time protection-capable Intelligent Electronic Devices (IEDs) to react and actuate in a very short time. The simulated faults will be sensed simultaneously by multiple IEDs. These devices will then need to communicate with each other and coordinate in very high speed in order to ensure logic selectivity (*i.e.*, in order to ensure that the fault is cleared by the closest device, leaving as many healthy sections of the network energized as possible).

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

4.6.1.2 General Assumptions

All items referred in section 4.4 are applicable to the protection coordination scenario and must be taken in consideration throughout the scenario definition and execution. Section 4.4 includes lists of IEC 61850 GOOSE and MMS features that are relevant for the present scenario.

Protection coordination takes place during the first stages of smart grid self-healing algorithms. The automatic network reconfiguration that will provide fast service restoration to the healthy sections that have been powered down during the present scenario is covered in another use case scenario, described in section 4.7.

4.6.2 Detailed Steps

This section describes in detail the workflow and sequence of events which characterize the execution of the protection coordination scenario.

4.6.2.1 Preconditions

Before the use case scenario is executed, the power system must be operating normally (all target sections must be energized) and all protection devices in the network must be online. All field devices must be communicating with each other (IEC 61850 GOOSE) and with the control center/ substation. Some of the communication with the control center or substation may be:

- IEC 61850 MMS communications;
- File retrieval from the IEDs (event logs, disturbance records, etc.);
- Configuration and operational settings deployment;
- Access to the IEDs' webserver.

Normal voltage and current levels throughout the network.

4.6.2.2 Metrics

The system should be monitored for a pre-defined time period while in normal operation, before the use case scenario events take place. QoE and QoS must be evaluated for peer-to-peer communications between field devices and for communications between the field devices and the control center/ substation.

Measure QoE according to the following criteria:

- Absence of GOOSE failure in all devices⁵;
- Out-of-order GOOSE frames⁵.

The following metrics should be used for measuring QoS:

- End-to-End (E2E) latency;
- Packet loss/ Bit Error Rate (BER);
- Out-of-order packets.

⁵ These metrics are provided by the IEC 61850 GOOSE modules running in the IEDs.

4.6.2.3 Trigger

The protection coordination scenario is triggered by a simulated fault on a power system network section.

4.6.2.4 Post Conditions

Once the use case has been executed, the entire system should maintain normal operation (communication-wise). The metrics defined for the pre-conditions should be used for the post-conditions as well.

The use case scenario will be successful if the GOOSE events are received within the defined time (in time for the protection functions to coordinate).

The use case scenario will be unsuccessful if the GOOSE events are not received within the defined time and the protection functions running in the different devices are unable to coordinate.

4.6.2.5 Workflow

Figure 11 represents the sequence of events that define the protection coordination scenario execution.

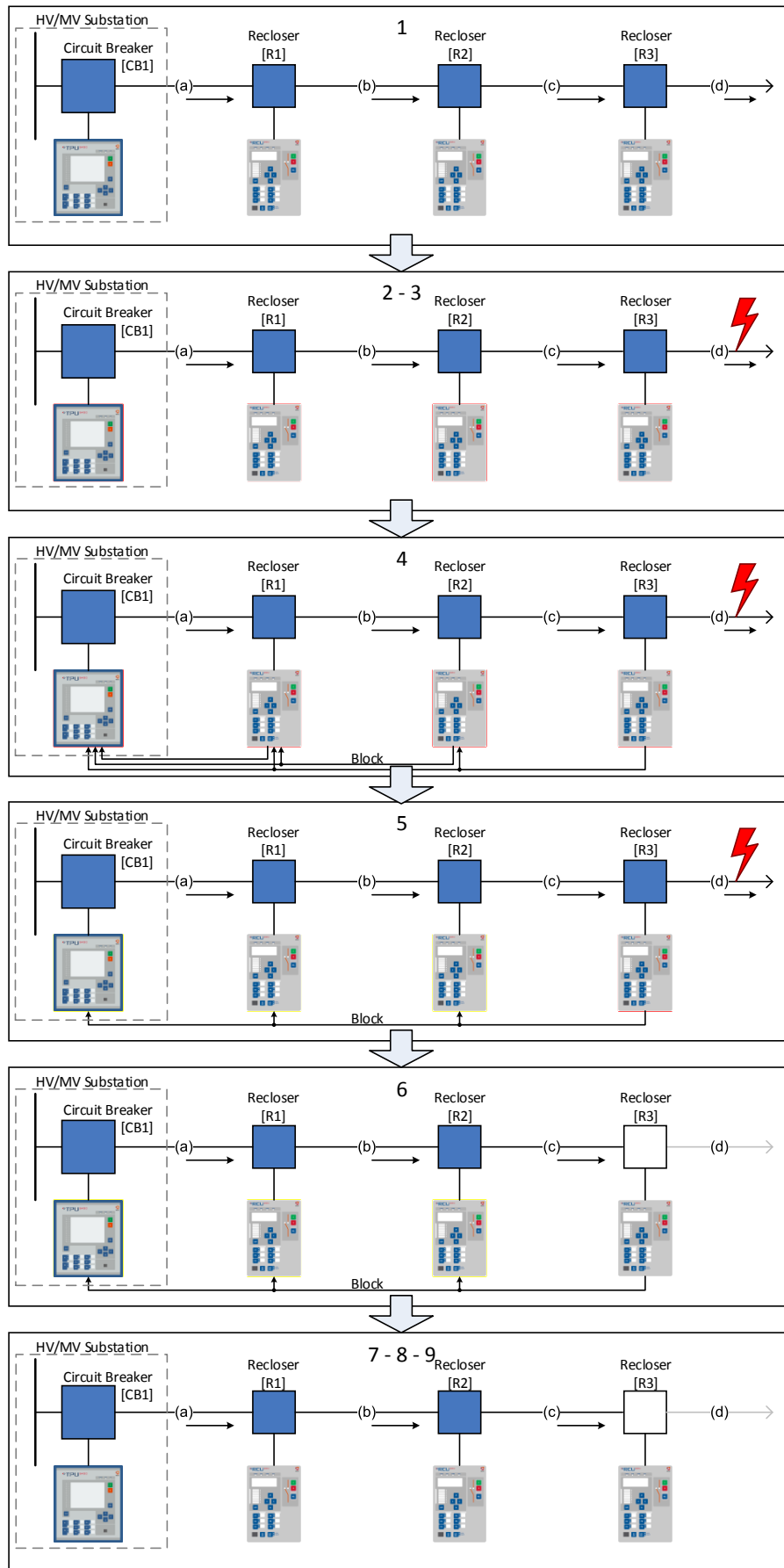


Figure 11 Protection coordination scenario activity flow

The protection coordination scenario activity diagram, illustrated in Figure 11, comprises the following sequence of states:

1. System is operating normally

The system is operating under normal conditions. All communications between field IEDs and between IEDs and the control center/ substation are up. Power system currents and voltages are stable and at normal levels.

2. Fault occurs in a downstream section

A fault is simulated in section d. Line current levels rise abruptly to fault current levels. Voltage levels are adjusted accordingly.

3. Fault is detected by all upstream devices

CB1, R1, R2, and R3 measure short-circuit current levels. Protection functions pickup (start) in all devices.

4. Devices that detect the fault send blocking signals to all upstream devices

All devices that detect the fault send blocking signals to all upstream devices via IEC 61850 GOOSE:

- R1 sends blocking signal to CB1;
- R2 sends blocking signal to R1 and CB1;
- R3 sends blocking signal to R2, R1, and CB1.

The GOOSE streams from the blocking signals change from FALSE to TRUE, temporarily increasing the frequency of message retransmissions (see Figure 10).

5. Upstream devices receive blocking signal

CB1, R1, and R2 receive blocking signal(s) via IEC 61850 GOOSE. Protection functions block and reset. Blocked devices stop sending their own blocking signals, and the corresponding GOOSE streams change from TRUE to FALSE.

6. The device closest to the fault trips, clearing the fault

After the configured delay⁶, R3 trips, opening the corresponding recloser and, consequently, clearing the fault.

7. The blocking signal is cleared

R3 stops sending the blocking signal. The GOOSE stream corresponding to the blocking signal changes from TRUE to FALSE, temporarily increasing the frequency of message retransmissions (see Figure 10).

8. Upstream devices stop receiving the blocking signal

CB1, R1, and R2 stop receiving the blocking signal. Protection functions in these devices are no longer blocked and are ready to operate if a new fault is detected.

9. Energized network sections are operating normally

All power system network sections between the substation and the open recloser (i.e., sections a, b, and c) are operating under normal conditions. Power system currents and voltages in these sections are stable and at normal levels. All communications between field IEDs and between IEDs and the control center/ substation are up (all communications must be up – even for IEDs in de-energized sections).

⁶ Protection functions have a configurable operational delay. This delay must be at least long enough to ensure that the opening command is not issued when blocking signals are sent by other devices (i.e., it must account for the maximum end-to-end GOOSE message latency). In some cases, it may be necessary to adjust (increase) this delay for the IEDs to coordinate with non-communicating devices in the power grid (e.g., fuses).

4.6.3 Performance Requirements

Table 5 Performance requirements for peer-to-peer communications

Requirements	Minimum	Optimal
E2E latency	≤ 10 ms	≤ 5 ms
BER	$< 10^{-4}$	$< 10^{-6}$
Bandwidth (down/up)	10/1 Mbps	20/2 Mbps

The values presented in Table 5 were estimated by analyzing the performance data indicated in [10] and [13] for the reverse blocking function, teleprotection, and telecontrol applications.

The smart grid self-healing use case presupposes protection coordination and automatic reconfiguration are implemented in the same network scheme. Hence, the performance requirements specified in section 4.7.3 for peer-to-peer communication should be also be considered, in addition to the values indicated in Table 5.

Although not as time-critical as the peer-to-peer communications, communications with the control center must also be considered for this scenario. Requirements for some of these supporting functions are presented in Table 9.

The bandwidth values indicated in Table 5 are not required for continuous streaming – they may be required for short periods of time (tens of milliseconds) during sporadic data bursts. This bandwidth can be shared with lower priority network traffic. These values refer to each IED's throughput and were discriminated for downloaded data (GOOSE traffic subscribed by the IED) and uploaded data (GOOSE traffic published by the IED).

The end-to-end latency in Table 5 regards the transfer time between any two IEDs in the network.

4.7 Use Case Scenario 2: Automatic Reconfiguration

4.7.1 Overview

4.7.1.1 Storyline

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

All smart grid self-healing scenarios will be based on laboratory simulations in which real-world power system conditions will be replicated. For the automatic reconfiguration scenario, faults will be induced in several locations in the simulated power system network, which will cause the real-time protection-capable Intelligent Electronic Devices (IEDs) to react and actuate in a very short time. Once a fault is cleared by one of the devices, part of the power network will be de-energized. In most cases the de-energized areas will include healthy network sections. In order to reduce power outage durations for a potentially large number of consumers, the power grid topology will reconfigure automatically, providing alternate power supply paths for the healthy sections.

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

4.7.1.2 General Assumptions

All items referred in section 4.4 are applicable to the automatic reconfiguration scenario and must be taken in consideration throughout the scenario definition and execution. Section 4.4 includes lists of IEC 61850 GOOSE and MMS features that are relevant for the present scenario.

Automatic network reconfiguration takes place after a fault has been cleared by protection-capable IEDs. The protection coordination and differential protection scenarios, described in sections 4.6 and 4.8, respectively, present two distinct approaches for implementing the first stage of the self-healing schemes, both based on peer-to-peer communications.

4.7.2 Detailed Steps

This section describes in detail the workflow and sequence of events which characterize the execution of the automatic reconfiguration scenario.

4.7.2.1 Preconditions

Before the use case scenario is executed, the power system must be operating normally (all target sections must be energized) and all protection devices in the network must be online. All field devices must be communicating with each other (IEC 61850 GOOSE) and with the control center/ substation. Some of the communication with the control center or substation may be:

- IEC 61850 MMS communications;
- File retrieval from the IEDs (event logs, disturbance records, etc.);
- Configuration and operational settings deployment;
- Access to the IEDs' webserver.

Normal voltage and current levels throughout the network.

4.7.2.2 Metrics

The system should be monitored for a pre-defined time period while in normal operation, before the use case scenario events take place. QoE and QoS must be evaluated for peer-to-peer communications between field devices and for communications between the field devices and the control center/ substation.

Measure QoE according to the following criteria:

- Absence of GOOSE failure in all devices⁷;
- Out-of-order GOOSE frames⁷.

⁷ These metrics are provided by the IEC 61850 GOOSE modules running in the IEDs.

The following metrics should be used for measuring QoS:

- End-to-End (E2E) latency;
- Packet loss/ Bit Error Rate (BER);
- Out-of-order packets.

4.7.2.3 Trigger

The automatic reconfiguration scenario is triggered by a simulated fault on a power system network section.

4.7.2.4 Post Conditions

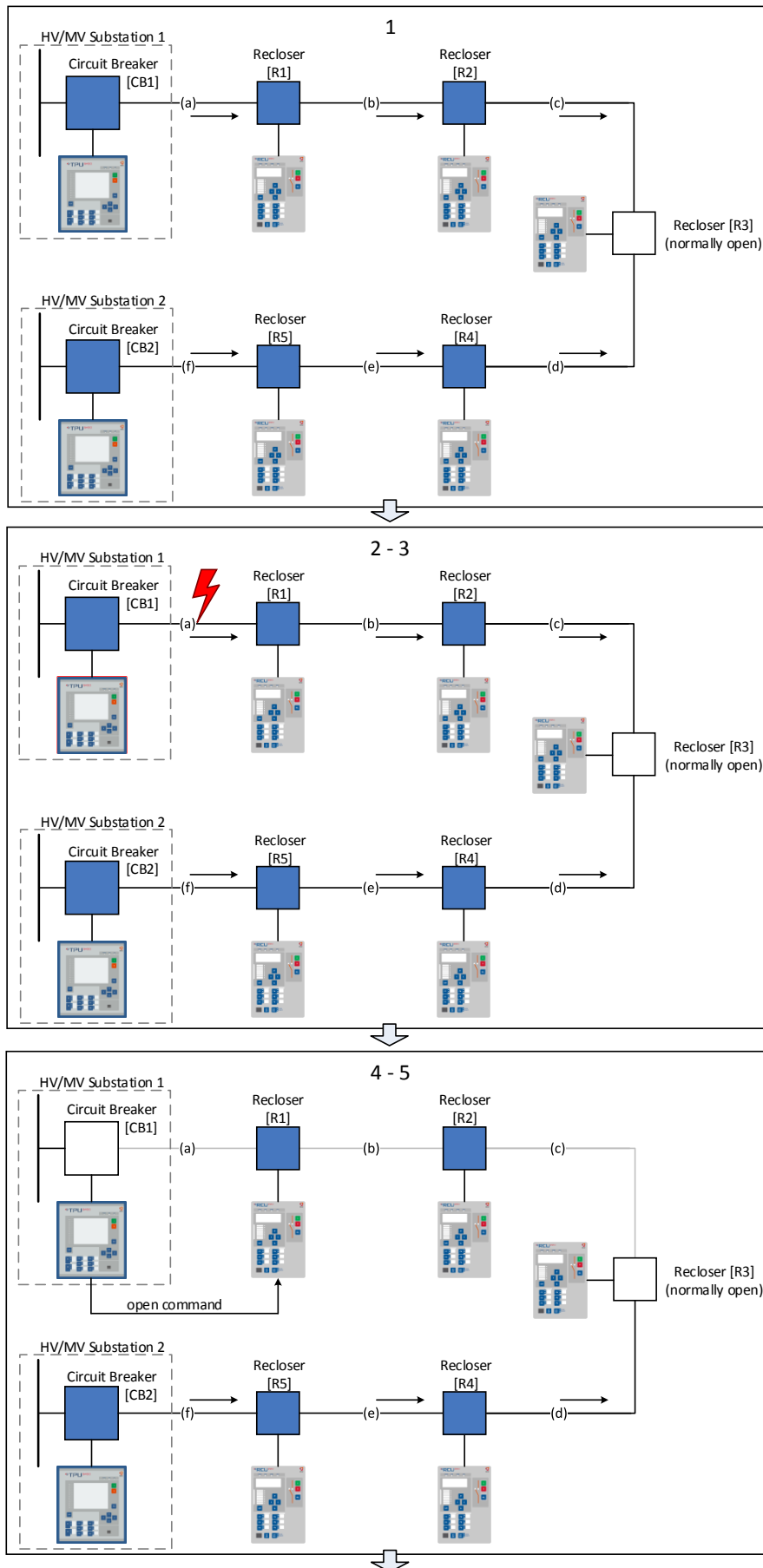
Once the use case has been executed, the entire system should maintain normal operation (communication-wise). The metrics defined for the pre-conditions should be used for the post-conditions as well.

The use case scenario will be successful if the GOOSE events are received within the defined time and the power system network is reconfigured correctly.

The use case scenario will be unsuccessful if the GOOSE events are not received within the defined time and the power system network is unable to reconfigure or if the reconfiguration is not done correctly.

4.7.2.5 Workflow

Figure 12 represents the sequence of events that define the automatic reconfiguration scenario execution.



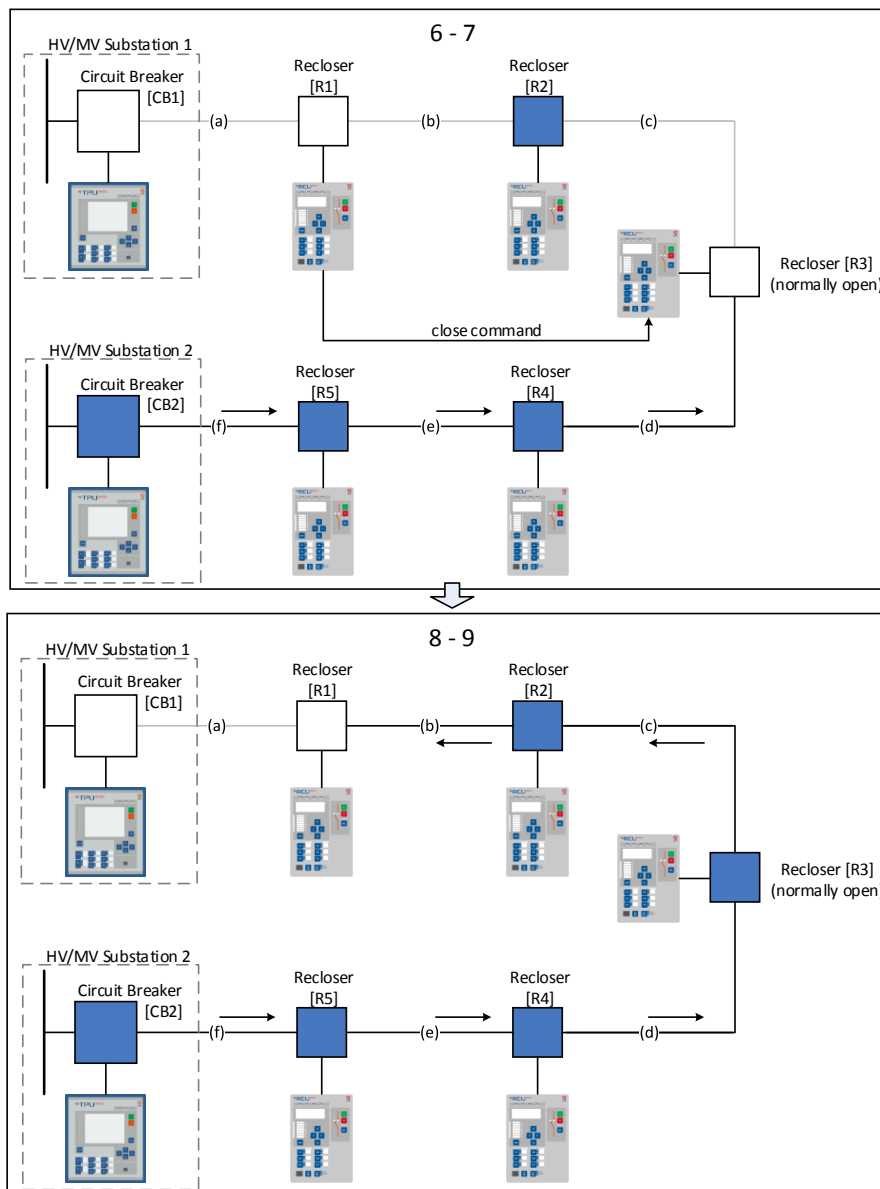


Figure 12 Automatic reconfiguration scenario activity flow

The automatic reconfiguration scenario activity diagram, illustrated in Figure 12, comprises the following sequence of states:

1. System is operating normally

The system is operating under normal conditions. All communications between field IEDs and between IEDs and the control center/ substation are up. Power system currents and voltages are stable and at normal levels.

2. Fault occurs in a network section

A fault is simulated in section a. Line current levels rise abruptly to fault current levels. Voltage levels are adjusted accordingly.

3. Fault detected

CB1 measures short-circuit current levels and its protection functions pickup (start).

4. Circuit breaker open, fault cleared

CB1 trips, opening the circuit breaker and clearing the fault. All line sections between the open circuit breaker and the normally open point (i.e., sections a, b, and c) will be de-energized.

5. Open command sent to the nearest downstream device

The device that cleared the fault (CB1) sends an open command to the nearest downstream device (R1) via IEC 61850 GOOSE.

6. Nearest downstream device opens

R1 receives the open command and opens the recloser.

7. Close command sent to the normally open device

After the device opens, a close command is sent to the IED connected to the normally open point (R3) via IEC 61850 GOOSE.

8. Normally open device closes, energizing the healthy sections

R3 closes, energizing the healthy line sections (sections b and c).

9. Energized network sections are operating normally

All line sections between the normally open recloser (which is now closed) and R1 (i.e., sections b and c) are now supplied from substation 2 (alternative path) and are operating under normal conditions. Power system currents and voltages in these sections are stable and at normal levels. All communications between field IEDs and between IEDs and the control center/ substation are up (all communications must be up – even for IEDs in de-energized sections).

4.7.3 Performance Requirements

Table 6 Performance requirements for peer-to-peer communications

Requirements	Minimum	Optimal
E2E latency	≤ 30 ms	≤ 10 ms
BER	< 10 ⁻⁴	< 10 ⁻⁶
Bandwidth (down/up)	5.9M/600k bps	17/1.7 Mbps

The values presented in Table 6 were estimated by analyzing the performance data indicated in [10] and [13] for the reverse blocking function, teleprotection, and telecontrol applications.

The smart grid self-healing use case presupposes protection coordination and automatic reconfiguration are implemented in the same network scheme. Hence, the performance requirements specified in section 4.6.3 for peer-to-peer communication should be also be considered, in addition to the values indicated in Table 6.

Although not as time-critical as the peer-to-peer communications, communications with the control center must also be considered for this scenario. Requirements for some of these supporting functions are presented in Table 9.

The bandwidth values indicated in Table 6 are not required for continuous streaming – they may be required for short periods of time (tens of milliseconds) during sporadic data bursts. This bandwidth can be shared with lower priority network traffic. These values refer to each IED's throughput and were discriminated for downloaded data (GOOSE traffic subscribed by the IED) and uploaded data (GOOSE traffic published by the IED).

The end-to-end latency in Table 6 regards the transfer time between any two IEDs in the network.

4.8 Use Case Scenario 3: Differential Protection

4.8.1 Overview

4.8.1.1 Storyline

The present scenario focuses on differential protection schemes, which provide an alternative to the protection coordination strategies introduced in the first scenario (see section 4.6). This method is faster and more accurate, and allows for more complex power system network topologies. However, it is computationally more demanding and has more ambitious communication requirements, which are not yet fully met by the public wide-area wireless networks currently available.

Differential protection works by comparing the current flowing through different points of the power system network. In order to be able to implement differential protection schemes, Intelligent Electronic Devices (IEDs) located in specific power system network sections rely on having access to an uninterrupted stream of the current values measured by remote devices, which will be continuously compared with the local measurements.

All smart grid self-healing scenarios will be based on laboratory simulations in which real-world power system conditions will be replicated. For the differential protection scenario, faults will be induced in several locations in the simulated power system network, which will cause the real-time protection-capable IEDs to react and actuate in a very short time. The simulated faults will only be sensed by the IED(s) monitoring that specific network section.

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

4.8.1.2 General Assumptions

All items referred in section 4.4 are applicable to the differential protection scenario and must be taken in consideration throughout the scenario definition and execution. Section 4.4 includes lists of IEC 61850 GOOSE and MMS features that are relevant for the present scenario.

The differential protection scenario provides an alternative to protection coordination, described in section 4.6 (the two approaches are not intended to be implemented on the same network scheme). The automatic network reconfiguration that will provide fast service restoration to the healthy sections that have been powered down during the present scenario is covered in another use case scenario, described in section 4.7.

Differential protection will be performed resorting to time-synchronized measurements (synchrophasors [14][15]). Synchrophasor measurements will be transmitted peer-to-peer using IEC 61850-9-2 Sampled Values (SV) [9][12].

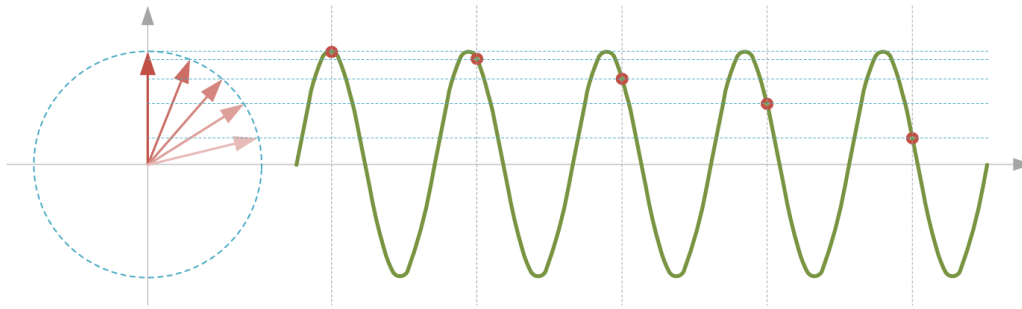


Figure 13 Synchrophasor measurement representation [19]

IEEE synchrophasor data characteristics:

- User Datagram Protocol (UDP) with multicast addressing;
- Continuous stream of phasor data (Figure 13), at fractions of network cycles (power system network frequencies can be 50 Hz or 60 Hz)⁸;
- Synchrophasor data requires accurate Coordinated Universal Time (UTC) time tagging (resolution of at least 1 μ s; accuracy of at least 2 μ s);
- Applications that subscribe the data stream will not be able to operate if more than one message per network cycle is lost or delayed.

4.8.2 Detailed Steps

This section describes in detail the workflow and sequence of events which characterize the execution of the differential protection scenario.

4.8.2.1 Preconditions

Before the use case scenario is executed, the power system must be operating normally (all target sections must be energized) and all protection devices in the network must be online. All field devices must be communicating with each other (IEC 61850 GOOSE) and with the control center/ substation; field devices must be streaming synchrophasor measurements via IEC 61850 SV. Some of the communication with the control center or substation may be:

- IEC 61850 MMS communications;
- File retrieval from the IEDs (event logs, disturbance records, etc.);
- Configuration and operational settings deployment;
- Access to the IEDs' webserver.

Normal voltage and current levels throughout the network.

4.8.2.2 Metrics

The system should be monitored for a pre-defined time period while in normal operation, before the use case scenario events take place. QoE and QoS must be evaluated for peer-to-peer communications between field devices and for communications between the field devices and the control center/ substation.

Measure QoE according to the following criteria:

⁸ A 50 Hz network will be simulated for the smart grid self-healing use case. The differential protection application will require measurement data to be sent every $\frac{1}{4}$ cycle (i.e., every 5 ms).

- Absence of lost synchrophasor data frames;
- Absence of out-of-order synchrophasor frames;
- Differential protection function should never block due to missing or delayed synchrophasor data frames;
- Absence of GOOSE failure in all devices⁹;
- Out-of-order GOOSE frames⁹.

The following metrics should be used for measuring QoS, and should be evaluated individually for GOOSE and for synchrophasor communication:

- End-to-End (E2E) latency;
- Packet loss/ Bit Error Rate (BER);
- Out-of-order packets.

4.8.2.3 Trigger

The differential protection scenario is triggered by a simulated fault on a power system network section.

4.8.2.4 Post Conditions

Once the use case has been executed, the entire system should maintain normal operation (communication-wise). The metrics defined for the pre-conditions should be used for the post-conditions as well.

The use case scenario will be successful if the continuous stream of synchrophasor data frames is received in time and in the correct order, ensuring the correct operation of the differential protection.

The use case scenario will be unsuccessful if the continuous stream of synchrophasor data frames is not received in time or in the correct order, and the differential protection is compromised or unable to operate.

4.8.2.5 Workflow

Figure 14 represents the sequence of events that define the differential protection scenario execution.

⁹ These metrics are provided by the IEC 61850 GOOSE modules running in the IEDs.

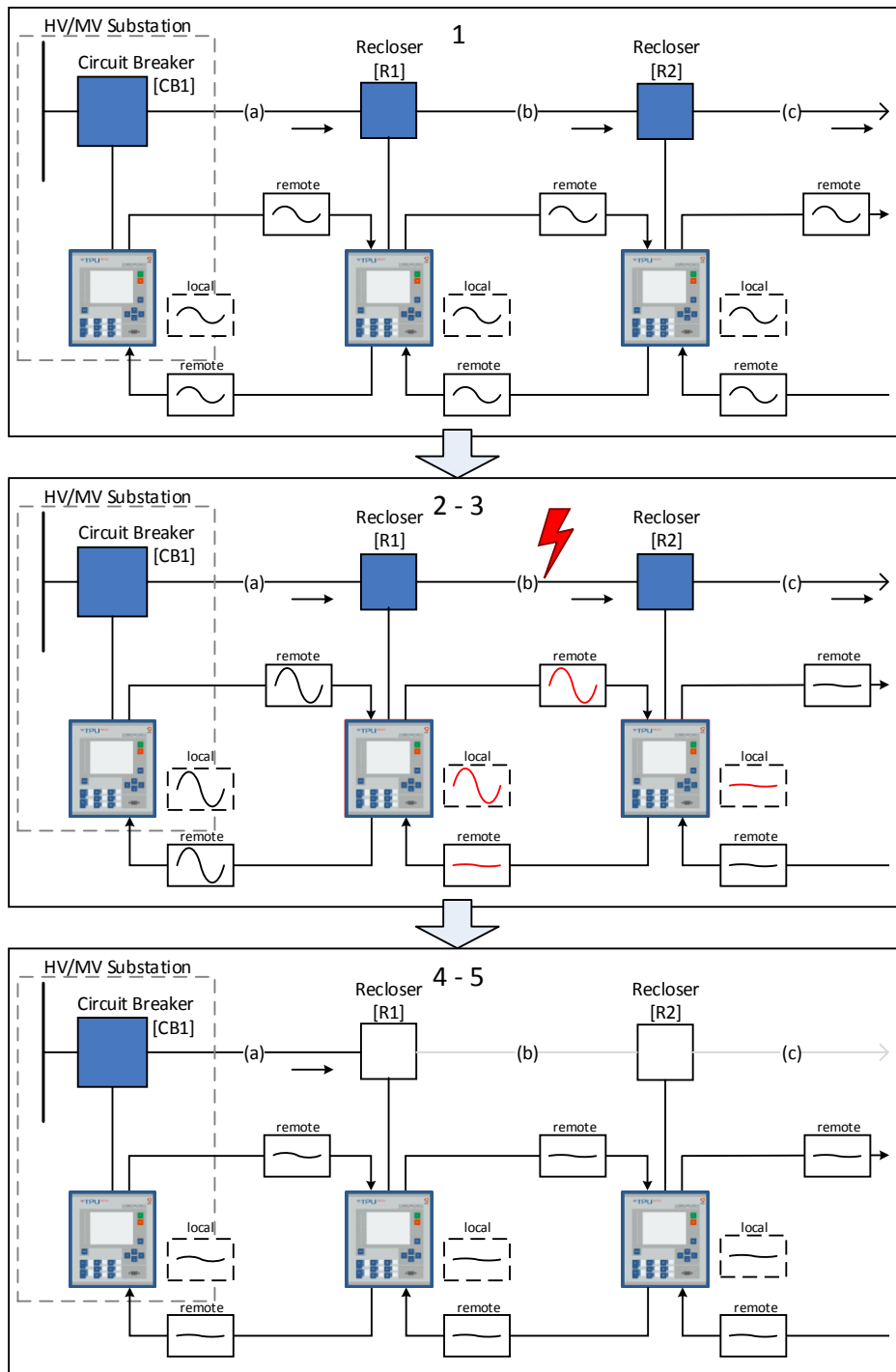


Figure 14 Differential protection scenario activity flow

The differential protection scenario activity diagram, illustrated in Figure 14, comprises the following sequence of states:

1. System is operating normally

The system is operating under normal conditions. All communications between field IEDs and between IEDs and the control center/ substation are up. Power system currents and voltages are stable and at normal levels.

2. Fault occurs in a network section

A fault is simulated in section b. Line current and voltage levels are adjusted accordingly for all devices. There will be significant differences between the current levels measured in section b and in section c.

3. The fault is only detected by the devices immediately upstream and downstream from the fault

R1 and R2 will be the only devices whose local measurements will be significantly different from the synchrophasor measurements sent by remote devices. Significant differences in local and remote measurements will cause the differential protection to start.

4. The devices that detected the fault trip, clearing the fault

R1 and R2 trip, opening the corresponding reclosers and, consequently, clearing the fault.

5. Energized network sections are operating normally

All power system network sections between the substation and the open recloser (i.e., section a) are operating under normal conditions. Power system currents and voltages in these sections are stable and at normal levels. All communications between field IEDs and between IEDs and the control center/ substation are up (all communications must be up – even for IEDs in de-energized sections).

4.8.3 Performance Requirements

Table 7 Requirements for IEC 61850 SV communications (for synchrophasor measurements)

Requirements	Minimum	Optimal
E2E latency	≤ 5 ms	≤ 3 ms
BER	$< 10^{-6}$	$< 10^{-8}$
Bandwidth (down/up)	1.6M/512k bps	3.2/1 Mbps

The values presented in Table 7 were estimated by analyzing the performance data indicated in [13] for differential protection and analogue value comparison teleprotection applications.

Table 8 Requirements for IEC 61850 GOOSE peer-to-peer communications (for event-driven communication)

Requirements	Minimum	Optimal
E2E latency	≤ 10 ms	≤ 5 ms
BER	$< 10^{-4}$	$< 10^{-6}$
Bandwidth (down/up)	17/1.7 Mbps	30/3 Mbps

The values presented in Table 8 were estimated by analyzing the performance data indicated in [13] for teleprotection and telecontrol applications.

The smart grid self-healing use case presupposes differential protection and automatic reconfiguration are implemented in the same network scheme. Hence, the performance requirements specified in section 4.7 for peer-to-peer communication should be also be considered, in addition to the values indicated in Table 7 and Table 8.

Although not as time-critical as the peer-to-peer communications, communications with the control center must also be considered for this scenario. Requirements for some of these supporting functions are presented in Table 9.

The bandwidth values indicated in Table 8 are not required for continuous streaming – they may be required for short periods of time (tens of milliseconds) during sporadic data bursts. This bandwidth can be shared with lower priority network traffic. These values refer to each IED's throughput and were discriminated for downloaded data (GOOSE traffic subscribed by the IED) and uploaded data (GOOSE traffic published by the IED).

The end-to-end latency in Table 7 and Table 8 regards the transfer time between any two IEDs in the network.

4.9 Technical Requirements

The technical requirements described in this section are further detailed in Annex A.

4.9.1 Requirements on Cognition (Intelligence)

It may be possible to distinguish two distinct system behaviors: normal operation and alarm operation. After a fault has been detected in the power grid, there will be an increased amount of GOOSE events, which will consequently increase the time-critical communication traffic (see Figure 10).

In this context, slice operation may vary between normal and alarm operation.

- State change should therefore be detectable by slice intelligent management to arrange resource and performance availability according to the timing requirements of the retransmissions;
- Intelligence should be able to process annotations to accommodate different behaviors.

This feature should only be considered/ implemented if switching between network states does not have a negative impact on peer-to-peer communication performance in the instant a power system fault is detected (when it is needed the most).

4.9.2 Requirements on the One-Stop API

The installation of power grid protection and automation devices along power lines are typically covered by utilities' stepwise investment plans. Therefore, it is often necessary to improve and increase the number of devices installed in a power system network over large periods of time.

Since utilities must be able to easily expand their power grid protection and self-healing capabilities, it is important to guarantee scalability and commissioning efficiency. This implies providing efficient means for deploying new power system equipment and IEDs in the power system networks.

Devices should be addressable and identifiable to allow for ownership management with automated inclusion in the slices allocated to the organization that deploys the equipment. Devices should be easily registered (offline) and detected when activated for being under the control of a common overlay management system.

Bandwidth requirements for peer-to-peer communications may vary with the number of IEDs integrating a self-healing scheme. The remaining requirements are constant, regardless of the number of IEDs (the values presented in Table 5, Table 6, and Table 8 have been estimated for a considerably large topology comprising 11 IEDs). If it is technically viable and considered to be economically expedite, the bandwidth levels provided by a slice may be adjusted when the number of IEDs implementing a self-healing scheme changes.

4.9.3 Requirements on Slicing/Slice

If viable, the IEDs could use two different slices: one for the more demanding real-time peer-to-peer communications, and the other for communicating with the SCADA system.

The slice defined for the time-critical peer-to-peer communications used for protection coordination (section 4.6), automatic reconfiguration (section 4.7), and differential protection (section 4.8) should guarantee the performance requirements described in sections 4.6.3, 4.7.3, and 4.8.3, as well as the availability, and cybersecurity requirements described throughout the following sections.

The slice defined for the management and control communications with the SCADA system is common to all scenarios and should guarantee the performance requirements indicated in Table 9, as well as the availability and cybersecurity requirements described throughout the following sections.

Table 9 Performance requirements for communications with control centre/SCADA

Application	E2E latency	BER	Bandwidth
Operator commands	≤ 300 ms	< 10 ⁻⁶	10 kbps
Alarms/ events /measurements	≤ 1 s	< 10 ⁻⁶	10 kbps
File transfer	≤ 10 s	< 10 ⁻⁶	1 Mbps

The values presented in Table 9 were estimated by analyzing the performance data indicated in [11] and [13] for file transfer and SCADA applications.

Slices should automatically attach devices when activated and for which the identity is related with the overall slice “ownership/allocation”. Slices should be expandable not only in terms of network resources at the core but also in terms of devices attached to them.

4.9.4 Requirements on Multi-domain Operations

Power system networks are spread out over wide areas (they may range to hundreds of km²). The IEDs operating in these networks are stationary, but may be integrated in self-healing schemes and may need to coordinate with other devices in remote locations (distances between two communicating devices in the same network may be longer than 40 km)¹⁰.

Peer-to-peer communication between remote IEDs and communication between these IEDs and the substation and/or control center must be seamless, even if the different devices are spread out among multiple operators and/or multiple providers. All other requirements must be complied with even under these circumstances.

¹⁰ The presented values are representative. Distances may vary with geography, network topology, voltage levels, and other factors.

Communication requirements should be addressable in multi-domain fashion. Assuming that Sshould guarantee overall Service Level Agreement (SLA) support and specifically scheduling of communications should be synchronized across different operators. Inter-domain scheduling should be subject to slice definition.

SLA-related requirements should be consistent throughout the entire system.

Table 10 Uptime/ availability requirements for all communications

Requirements	Minimum	Optimal
Uptime/ availability	$\geq 99.999\%$	$\geq 99.9999\%$
Downtime (per 30 days)	$\leq 25.920\text{ s}$	$\leq 2.592\text{ s}$
Downtime (per day)	$\leq 864\text{ ms}$	$\leq 86.4\text{ ms}$

Table 11 Recovery delay requirements, per application

Message type/ application	Minimum	Optimal
Peer-to-peer synchrophasor measurements communication (IEC 61850 SV)	$< 50\text{ ms}$	0
Peer-to-peer event-driven communication (IEC 61850 GOOSE)	$< 500\text{ ms}$	$< 50\text{ ms}$
Operator commands	$< 500\text{ ms}$	$< 50\text{ ms}$
Alarms/ events/ measurements	$< 2\text{ s}$	$< 50\text{ ms}$
File transfer	$< 20\text{ s}$	$< 500\text{ ms}$

The values presented in Table 10 and Table 11 were estimated by analyzing the performance data indicated in [13] for generic IP traffic and for differential protection, teleprotection, and telecontrol applications.

4.9.5 Requirements on RAN

High-level communication scheduling should be applied to Radio Access Network (RAN) management (resources and timings). This may require Real-Time constraints and proactive radio resources allocation ready to be utilized by devices.

4.9.6 Requirements on MEC

Although confidentiality is not critical for these applications, it is very important to guarantee that the data exchanged between power system devices is not tampered with. This is particularly relevant for devices communicating over a public network, where they become more vulnerable to malicious attacks.

A high level of reliability and cybersecurity (mainly for guaranteeing availability and data integrity) should be ensured by the 5G infrastructure by resorting to technologies and algorithms such as:

- Encryption for data integrity assurance (e.g., using encrypted hashes or a signature-based approach);
- Transmission path selection/ assurance (selection of a trusted communication path).

Mobile Edge Computing (MEC) should be able to instantiate virtual functionality aiming at addressing any close-to-device processing.

4.9.7 Requirements on Core

The communication infrastructure used for IEC 61850 SV and IEC 61850 GOOSE requires UDP with multicast addressing.

4.9.8 Requirements on Enterprise Network

The smart grid enterprise network, represented in Figure 15, is not approached by any of the presented scenarios. There are several applications that are typically run and managed by the Distribution System Operator (DSO) on the enterprise network, such as asset management, enterprise resource planning, geographic information system, market management system, or account management. It's crucial that this network is securely isolated from the SCADA, substation, and remote devices.

The enterprise network will not be connected to the 5G network and, consequently, will not be covered by the E2E network slices.

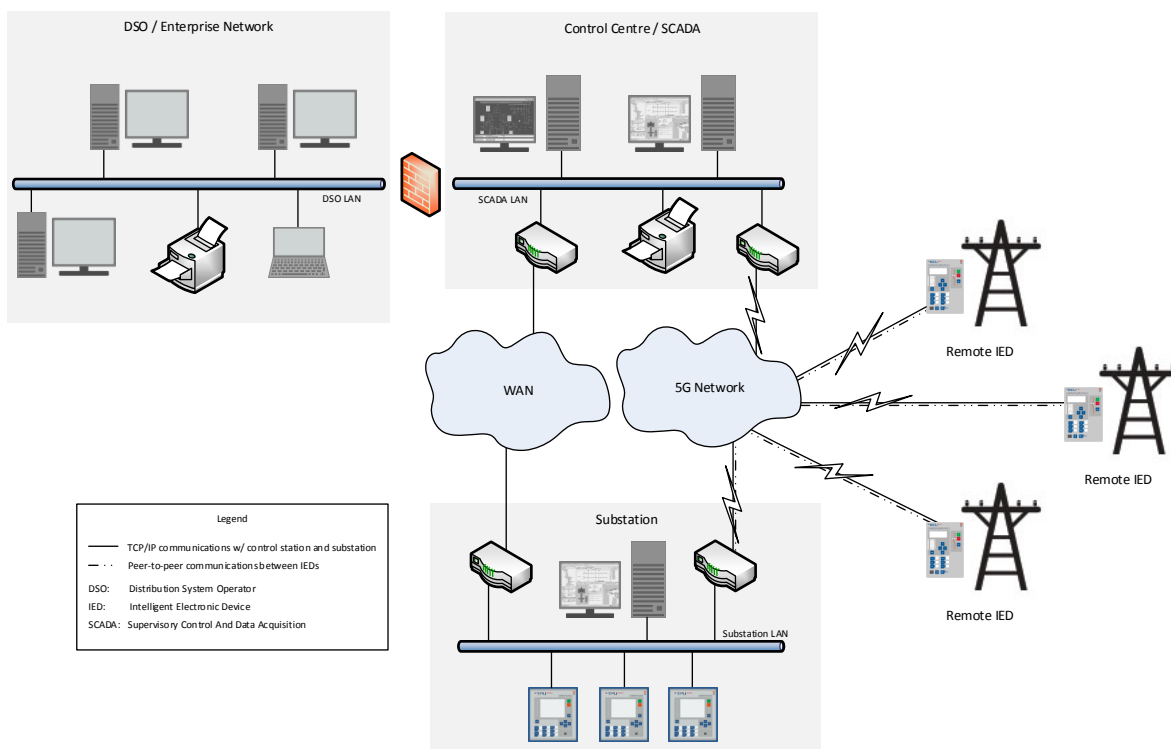


Figure 15 Smart Grid communication architecture, figuring the enterprise network

4.9.9 Non-functional Requirements

During power outages, the IEDs must be able to operate and communicate on battery power for extended time periods. It is crucial that, even under these circumstances, the switching devices (e.g., reclosers) are still capable of performing switching and closing operations. Since these operations are power consuming, it is important to save as much battery power as possible. Therefore, low power-consuming communications add value to power grid automation.

4.9.10 Coverage of Service Life-cycle Phases

The smart grid devices used for self-healing applications, which are the basis of this use case, require continuous service. Typically, the service request will be issued by the utilities, the conditions will be negotiated with the service providers/ operators, and the resulting service/ slice(s) will remain active for an extended period (indefinitely).

This use case does not cover the different service life-cycle phases – it takes place solely on the Operation and Monitoring phase (phase 4).

4.10 Implementation, Evaluation and Impact

4.10.1 Prototyping/Testbed

A power system network will be simulated in laboratory environment. The self-healing scheme will be implemented with a maximum of 11 IEDs (an example is shown in Figure 16). These values are merely informative and correspond to the absolute maximum – less complex topologies will likely be used.

- A maximum of 3 substation IEDs;
- A maximum of 8 remote IEDs (6 normally closed devices and 2 normally open devices).

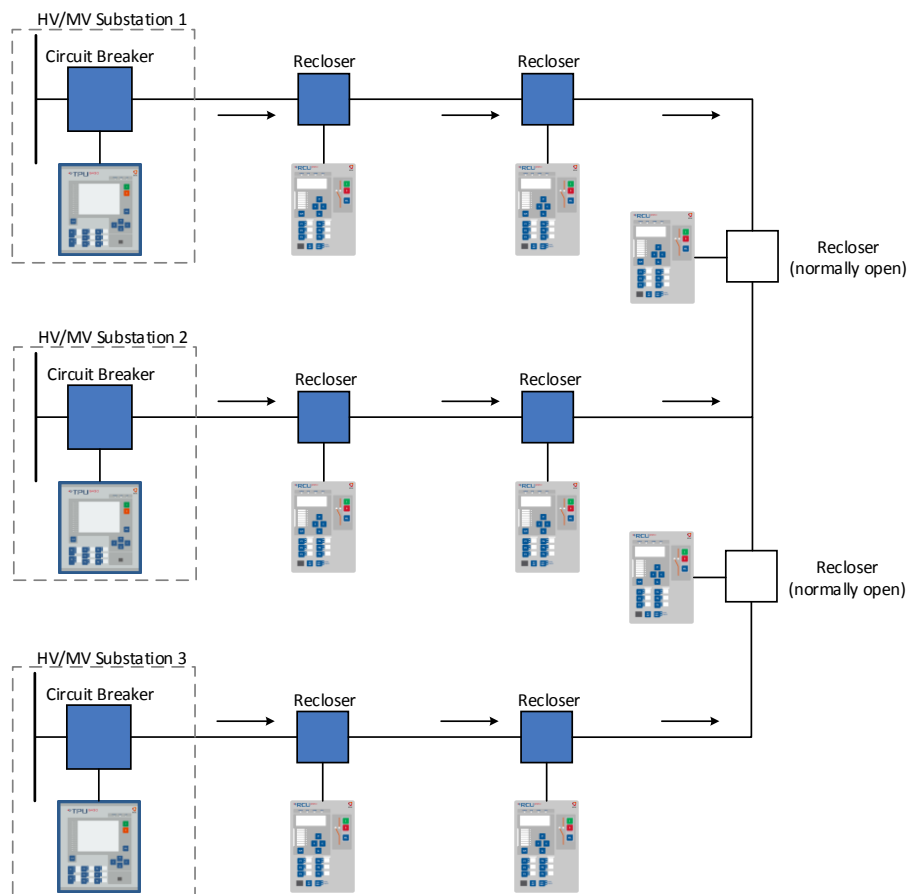


Figure 16 Example of a maximum topology

The smart grid self-healing use case will be tested in laboratory environment, using the following devices:

- Scenarios 1 and 2:
 - Efacec RCU 220E recloser controller units (protection-capable remote IEDs) [17] equipped with 5G-capable modems;
 - Efacec TPU S220/ TPU S430 terminal protection units (protection-capable substation IEDs) [17];
- Scenario 3:
 - Efacec TPU 500 Ed. 2 terminal protection units (protection-capable IEDs) [17] equipped with 5G-capable modems;
- Common to all scenarios:
 - PC(s) running Efacec software [18]:
 - UC 500;
 - Automation Studio (engineering tool);
 - System Point (system management tool);
 - Substation equipment and PC must be connected to a 5G-capable modem.

Power system network quantities (i.e., currents and voltages) in normal operation and during faults will be simulated using secondary injection test sets and a power system simulation engine. Power system quantities will be simulated at a 50 Hz rated network frequency.

4.10.2 Benchmarking and Validation

The success or failure of the use case scenarios will be evaluated by analyzing the event logs, disturbance records, and fault reports registered by all devices that integrate the test system.

Network metrics will be validated using network analysis tools. The network analysis will be performed on data collected during network reconfiguration, during a pre-defined time period prior to the scenario trigger (pre-test conditions), and during a pre-defined time period after the system is stable once more (post-test conditions).

The test should be performed under different network conditions (e.g., no other network activity; non-time-critical network activity in some of the key IEDs; network congestion in other slices).

In pilot phase, if possible, the test should be performed in conjunction with the use cases from other verticals.

If possible, a benchmarking analysis will be performed by repeating the tests using 4G communications.

4.10.3 Relevant Standards

IEC 61850 (Communication networks and systems for power utility automation) [7][8][9][10][11][12][13], which is exhaustively referred throughout all the use case scenario definitions, is the most significant standard for the smart grid self-healing use case.

Although IEC 61850 will also be used for transmitting synchrophasor data in scenario 3, IEEE C37.118 (IEEE standard for synchrophasor) [14][15] is of great relevance for the differential protection scenario.

4.10.4 Relation to 5G-PPP KPIs

The smart grid self-healing use case will contribute to advancements in 5G-PPP KPIs by boosting the developments in 5G communications necessary for meeting the requirements defined for the proposed scenarios.

This use case is expected to impact on the performance KPIs listed below:

- *Providing 1000 times higher wireless area capacity and more varied service capabilities compared to 2010.*

Since the use case scenario will be implemented and validated in controlled laboratory environment, it will not possible to evaluate the impact it will have in this KPI. Nevertheless, high-availability and QoS/QoE over a wide geographical area is without a doubt one of the most relevant requirements for smart grid communications.

- *Saving up to 90% of energy per service provided.*

Although not one of the most critical requirements for this application, reduced power consumption is valued, particularly since many of the IEDs integrated in smart grid self-healing schemes are remote devices that must occasionally rely on battery power for considerable periods of time.

- *Creating a secure, reliable and dependable Internet with a “zero perceived” downtime for services provision.*

Availability is a highly critical aspect of smart grid protection and automation, particularly for self-healing applications. If such applications are communication-dependent, as is the case for the present use case scenario, this level of criticality is extended to the communication network. This KPI is particularly relevant for the presented applications since, in these cases, QoE prosumers are machine-based hard real-time systems.

- *End-to-End latency of < 1ms.*

The latency guaranteed by fourth generation wireless communications has not reached the optimal values for power system protection applications. The high-performance communication requirements presented by the smart grid self-healing use case should be able to lever additional advancements and to bring developments in this particular field closer to reaching this KPI.

This use case is expected to impact on the following societal and business KPIs:

- *European availability of a competitive industrial offer for 5G systems and technologies.*
- *Establishment and availability of 5G skills development curricula.*
- *Leverage effect of EU research and innovation funding in terms of private investment in R&D for 5G systems in the order of 5 to 10 times.*

4.10.5 Technical Innovation in the Field

This use case will attest to the existence of a public, affordable, wide-area communication network capable of meeting the demanding requirements imposed by mission-critical power grid applications. The existence of such a communication infrastructure is bound to bring forward the development of communication-based wide-area solutions in the energy sector. A wide range of applications that go beyond the high-speed self-healing or differential

protection solutions addressed by this use case will benefit from these technological advances and will surely take advantage of them to promote further innovative developments in the sector (e.g., innovations in islanding detection, volt-VAR control, enhanced fault location and power swing algorithms).

4.10.6 Business Impact in the Sector

One of the most important goals of the energy sector applications addressed by this use case is the improvement of the power supply QoS ensured by utilities. European power regulators are known to apply financial incentives and/or penalties based on the quality of the supplied power. Although QoS targets and incentive/ penalty schemes are implemented differently for each country, QoS metrics are often based on reliability indicators that account for the frequency and duration of power supply interruptions. The implementation of very-high-speed self-healing solutions aims at reducing the frequency and duration of outages, allowing electric power utilities to improve their reliability indicators, which has a direct financial impact.

SLICENET will provide a cost-effective, industry-ready, multi-tenant, ultra-reliable communication infrastructure that will enable the implementation of affordable high-end automated solutions for the power grid, such as the solutions covered by the smart grid self-healing use case.

Actual smart grid stakeholders' expectations in the context of the new 5G technology introduction were surveyed as described in Annex B.

4.10.7 End User Benefits

Two distinct groups of end users can be associated to the smart grid self-healing use case, each with their own set of benefits: electric power utilities, the end users of the 5G network, and the consumers, the end users of the smart grid.

As was referred in section 4.10.7, SLICENET in particular and 5G technologies in general will empower utilities with an affordable high-end communication infrastructure which will allow them to deploy automated solutions aimed at improving the reliability indexes and reducing the operational effort.

Consumers will indirectly gain from these advances in the Information and Communications Technology (ICT) sector by being granted increased QoS from the electric power providers.

5 eHealth Smart/ Connected Ambulance Use Case

5.1 General Background

The aim of this use case is to demonstrate how 5G technology can be leveraged to provide one-stop shop end-to-end services for offering enhanced Quality of Service and Quality of Experience for health scenarios. It will highlight the benefits and impact of the slice project by providing a basis for demonstrating easy provisioning of advanced network capability management features. It will do this by engaging with Health Service Administrators who are looking at how advanced technologies can play an enabling role in the transformation of the delivery of healthcare through the design of better-connected, integrated and coordinated services.

Communication capabilities that can deliver challenging performance requirements in 5G will be fundamental, as the Connected Ambulance will act as a connection hub (or mobile edge) for the emergency responders, enabling storing and potential real-time streaming of patient data to the team at the paramedic ambulance control centre and/or clinical emergency response team. It will do this by focusing on the smart transmission of ultrahigh definition video streams from emergency accidents scenes, through to the arrival of the patient to the emergency department. It will demonstrate how the 5G technology developed in SLICENET can cope with high definition video by offering enhanced mobile broadband (MBB) communication across domains, while coexisting with other SLICENET use case scenarios.

Currently with RedZinc's BlueEye wearable camera, latency of approximately above one second is observed at application level on Vodafone's LTE network in Dublin. Ideally the application delay would be of the order of 100ms based on suggestions of ITU¹¹ for conversational video. 5G is focused on low delays such as 10ms and this seems not necessary for conversational video. At this point, there is no evidence to suggest that tighter delay is required at the level of an interactive video application. Certainty better than 1000ms is required and closer to 100-200ms would be ideal

Uplink bandwidth capacity also limits image definition. Usually networks are dimensioned asymmetrically with capacity more allocated to the downlink for delivering content, whereas paramedic video requires mostly up link video the usual service mode is simplex video with duplex audio.

A variety of scenarios can benefit from SLICENET 5G technology. The hierarchy shown in Figure 17, listing possible situations, organised at high level into single patient or multi-patient incidents. Single patient events that could most benefit are ischemic [31] stroke and cardiac arrest. Ischemic stroke is caused by thrombotic or embolic occlusion of a cerebral artery. Rapid diagnosis by a proficient clinician using the NIH Stroke Scale (NIHSS) [31] is critical to effective treatment. The National Institutes of Health Stroke Scale, or NIH Stroke Scale (NIHSS) is a tool used by healthcare providers to objectively quantify the impairment caused by a stroke and cannot be administered by a paramedic. For a range of these strokes

¹¹ ITU-T Rec. G.1010 (11/2001) End-user multimedia QoS categories

it is crucial to administer thrombolytic therapy (clot busting drugs), which is a treatment to dissolve dangerous clots in blood vessels, improve blood flow, and prevent damage to tissues and organs. Therefore, a 5G assessment enabled by 5G ultra-high definition video could have a major impact on the effectiveness of this treatment. Telemetry from Mobile CT Scanner technology could also assist in assessment of stroke over 5G [33]. Cardiac arrest could benefit from 5G enabled drone technology, such as delivery of AEDs to remote patients [33][34].

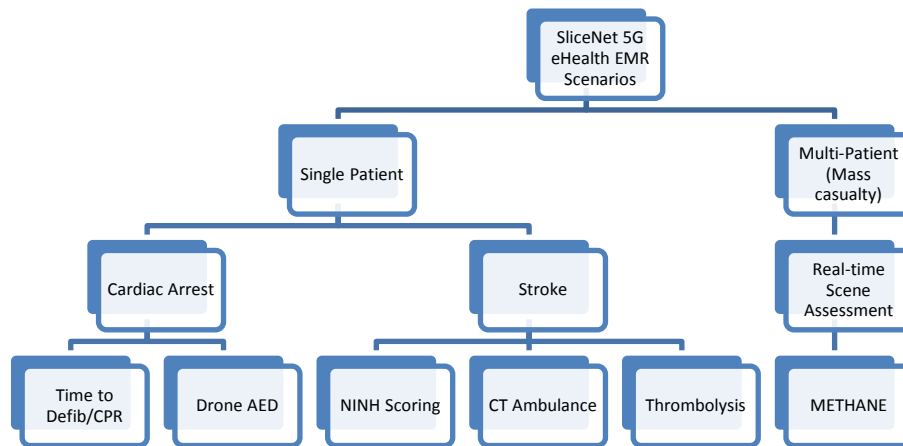


Figure 17 Scenarios likely to benefit from 5G SLICENET technology

For multi-patient scenarios 5G could add significant benefit by providing real-time scene assessment using the METHANE [36] protocol, which is used by emergency services to report major incidents. METHANE stands for:

1. Major Incident Declared,
2. Exact location,
3. Type of incident,
4. Hazards,
5. Access,
6. Number and type of casualties, and
7. Emergency services present and required.

A mast or drone mounted 5G camera deployed from a connected ambulance could provide emergency services controllers with a valuable platform for real-time METHANE driven assessment.

Drone or camera mounted devices provide for both physical and virtual sensors and actuators:

1. Physical Sensors: charge coupled device/ infrared, drone GPS, altitude.
2. Physical actuators: zoom, pan, flight path.
3. Virtual Sensors: scene patient analysis.
4. Virtual actuators: frame boosting.

The easy provision and configuration of the ultra-reliable low latency communication video use case will also be demonstrated, where digital service customers such as emergency medicine organisations, can requisition appropriate 5G services, see Figure 18.

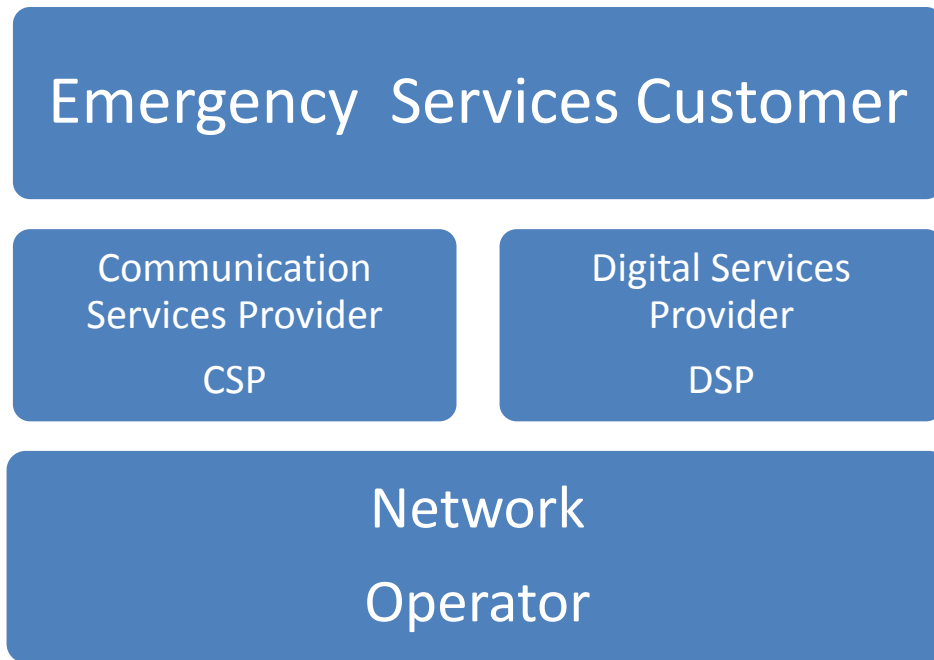


Figure 18 High-level model of SLICENET roles

5.2 Use Case Scenario: Ultra-High Definition Video and IoT for Connected Ambulance

5.2.1 Overview

5.2.1.1 Storyline

The scenario for the ultrahigh definition video health scenario begins with the continuous collection and streaming of patient data, when the emergency ambulance paramedics arrive at the incident scene, see Figure 19.

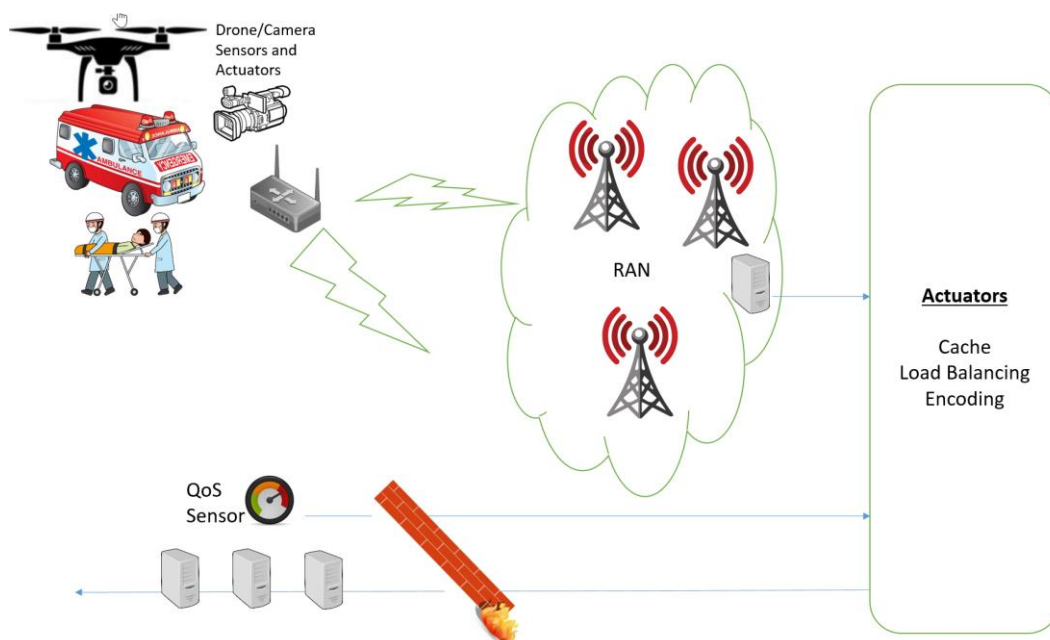


Figure 19 SLICENET overview of use case scenario

Wearables/mounted/drone cameras will enable the provision of enhanced patient insights and the goal is for all paramedics to have wearable clothing that can provide real-time video feeds as well as other sensor related data pertaining to the immediate environment.

The availability of patient related real-time video stream to the awaiting emergency department will enable more intelligent decision support for the paramedics attending the patient.

Real-time streaming video will enable paramedic professionals to remotely monitor the patient for conditions that are not easily sensed such as skin pallor and patient demeanour.

In a more ambitious scenario, life-saving remote assistance might be required on the ambulance, supervised by a specialist located elsewhere and connected to the same platform. Ischemic stroke diagnosis by a proficient clinician using the NIH Stroke Scale (NIHSS) [31] will support effective treatment.

Connected Ambulance will act as a connection hub (or mobile edge), using IoT edge gateways such as the Dell Gateway series, for the emergency medical equipment and wearables, enabling storing and potential real-time streaming of patient data to the awaiting emergency department team at the destination hospital.

Security and privacy of eHealth data is paramount, so with that in mind, a robust security management for 5G slice services over multiple virtualised domains shall be provided.

In this use case scenario emergency service providers will act as the digital services customer. They will specify the particulars of the service needs for their use cases. For example, a may wish to provision a fleet of 10 ambulances in a particular geographic location that will require ultra-high-definition video to be delivered using ultra reliable low latency communication across a network. In another scenario, the may wish to configure five ambulances provide ultrahigh definition video conjunction with deployable drones for METHANE scene assessment. In each of these cases they will specify the particular requirements to the slice net communications service provider and digital service provider of the SLICENET one-stop shop application programming interface (API), via an easy to use online 5G services configuration tool.

The proposed use case scenario, shown in Figure 20 will also introduce a set of virtualised SLICENET sensors and actuators to meet the requirements of the situation. Cognitive network management tools will be provided by slice net to detect and resolve 5G network issues in order to maintain high definition video quality of service.

RedZinc is providing BlueEye as an application to the SLICENET project. The BlueEye system has been developed in the LiveCity smart cities PSP project and in the H2020 Q4Health, see Figure 20.

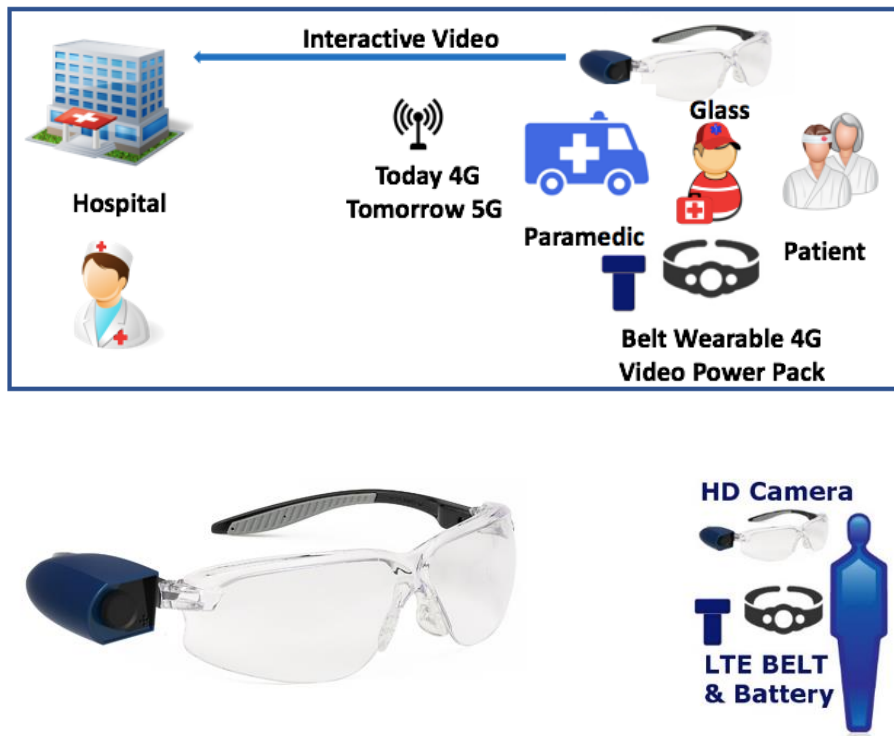


Figure 20 RedZinc BluEye system

5.2.1.2 Relation to 5G Requirements and Visions

These events will require high-resolution video capabilities, e.g., the remote assistance will require ultra-high-definition video streaming from the ambulance to the remote site where the specialist is located.

SDN/NFV functionality for video caching, load balancing and traffic offloading should be utilised to maintain QoE.

Videos shall be encoded in a suitable new and emerging video coding format that has the highest impact on an end user’s perceived visual quality or Quality of Experience (QoE). It should support U-HDTV, which is one of the “5G Priorities & Drivers” [38], by exploiting video codecs such as H.264. Emphasis will be placed on adaptive video codecs especially the capabilities of H.264. This will provide adaptive video streaming which will allow slice actuators to respond to varying conditions, in order to maintain quality of service. SLICENET will also support rapid deployment of video digital services and will accelerate provisioning time and support a number of viable concurrent video traffic flows to improve the patient/clinician experience.

The objective is to maintain or optimise the perceived quality of the slice-based/enabled services for the service users through cognition-based self-optimisation and self-configuration capabilities.

The cognitive, agile QoE management will maximise the application-level quality for the service users at given resource constraints/budgets and Service Level Agreements (SLAs), e.g., perceived video quality for the 5G Ambulance.

To secure the committed SLA whilst maximising the global resource efficiency, SLICENET will employ a cognition-based approach to dynamically maintain/optimize the QoE of a slice

service even in adverse QoS conditions.

A set of novel QoE sensors and actuators will be required to dynamically optimise slice operation, driven by maintaining or improving QoE in real time.

Congestion at the RAN and the core layer should be detected non-essential video frames should be dropped.

SDN/NFV functionality for video caching, load balancing and traffic offloading should be utilised to maintain QoE.

Fault management will detect and resolve slices' operational problems, and minimise the downtime of slice operations. Configuration management will coordinate changes in the operation of slices, and manage dynamic slice configuration and reconfiguration.

Accounting management will optimise the resource distribution for slices and provide the billing service for slice users.

Performance management will assure the overall performance (especially scalability) of the whole system running numerous slices, in collaboration with the QoE management for individual slices.

Security management will secure the use of slice-based/enabled services for users, protecting the system against cyber-attacks, and providing authentication and authorisation for these services.

Edge computing should be used at the edge to analyse and adapt video stream to focus on patient well-being.

The ambulance 3000 series Edge gateway will act as a connection hub for the emergency medical equipment and wearables, enabling storing and potential real-time streaming of patient data to the awaiting emergency department team at the destination hospital

Enable trustworthy interoperability across multiple virtualised operational domains.

Provide management of multi-domain virtualised networks with coverage of security architectures.

Provide 5G slicing system and services security for eHealth.

5.2.1.3 Goals

This enhanced and interactive communication between the medical professional teams and the remote paramedics attending to the patient will lead to fundamental improvements in emergency medical care and improve the probability of better patient outcomes. CIT Infinite and Dell EMC plan to develop a demonstrator for this 5G eHealth Connected Ambulance use case in Ireland within this project.

The main goals are:

- Provide a connection hub (or mobile edge) for the emergency medical equipment and wearables, enabling storing and potential real-time streaming of patient data via ambulance/wearable/drone mounted camera to the awaiting emergency department team at the destination hospital.
- Maintain QoS and QoE by using adaptive MEC to analyse and filter video and IoT device feed, through cognition-based capabilities, beyond the conventional QoS

management that focuses on low-level, mainly network-level metrics such as bandwidth and delay.

- Detect and resolve eHealth slices’ operational problems, and minimise the downtime of slice operations to provide QoE for eHealth
- Optimise the resource distribution for slices and provide the billing service for eHealth slice users.
- Assure the overall performance (especially scalability) of the whole system running numerous slices, in collaboration with the QoE management for individual slices.
- Secure the use of 5G /enabled services for users, protecting the system against cyber-attacks, and providing authentication and authorisation for these services.
- Provide pertinent clinical information related to patient well-being and demeanour.
- Provide management of multi-domain and multi-tenant virtualised networks with coverage of security architectures.
- Provide one-stop portal that leverages SLICENET API to provide ultrahigh definition video to provide ultra-reliable low latency communication services digital services customers such as ambulance services.
- Provision of a Public Safety Slice (supporting first responders fire, police ambulance) using the same platform.
- Provide image processing value added functions in the UE supported, by where necessary, MEC servers, with low latency connection to the UE.
- Provide video storage functions in in the Slice (for evidence, archive and training)
- Provide value added functions such as ECG from peripheral devices into the hospital application environment.

The system will be developed in an agile and incremental fashion, with a first early pilot demonstrator in Cork, see Figure 21.

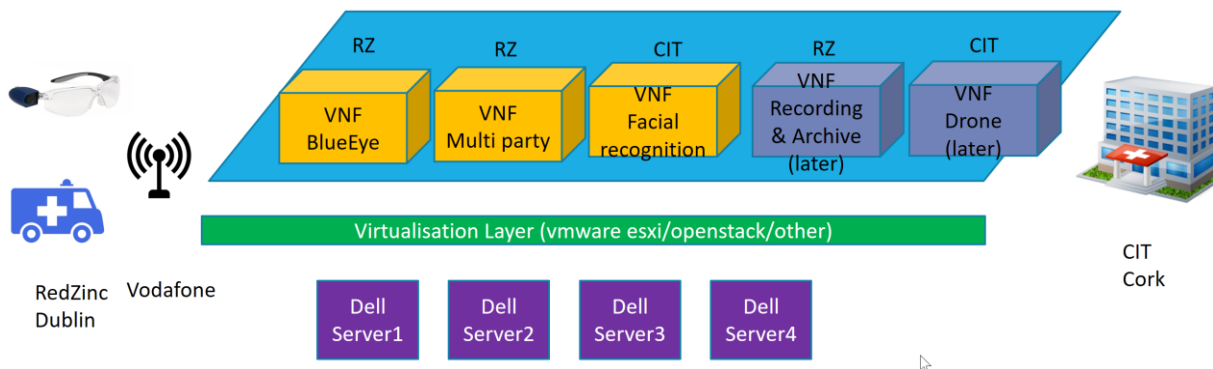


Figure 21 This is a suggested initial slice to be built by RedZinc/CIT/DELL EMC

5.2.1.4 Actors

SLICENET Components

The slice is the set of cloud and networking resources on top of which multiple video services are operated and dynamically instantiated. It will include MEC components to analyses and process video streams.

1. Paramedic
2. Patient
3. Physician

4. Controller
5. Hospital/Ambulance/Health service management - Digital service customer, i.e. the slice owner and ultimate consumer

The slice could be deployed over network operator(s) infrastructure(s), or even on top of an MVNO.

5.2.1.5 General Assumptions

1. Videos based on H.264 encoding standard
2. BlueEye
 1. LTE FDD Category 4 1080p @ 30 fps
 2. Maximum up/download speed is 50/150 Mbps
 3. Supports 802.11a/b/g/n.
 4. Recommended video bitrates for Standard DR uploads: 1080p: 8 Mbps
 5. Recommended video bitrates for High DR uploads: 1080p: 10Mbps
 6. Bitrates required for H.264 video encoding is 5.12 Mbps (4992 kbps for video + 128 kbps for Audio).
 7. <https://support.google.com/youtube/answer/1722171?hl=en>
 8. <http://www.lighterra.com/papers/videoencodingh264/>
3. System should also support RealSense camera hardware to facilitate patient demeanour detection. The RealSense camera provides and API to support facial landmark feature detection:
 1. <https://us.creative.com/p/web-cameras/creative-senz3d>
 2. RGB video resolution, HD 720p (1280x720)
 3. IR depth resolution
 4. QVGA (320x240)
 5. Frame rate up to 30 fps
 6. FOV (Field-of-View) 74°
 7. Range 0.5ft ~ 3.25ft
 8. Size 4.27" x 2.03" x 2.11"
 9. Weight 271g
4. Cameras with the High definition cameras should be considered, with the following video specifications:<https://www.qualcomm.com/news/onq/2017/02/27/powered-snapdragon-835-sony-xperia-xz-premium-reaches-gigabit-speeds>.
5. Drone mounted camera:
 1. UHD: 4096 x 2160 (24/25p) and 3840 x 2160 (24/25/30p) max video bitrate of 60 Mbps
6. Holo cameras such as Microsoft HoloLens could also be interesting to evaluate as they could potentially immerse the remote doctor in a 3 dimensional world. HoloLens provides an interesting 3D image but the sensing technology to render a real scenario (as opposed to computer generated one) may still be several years away.
7. The system can also provide IoT gateway connectivity via Dell Edge Gateway series, <http://www.dell.com/ie/business/p/edge-gateway>.

5.2.1.6 SLICENET QoS Sensors

1. Video Sensor, IoT and a QoS Sensors (CLI speedtest or iperf or ditg are useful for this) are required

2. Collect video specific and flow level metadata and metrics.
3. In terms of latency, jitter and packet loss rate, Cisco TelePresence could be a reference point:
4. 30ms to 100ms latency end to end.
5. 10 ms peak-to-peak jitter
6. 0.03 to 0.05% random packet loss

5.2.1.7 SLICENET QoE Actuators

1. Discard frames in response to congested network.
2. Switch domains in response to network load.
3. Drone remote control
4. Camera panning, zooming, focus, aperture

5.2.1.8 External Systems

1. RealSense Camera
2. Dell Gateway
3. BlueEye
4. Drone
5. Video codecs

5.2.2 Detailed Steps

5.2.2.1 Preconditions

The emergency communication and the transmission of the real-time video of an emergency situation will be sent to a response team using a SLICENET capable device.

SLICENET functions are initiated in response to network availability, network congestion.

Sensors detect or predict the following events:

- QoS of video stream drops.
- Network congestion
- Decreasing bandwidth at radio access network.

5.2.2.2 Metrics

International Telecommunication Union Telecommunication Standardization Sector ITU-T P.10/G.100 defines the QoE as “level of user’s acceptance towards application and services is referred as QoE”.

European Network on QoE in Multimedia Systems and Services. Qualinet defines QoE “level of end user’s delight towards services. While services are directly dependent on network, devices and context based facilities provided by core network (service vender)”

QoS is analyzed on technical measures like peak data rate, spectral efficiency, packet loss, delay, jitter and other parameters which can present the negative or positive QoS.

Edge detection at scene - patient demeanour, stroke facial symptoms, see Figure 22.

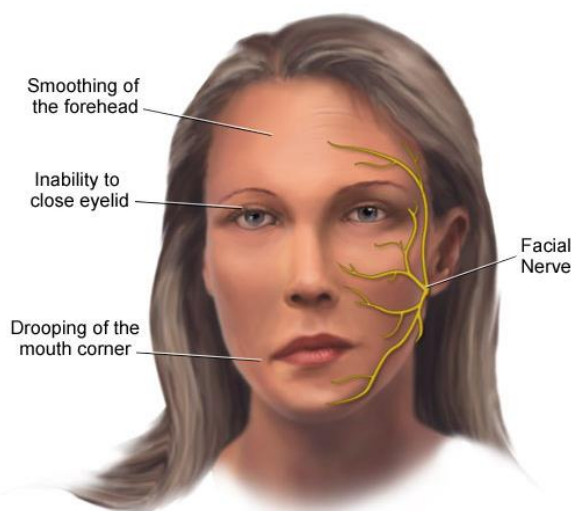


Figure 22 Stroke facial symptoms

5.2.2.3 Trigger

1. Request for Ultra-Hi-definition video slice at emergency.
2. Drop on QoE and QoS.
3. Network congestion event predicted/detected.
 - Edge processing detects change in patient demeanor.

5.2.2.4 Post Conditions

- Network congestion resolved
- Video service QoE level maintained.

5.2.2.5 Workflow

User Scenario:

- Paramedic initiates an Emergency Services session to establish an ultra hi-definition video stream to provide assistance an emergency scene and starts streaming real-time video to as part of the original communication session using his Emergency Services capable device, via BlueEye or a 5G capable gateway such as Dell Edge Gateway 3000 series model to ER and/or command and control centre. Each ambulance may provide multiple video sources, e.g., medic body cams, vehicle mounted camera.
- Video is streamed real-time along with voice communication with the ER/control centre via the SLICENET system.
- SLICENET provides Ultra-HiDef Video slice
- SLICENET will also provide high quality full duplex voice services between the paramedics and hospital based clinician.
- SLICENET monitors QoE and QoS and provides cognitive network management to maintain quality levels
- Video slice co-exists with other slices such as voice and IoT traffic.
- Additional ambulances may be dynamically added to existing slice at any point during the slice's lifecycle

The typical life-cycle of an ultra-high definition video slice session is shown in Figure 23.

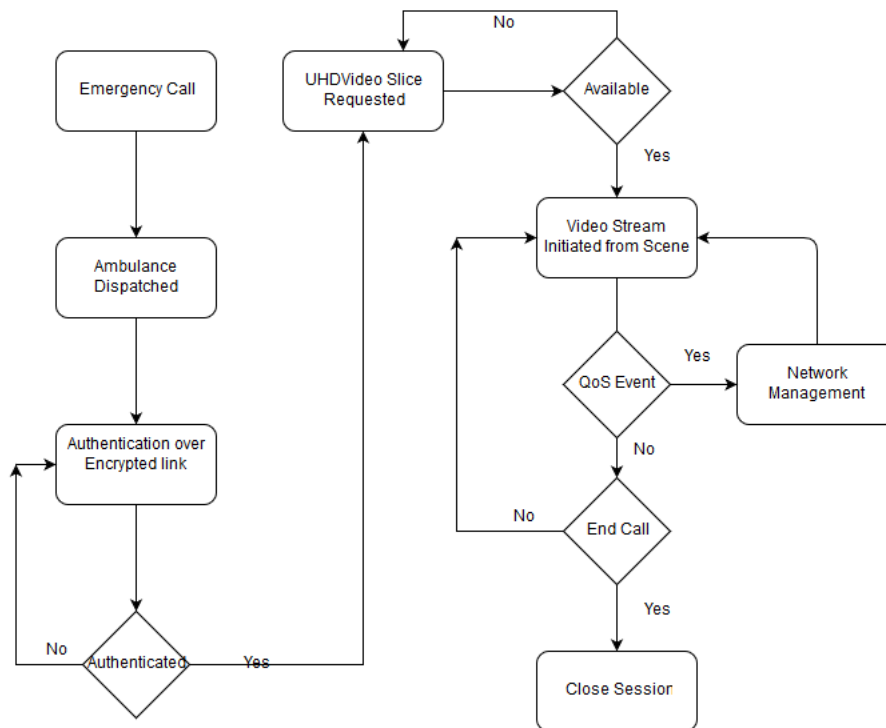


Figure 23 UHD Video flow in SLICENET

We envisage that ambulance/health service providers will request a UHDVideo slices for each ambulance video gateway unit. I think of this as requesting a “hand set” from a mobile telecom, where you can specify QoS needed for the “video stream hand set(s)”. The ambulance gateway will have the SIM card and the slice capability is assigned to that sim card 5G unique number. The business model could be a premium subscription where certain “UHDVideo slices” are made available to that unit for a certain number of minutes per month.

A digital service provider (DSP) such as RedZinc or CIT-Infinite will engage with digital service customers such as ambulance and health services to provide ultra-high definition video slices suitable for their needs, built on slice offerings from network operators, see Figure 24.

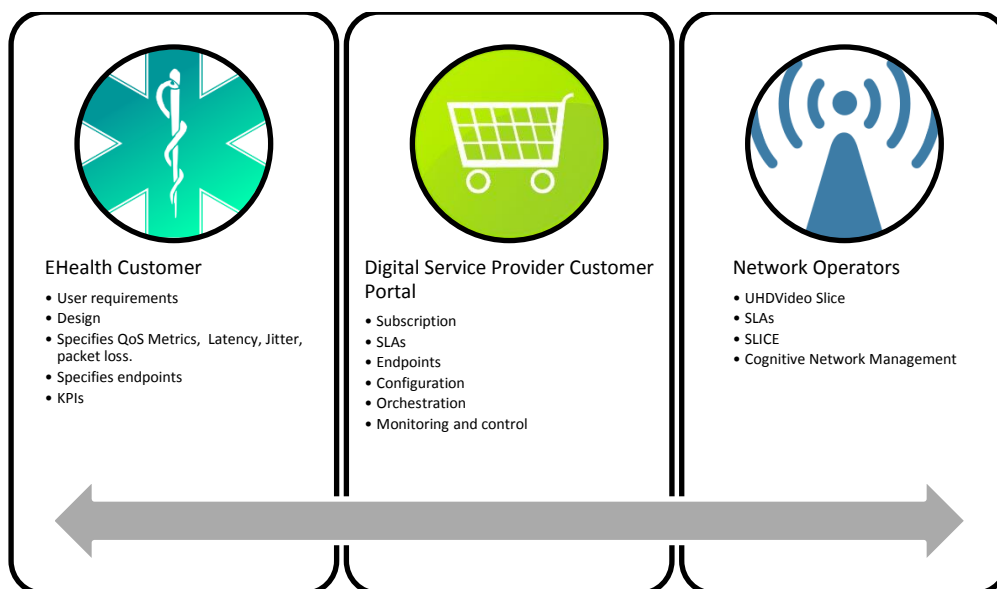


Figure 24 End to end Provisioning

5.2.3 Technical Requirements

The technical requirements described in this section are further detailed in Annex A.

5.2.3.1 Requirements on Cognition (Intelligence)

Maintain the perceived quality of the slice-based/enabled services for the service users through cognition-based self-optimisation and self-configuration capabilities.

The cognitive, agile QoE management should maximise the application-level quality for the service users at given resource constraints/budgets and Service Level Agreements (SLAs), e.g., perceived video quality for the 5G Ambulance.

Cognitive Network Management to facilitate self-adaption - the adjustment of behaviour in response to the perception of the environment and the data that has already been processed. Adaptively select different functionalities by using different software components.

A complete cognition-driven, intelligence-enabled control loop shall be provided, including QoE sensing, QoE monitoring, QoE analytics, QoE optimisation decision-making, and QoE actions, to achieve this QoE-oriented operation.

A cross-plane orchestrator will be driven by the QoE optimisation intelligence and deploy the selected QoE actuators (VNFs) to enforce the optimisation intelligence at the right time in the right place to optimise the performance of any of the infrastructure layers or the management, control and data planes in the framework.

Resource cognitive engine achieves the required ultra-low latency and ultra-high reliability of the system by using a software defined network (SDN) to cognize the resources in the network.

Autonomic software-defined networks, instantiating new virtual resources based on the existing network knowledge to further enhance network, proactively managing the network based on anticipated future events.

Autonomic diagnosis/anticipation, predictive tools are used to align the network history profile with the current network trends.

Cognitive medical intelligence shall be provided at the edge: video stream is analysed in real-time for detecting patient demeanour.

5.2.3.2 Requirements on the One-Stop API

A novel mySlice subsystem in the SLICENET framework shall be provided to offer a 'one-stop shop' solution to the diverging service requests from diverse vertical businesses.

The one-stop shop solution enabled by mySlice shall facilitate the smooth and efficient migration for ambulance services providers to adopt 5G slices for enhancing emergency response, by providing drop-in-style onboarding, prompt slicing provisioning, flexible and efficient control and management.

It shall provide customisable plug & play control, aligned with and to be integrated with end-to-end slicing, QoE-oriented slice management, and service orchestration subsystems.

E2E slicing (slice provisioning) shall be provided and slice services creation by establishing slicing/slice-friendly, integrated 5G MEC infrastructure and efficient operations of the

control and management planes, which are further optimised through the proposed cross-plane coordination and service orchestration for autonomic slice service deployment.

Slice instantiation must take into account the geographical locations of the involved resources (e.g. ambulance position and supporting staff location) to optimize the allocation of the physical resources to meet QoS requirements.

5.2.3.3 Requirements on Slicing/Slice

Slice instantiation must complete within a pre-defined timeframe to ensure critical support can be provided to patients.

Standard H.264 that allows a layered encoding of video, as well as HD and UHD resolutions.

Codecs that allow layered encoding to facilitate layer-specific packets to be dropped, reducing video quality, whilst preserving the video service continuity.

Allows the video stream to be manipulated in such a way that the QoE is maintained for the end user without the need to use an expensive operation such as transcoding.

Differentiate urgent video streams such as telemedicine from normal streams like a regular video call.

If the RAN is congested, some nonessential layers of the video can be dropped, hence consuming less resources, allowing the QoE to be maintained.

If the core network is congested, caches should be deployed on the network, reducing the pressure on the congested links by serving the most common streams from a cache placed as close to the end user as possible.

5.2.3.4 Requirements on Multi-domain Operations

Medical emergencies can occur anywhere over a wide geographical area. Also, emergencies can occur in areas where there is poor coverage. Therefore, access to slicing across multiple administrative domains is necessary. Control and management plane enablers (including extensions to existing single-domain schemes) for slicing request initialisation, intra- and inter-domain as well as cross-plane slicing negotiation and on-demand renegotiation etc., enablers for multi-operator, multi-provider and multi-domain resource sharing and access, and enablers for dynamic multi-domain slicing routing and roaming should be considered.

Security is always a top concern for eHealth, especially in the challenging multiple operator domains environment. SLICENET shall mitigate this security concern for 5G operators and users by focusing on providing robust security management for 5G slice services over multiple virtualised domains as part of the FCAPS slice management.

5.2.3.5 Requirements on RAN

The system shall have low latency and high reliability.

It shall dynamically perceive resource consumption, signal interference, energy consumption and workload in the base station, to allocate the wireless sources elastically and maximize the capacity and efficiency. Predict and traffic requirements, and to allocate appropriate wireless resources for users in advance.

Efficiently use the radio and energy resources.

Ultra-high reliability & Ultra-low latency

- 30ms to 100ms latency end to end.
- 10 ms peak-to-peak jitter
- 0.03 to 0.05% random packet loss

5.2.3.6 Requirements on MEC

The SLICENET architecture will integrate E2E network segments with MEC explored to support the envisioned large-scale, multi-domain networking environment.

The system shall host compute-intensive applications at the network edge, such as the extraction of facial features for detection of strokes or other critical conditions.

The system shall perform pre-processing of large data before sending it (or some extracted features). Functions that perform a resolution conversion of live video streams to reduce network load (e.g. non-monitored video feeds may be transmitted with a lower resolution)

Utilise context aware services with the help of RAN information such as cell load, user location, and allocated bandwidth.

5.2.3.7 Requirements on Core

The system shall securely provision reliable multi-tenant slice high band width slice.

5.2.3.8 Requirements on Enterprise Network

All communications should be compliant with GDPR. It is envisaged that ultra high-definition video streams captured on BlueEye and other video devices will be made available by a cloud-based end user client, which will be accessed securely through the hospital enterprise network file, see Figure 25.

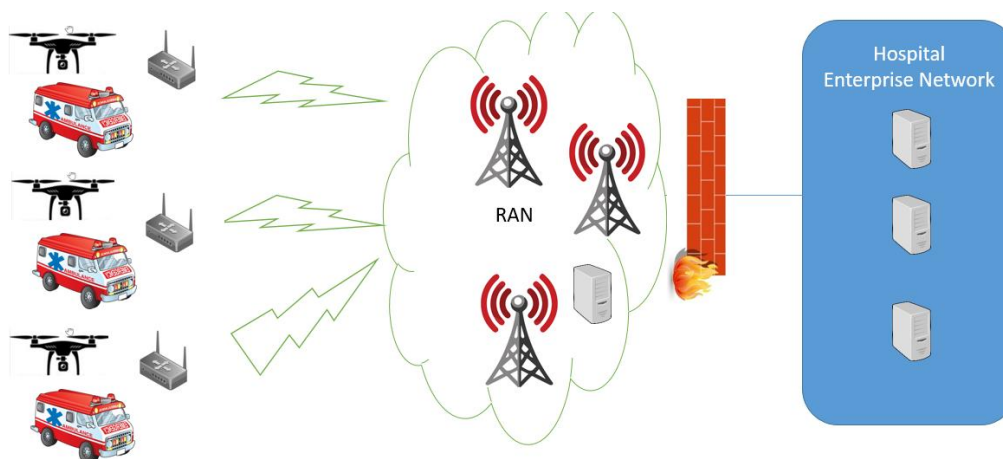


Figure 25 Relation to hospital enterprise network

5.2.3.9 Non-functional Requirements

Low latency service delivery is available at the data plane with sufficient available bandwidth to maintain minimal video quality.

5.2.3.10 Legal, Policy and Regulation Requirements

The **General Data Protection Regulation (GDPR)** (Regulation (EU) 2016/679) is a regulation by which the European Parliament, the Council of the European Union and the European Commission intend to strengthen and unify data protection for all individuals within the European Union (EU).

Recommended Steps:

1. Awareness

You should make sure that decision makers and key people in your organization are aware that the law is changing to the GDPR. They need to appreciate the impact this is likely to have.

2. Information you hold

You should document what personal data you hold, where it came from and who you share it with. You may need to organize an information audit.

3. Communicating privacy information

You should review your current privacy notices and put a plan in place for making any necessary changes in time for GDPR implementation.

4. Individuals' rights

You should check your procedures to ensure they cover all the rights individuals have, including how you would delete personal data or provide data electronically and in a commonly used format.

5. Subject access requests

You should update your procedures and plan how you will handle requests within the new timescales and provide any additional information.

6. Lawful basis for processing personal data

You should identify the lawful basis for your processing activity in the GDPR, document it and update your privacy notice to explain it.

7. Consent

You should review how you seek, record and manage consent and whether you need to make any changes. Refresh existing consents now if they don't meet the GDPR standard.

8. Children

You should start thinking now about whether you need to put systems in place to verify individuals' ages and to obtain parental or guardian consent for any data processing activity.

9. Data breaches

You should make sure you have the right procedures in place to detect, report and investigate a personal data breach.

10. Data protection by design and data protection impact assessments

You should familiarize yourself now with the practice on Privacy Impact Assessments and work out how and when to implement them in your organization.

11. Data protection officers

You should designate someone to take responsibility for data protection compliance and assess where this role will sit within your organization's structure and governance arrangements. You should consider whether you are required to formally designate a Data Protection Officer.

12. International

If your organization operates in more than one EU member state (ie you carry out cross-border processing), you should determine your lead data protection supervisory authority.

5.2.3.11 Coverage of Service Life-cycle Phases

Maintain ultra-high definition video QoE.

One stop shop E2E service creation and deployment, where the lifecycle is managed by the SLICENET framework.

Phase 1 [Service request / SLA negotiation]: Commissioned through One-Stop API

Phase 2 [Planning / Design]: Plan for single/multipatient scenarios, QoS, QoE KPIs

Phase 3 [Deployment]: Deployment and configuration of edge software.

Phase 4 [Operation and Monitoring]: Dashboard for digital services customer

Phase 5 [Billing]: Monthly subscription and/or per number of devices basis

Phase 6 [Decommissioning]: At end of subscription or on customer's request.

5.2.4 Implementation, Evaluation and Impact

5.2.4.1 Prototyping/Testbed

Prototyping shall be carried out in a IoT mobile edge Dell Gate way 3000 series vehicle in a TRL 3-4 scenario.

5.2.4.2 Benchmarking and Validation

The proposed use case scenario will be implemented, tested, validated and evaluated in the CIT Infinite TRL 3 local testbed.

It will then be evaluated in pilot phase to demonstrate co-existence with other energy and smart grid use case scenarios.

Video optimization and streaming will be compared with current state-of-the-art.

5.2.4.3 Relevant Standards

Codecs that allow layered encoding to facilitate layer-specific packets to be dropped, reducing video quality, whilst preserving the video service continuity.

5.2.4.4 Relation to 5G-PPP KPIs

This use case is expected to contribute to the following performance KPIs:

- Providing an order of magnitude times higher wireless area capacity and more varied service capabilities compared to 2016.
- Reducing the average service creation time cycle from many hours to just minutes.
- Creating a secure, reliable and dependable video stream along with IoT medical device data with a “zero perceived” downtime for services provision.
- Enabling advanced user controlled privacy.
- To improve the speed of video delivery, aim for the ultra-low latency envisioned in 5G (sub-1ms latency Performance KPI within 1 Km).

This use case is expected to contribute to the following societal KPIs:

1. Enabling advanced User controlled privacy;
2. European availability of a competitive industrial offer for 5G systems and technologies;
3. Stimulation of new economically-viable services of U-HDTV to provide high societal value in terms of emergence medical care;
4. Establishment and availability of 5G skills development curricula (in partnership with the EIT).

This use case is expected to contribute to the following business KPIs:

- Leverage effect of EU research and innovation funding in terms of private investment in R&D for 5G systems in the order of 5 to 10 times;
- Target SME such as RedZinc participation under this initiative;
- Reach a global market share for 5G equipment & services delivered by European headquartered ICT companies at, or above, the reported 2011 level of 43% global market share in communication infrastructure.

5.2.4.5 Technical Innovation in the Field

SLICENET will enable U-HDTV applications for emergency medical care.

SLICENET will provide innovation in the control plane of 5G networks to equip eHealth stakeholders with plug & play programmable control plane functionality so that they are enabled to provide their own customised control of the data plane to fulfil their use cases' requirements.

5.2.4.6 Business Impact in the Sector

The global eHealth market is forecast to grow from 7.6 to 17.6 billion Euros by 2017. 5G technology can play an enabling role in the transformation of the delivery of healthcare through the design of better-connected, integrated and coordinated services. The 5G “Connected Ambulance” concept, will advance the emergency ambulance services through the development of telemedicine supporting technology to help create improved experiences and outcomes for patients in their care. The remote assistance will require ultra-high-definition video streaming from the ambulance to the remote site where the specialist is located. This enhanced and interactive communication between the medical professional teams and the remote paramedics attending to the patient will lead to

fundamental improvements in emergency medical care and improve the probability of better patient outcomes.

Actual eHealth stakeholders expectations in the context of the new 5G technology introduction were surveyed as described in Annex B.

5.2.4.7 End User Benefits

Network slices will maximize the sharing of network resources within and across domains, thereby substantially reducing the capital expenditure (CAPEX) for 5G network operators.

Network slicing allows a high-degree of flexibility of creating dedicated logical networks with eHealth specific functions and thus can meet diverse eHealth requirements.

Network slices can will upgrade operational capabilities as with intelligent slicing and slice lifecycle management it is possible to offer configurable warranties in Quality of Service (QoS) and/or Quality of Experience (QoE).

Reliable remote mobile life assistance could become a reality where an Ultra-High-Definition (e.g., 4K) video stream can be transmitted with the warranted ultra-low-latency and mobile broad bandwidth. Therefore, if the full potential is achieved, 5G slicing could be considered as one of the most important innovations in the communications of the decade due to its impact at worldwide level.

6 Smart City Use Case

6.1 General Background

Smart City is an important worldwide initiative, and in EU only the annual smart city benefits from 5G is estimated to reach 8.1 billion Euros in 2025 [EU-5G].

Over the last decade, the evolution of information technologies and communications networks, sensors, actuators, cloud infrastructure, big data and products/services based on these enablers has changed the way people live in a city. Access to information, services and communication is now provided anywhere and anytime by smartphones and modern people have adapted to this new way of living. Meanwhile, various actors that create “smart city technologies” are trying to convince the governments and the public administrations that these technologies can help cities improve the efficiency, availability, quality and cost of providing city services. At the same time, governments make transition to online services, but they must ensure that no one is left behind, not even those without access to this technology.

In this use case, we will observe how Alba Iulia, a small to middle size city in Romania with about 70k inhabitants, is moving forwards as a smart city by adopting the latest ICT technologies including LoRaWAN, LTE-M and finally 5G enablers. For the smart city use cases Orange proposes an open data strategy and open architecture that give access to further development of new applications by monetizing datasets from the city itself. The high-level architecture is constructed on three levels: data collection and transport layer, open IoT middleware layer and application layer. The data collection and transport layer will provide LoRaWAN, LTE-M and 5G specific connectivity for all sensors, actuators and consequently raw datasets that will be generated from the smart city solutions. These datasets will be sent to the open middleware platform to be stored, processed and secured. The open middleware can work also with other datasets that are not real time accessible through sensors or actuators. For example, we can consider the 1k datasets available on the Romanian Government Open Data Portal [DATA.GOV.RO], the 11k datasets available on the EU Open Data Portal [EUODP] or the 197k datasets available on the US Government’s data portal [US DATA.GOV]. There is the possibility that middleware becomes available to trusted applications developers using REST APIs, creating the opportunity of building a dedicated market place for the smart city ecosystem.

6.2 Use Case Scenario: Smart Lighting (SmaLi-5G)

6.2.1 Overview

6.2.1.1 Storyline

Alba Iulia has been selected by Orange to demonstrate the capabilities of the targeted smart city high level architecture in dealing with critical smart lighting infrastructure under the SmaLi-5G SLICENET use case. In case of Alba Iulia, we plan to build a live testing infrastructure of at least 100 smart controllers (actuators) that will be deployed on the main roads of the city. This will help the authorities understand the aggregated benefits of the solution and compare the them with the status quo.

The SmaLi-5G use case will facilitate three key functionalities that are impossible or hard to be efficiently provided today over legacy city lighting infrastructure and even modern lighting infrastructure, regardless the development of modern Low Power Wide Area Networking (LoRaWAN) technology or cellular IoT technologies (LTE-M, NB-IoT):

1. According to this use case, the responsible entity will be able to remotely control in real time and in a secure way every single lighting pole from the target network, in order to adjust the lighting intensity and efficiently manage energy consumption. The system will give public lighting distribution company reporting to the city manager, the ability to automatize the control of the lights, including the on/off and diming capability according to certain policies (e.g. day time moment, natural light intensity, location, traffic). This system, combined with the adoption of more efficient LED based ballast lamps, is anticipated to generate a reduction of energy costs for up to 80%, and a return of investment in just four - five years. According to a report [Philips Lighting and World Council of City Data], only about 10% of the 300 million street lights poles in the world are using energy-efficient LEDs, and just 2% are connected thanks to legacy communication technologies such as PLC and 2G/3G.
2. Moreover, the system will allow real time and history based energy consumption measuring. The city of Los Angeles [Philips Lighting and World Council of City Data] made energy savings of 63% in 2016 just by switching to 100% LED street lighting, generating cost savings of USD 9m and reducing its annual greenhouse gas emissions associated with public lighting by 47,000 metric tons. This is equivalent to the greenhouse gas emissions from almost 10,000 passenger vehicles driven for one year.

The entity responsible with the streets lighting infrastructure operation and maintenance will be able to proactively spot the malfunctions, energy loss or energy theft tentative on the public lighting network, as the system will generate intervention ticket in real time per pole or branch of poles. This capability will highly improve the city lighting service availability and will decrease the operational costs with maintenance activities. There is an international standard [ISO 37120] that specifies a set of indicators meant to define and measure the performance of quality of life and city services. This is applicable to any city or municipality that targets to measure its performance in a comparable and verifiable manner, irrespective of size and location. Street lighting can consume between 15 – 50% of public electricity [ISO 37120]. Electricity consumption of public street lighting is calculated as the total electricity consumption of public street lighting (numerator) divided by the total distance of streets where street lights are present (denominator). The result shall be expressed as kWh per kilometer per year.

Therefore, increasing the street lighting's efficiency is one of the most relevant and cost-effective steps that a municipality can consider to improve energy efficiency. Increasing the efficiency and quality of public street lighting generate multiple co-benefits including improved citizen perception of public safety and reduced crime rates, reduced maintenance costs, improved street and traffic safety, enhanced city attractiveness and community identity, improved air quality, and increasing economic productivity by extending business hours in commercial areas. According to [Philips Lighting and World Council of City Data] Los Angeles administration highlighted a 10.5% drop in crime rates regarding vehicle theft, burglary and vandalism in the first 2 years of its LED conversion program.

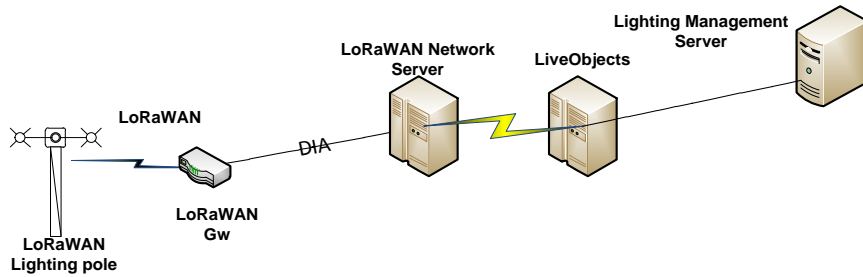


Figure 26 Smart Lighting LoRaWAN based architecture

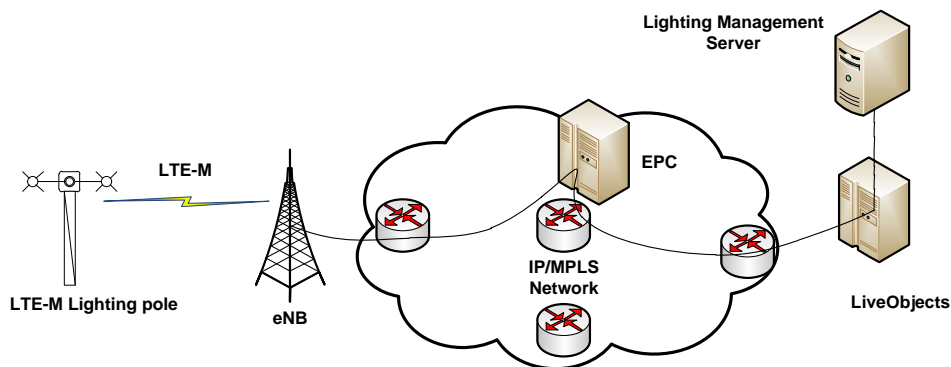


Figure 27 Smart Lighting LTE-M based architecture

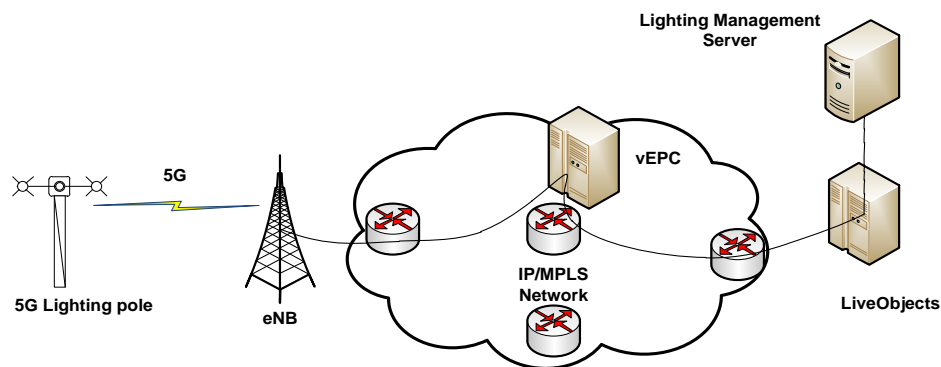


Figure 28 Smart Lighting 5G based architecture

The SmaLi-5G use case to be demonstrated in Alba Iulia pilot will consider the following high-level building blocks:

- The network of connected actuators/controllers that will be deployed one per each public lighting pole and poles aggregation node from the selected area;
- The competing connectivity networks that will include: LoRaWAN, LTE-M and 5G technologies, each with its own access layer, transport layer, security layer, management layer and core layer network components;
- The open IoT middleware;
- The street lighting and energy management layer that integrates the connected actuators/controllers with web-based management applications, including a remote

street lighting poles and energy management tool for city to measure, manage and monitor connected public street lights by using a real-time, map-based view, and a street lighting poles asset management application which helps maintenance planning and operations management.

The goal of the use case is to implement in the end a smart lighting services within Smart City use case, over a 5G enabled architecture, with slicing support, from IoT devices to the smart lighting cloud application. There are depicted two steps of implementation:(1) transition from existing LoRaWAN infrastructure to a LTE-M enabled network with KPIs and functionalities preservation, using the existing 4G network infrastructure, on RAN and Core physical infrastructure, with extension of implementation (1') to a virtualized EPC Core; (2) SLICENET 5G architecture and components within the open Smart City open framework.

The high-level network required transformation from step (1) to step (2) 5G implementation is described in the next architectural proposal, including key elements for infrastructure, application and security side:

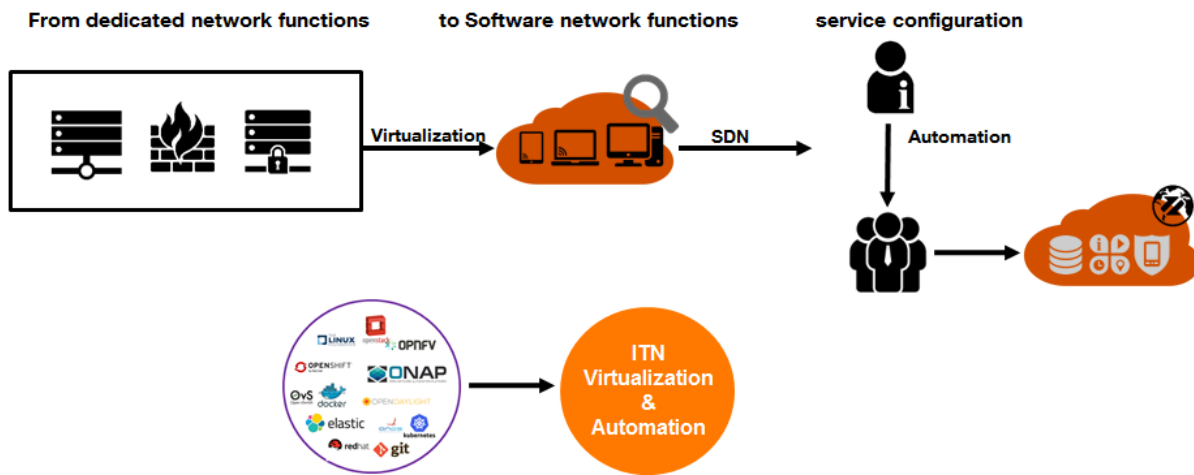


Figure 29 SmaLi-5G required network transformation

The slicing Smart City lighting use case concept is depicted into the following picture:

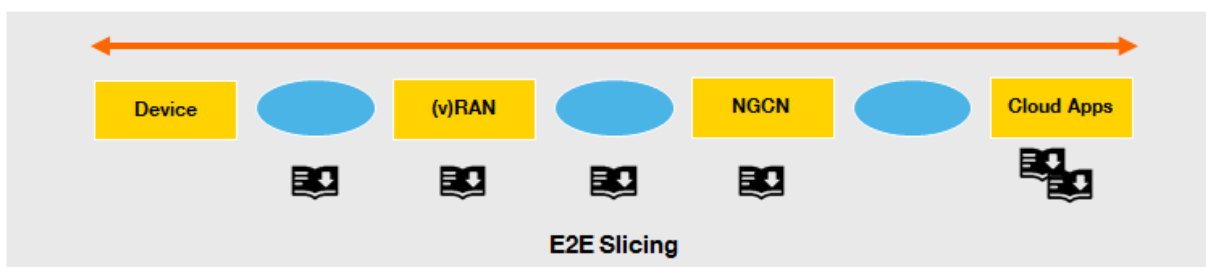


Figure 30 SmaLi-5G End-to-End slicing concept

6.2.1.2 Relation to 5G Requirements and Visions

We envisage to demonstrate the benefits of the SLICENET technical approach by validating the project developments through selected 5G use cases in an integrated environment that will include all the control and management components to support the Network Slices lifecycle. The result of the SLICENET project will be used to validate and demonstrate 5G capabilities (slice management etc.) in the context of SmaLi-5G verticals use case proposed by Orange in Alba Iulia.

It will be extremely relevant to seamlessly map and evolve the SmaLi-5G use case towards 5G-PPP SLICENET based architecture assessing the various technical and operational KPIs against the initial status quo built on legacy, LoRaWAN or LTE-M connectivity technologies.

Regardless the ultra-low-latency and high bandwidth that are not key requirements, SmaLi-5G use case will be considered in the scope of the 5G Massive machine-type communication category where the challenge is to accommodate the massive number of connected actuators/controllers without impacting the QoS and QoE. The case may be extended to a real big city within millions of lighting poles scenario, that will be connected to network, as a massive IOT service. Another service requirement to be met by the SmaLi-5G use case is to assure ultra-high network reliability and availability, while low-power, context awareness and location awareness requirements for managing the connected actuators/controllers over the access and transport layers can further improve the solution cost efficiency. This will be especially important during the daytime when the smart streets lighting poles infrastructure is supposed to remain powered to facilitate other city services (e.g. public safety surveillance, air quality monitoring, public Wi-Fi hotspots, advertising).

During the SmaLi-5G demonstration we will rely on various network analytics tools, extended towards SLICENET operations to cope with complex, dynamic, and heterogeneous networks featuring large numbers of connected nodes, and to correlate all monitoring sources in order to create a cognitive real-time supervision of QoS and QoE. In the same time we will look forward to monetize the cognitive insights generated within the SmaLi-5G use case, by exposing them to third parties that are developing additional use cases.

6.2.1.3 Goals

The main goals of the SLICENET SmaLi-5G use case are:

- Specification of business, functional and security requirements for Smart City IoT – Smart Lighting infrastructure with focus on energy consumption optimization and intelligent lighting in order to be mapped on the proposed 5G SLICENET enablers developed in the context of the current proposal;
- Map and benchmark the LoRaWAN and LTE-M based architectures used to assess the Smart City IoT applications over the promised 5G SLICENET based architecture in order to assess the various technical and operational KPIs against the initial status quo;
- Integration and testing of the Smart City SmaLi-5G vertical use case within the project's 5G communication framework;
- Prototype demonstration of the SmaLi-5G targeting the requirements identified for this specific vertical use case;
- Demonstration of the openness of 5G to different radio access technologies
- Demonstration of the coexistence of selected Smart City IoT applications in the shared 5G infrastructure, without decreasing the value for KPIs achieved in the initial setup demonstration;
- Timing service creation from weeks or days to hours or minutes;
- Extended network coverage, new service capabilities and new business models;
- Enhanced network management and network control;
- Usage of different types of RAN terminals

- Prototype the network slicing model for the targeted use-case, based on SmaLi-5G requirements. As the devices transmit data information to a centralized server with respect of low-power, low energy characteristic it may be implemented the concept over the already sliced operator network.
- LoRaWAN classes include Class A, Class B, Class C used for different functionalities, that will be evaluate in LTE cat M1 cellular technologies and further in the next NR 5G generation.

A best practice will be to create a measurement framework that can monitor and evaluate city-level impacts of smart and connected lighting investments thanks to SmaLi-5G. The adoption of 5G based smart city datasets will help to build the investment case for smart technology projects. These datasets can clearly define how investments can improve infrastructure QoS and QoE across a city and deliver benefits to its citizens.

6.2.1.4 Actors

Orange Romania, Alba Iulia Municipality [27], Flash Lighting Services S.A., Flashnet SRL [28], BOX2M [29].


6.2.1.5 General Assumptions

The Smart Lighting solution will reside in the Cloud edge part of the 5G Architecture. It is not a low latency or high bandwidth solution and in this particular case, the virtualization of this service doesn't have to stay near (location wise) to the deployment. The lighting poles provide and transmit to Management Server indicators related to power, voltage, electrical current, active/reactive/apparent power, power factor, energy (active/reactive) and functioning time.

From the transport network perspective, the traffic is characterized by small bursts of data from a large number of devices. The size of packets transmitted by lighting pole counters 30 bytes.

Table 12 outlines the lamps technical specifications.

Table 12 Lamp technical specifications

Picture	
Input Voltage	100-277VAC 50/60HZ
Rated Power	40W
Luminous Flux	4800lm
Luminous Efficiency	120lm/w
Beam Angle	140° x 70°
Power Factor	>0.9
IP Rating	IP66
Power Efficiency	88%
Correlated Colour Temperature	3000-3500K, 4000-4500K, 5000-5500K, 6000-6500K
Colour Rendering Index	Ra>70
Total harmonic distortion	THD<20%

Storage Temperature	-40° - +80°
Operation Temperature	-40° - +50°
Housing Material	Aluminium Alloy + PC
Net Weight	4.5 Kg
Gross Weight	5.8 Kg

A LoRaWAN is composed of end devices and gateways, and based on MAC layer there are three end-device classes defined as Class A, Class B and Class C, that are bi-directional for communication. Each class of LoRaWAN has its sets features.

Class A end devices (bidirectional communication):

- The frame is divided into uplink transmission and downlink transmission. Uplink is consists of 1 slot followed by 2 downlink slots
- Uplink slot is scheduled by End device itself based on its need, decided on random basis similar to ALOHA protocol.
- It is the lowest power LoRa end device
- Battery powered sensors
- Most energy efficient
- Must be supported by all devices
- Downlink available only after sensor TX

Class B end devices (bidirectional communication):

- In addition to Class A, Class B random receive windows, devices open extra receive windows at scheduled times
- The end-device open its receive window at the scheduled time by receiving a time synchronized Beacon from the gateway.
- The server knows when the end-device is listening
- Battery powered actuators
- Energy efficient with latency controlled downlink
- Slotted communication synchronized with a beacon

Class C end devices (directional communication with maximal receive slots):

- Nearly continuously open receive windows, only closed when transmitting
- Main powered actuators
- Devices which can afford to listen continuously
- No latency for downlink communication

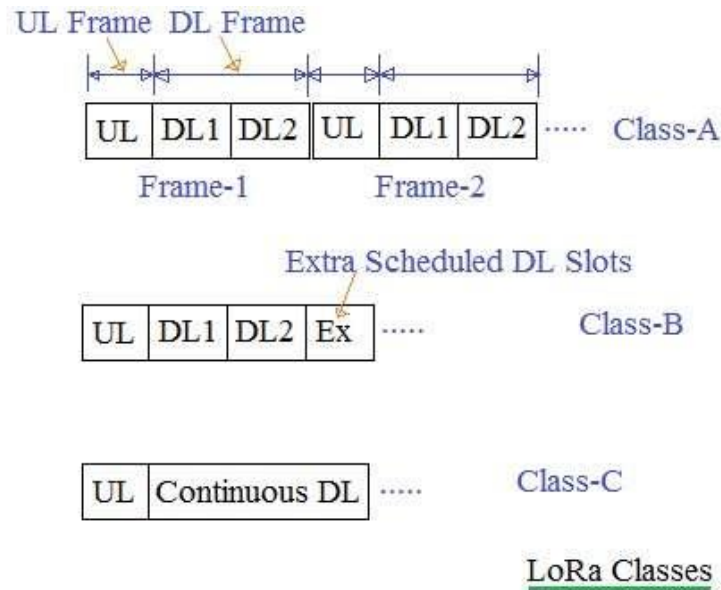


Figure 31 Summarized LoRaWAN Classes and frames transmission

General LoRaWAN Architecture [30], as described by Lora Alliance, including sensors (application, physical, processor) to the network server (server logic, IP stack) and encrypted backhaul is as follows:

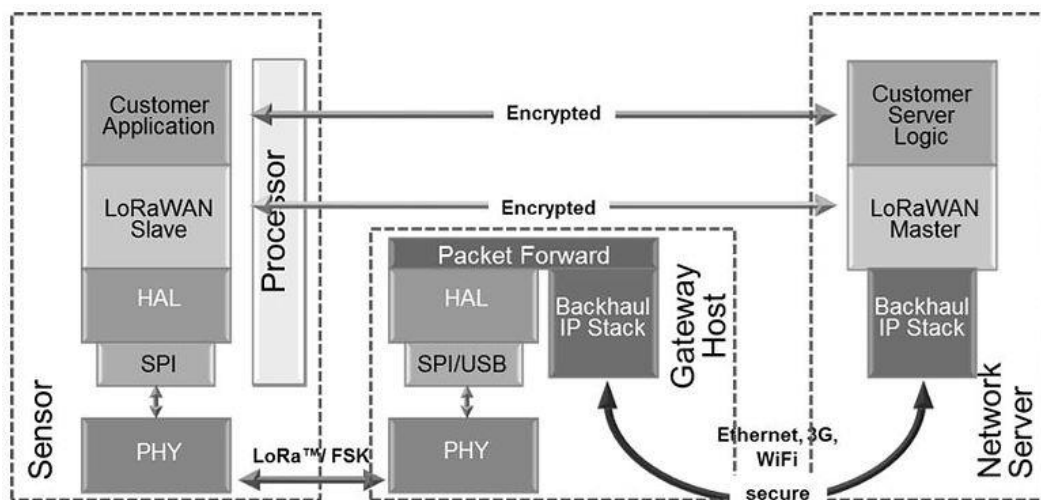


Figure 32 General LoRaWAN Architecture [30]

LoRaWAN is typically laid out in a star-of-stars topology, gateways is a transparent bridge relaying messages between end-devices and a central network server in the backend [Lora Alliance Technology], with data rates range from 0.3 kbps to 50 kbps.

As in RF Wireless-World (rfwireless-world.com), the general summary is:

LoRa Class A	LoRa Class B	LoRa Class C
Battery Powered	Low Latency	No Latency
Bidirectional communications	Bidirectional with scheduled receive slots	Bidirectional communications
Unicast messages	Unicast and Multicast messages	Unicast and Multicast messages
Small payloads, long intervals	Small payloads, long intervals, Periodic beacon from gateway	Small payloads
End-device initiates communication (uplink)	Extra receive window (ping slot)	Server can initiate transmission at any time
Server communicates with end-device (downlink) during predetermined response windows	Server can initiate transmission at fixed intervals	End-device is constantly receiving

Figure 33 LoRaWAN general summary capabilities

Battery life of the end-devices and network capacity in a general deployment scenario is relevant so the LoRaWAN network server manages the data rates and RF output for each end-device individually by means of an adaptive data rate (ADR) scheme.

Related to the gateways, they are connected to the network server via standard IP connections while end-devices use single-hop wireless communication to one or many gateways. The network server deployment and hosting is relevant for the smart city use case.

LoRa internet of things network is considered as critical infrastructure, needing the confidentiality of personal data or functions for the society, by deploying secure communication. LoRa introduces the following layers of encryption:

- Unique Network key (EUI64), ensure security on network level
- Unique Application key (EUI64), ensure end to end security on application level
- Device specific key (EUI128)

LoRaWAN for Europe characteristics:

- LoRaWAN™ defines ten channels, eight of which are multi data rate from 250bps to 5.5 kbps, a single high data rate LoRa® channel at 11kbps, and a single FSK channel at 50kbps.
- The maximum output power allowed by ETSI in Europe is +14dBm

As LoRa® Alliance Technical Marketing Workgroup, the next table guides the steps to LTE-cat-M1 migration and further to NR generation access, with respect of data rate, power efficiency, battery life time:

Feature	LoRaWAN	Narrow-Band	LTE Cat-1 2016 (Rel12)	LTE Cat-M 2018 (Rel13)	NB-LTE 2019(Rel13+)
Modulation	SS Chirp	UNB / GFSK/BPSK	OFDMA	OFDMA	OFDMA
Rx bandwidth	500 - 125 KHz	100 Hz	20 MHz	20 - 1.4 MHz	200 KHz
Data Rate	290bps - 50Kbps	100 bit/sec 12 / 8 bytes Max	10 Mbit/sec	200kbps – 1Mbps	~20K bit/sec
Max. # Msgs/day	Unlimited	UL: 140 msg/day	Unlimited	Unlimited	Unlimited
Max Output Power	20 dBm	20 dBm	23 - 46 dBm	23/30 dBm	20 dBm
Link Budget	154 dB	151 dB	130 dB+	146 dB	150 dB
Battery lifetime - 2000mAh	105 months	90 months		18 months	
Power Efficiency	Very High	Very High	Low	Medium	Med high
Interference immunity	Very high	Low	Medium	Medium	Low
Coexistence	Yes	No	Yes	Yes	No
Security	Yes	No	Yes	Yes	Yes
Mobility / localization	Yes	Limited mobility, No loc	Mobility	Mobility	Limited Mobility No Loc

Figure 34 Migration Steps to Next Generation 5G Radio

The assumption is to extend the access LoRaWAN technology and feature to LTE Cat M1 and further to the NR 5G generation.

LTE Cat M1 is a new cellular technology, specifically designed for the needs of applications targeting the Internet of Things (IoT) or machine-to-machine (M2M) communications (<https://www.u-blox.com/en/lte-cat-m1>).

LTE Cat M1 is a low-power wide-area (LPWA), there are develop tests of access technology to be adapted to the existing RAN deployments (as described in the Figures), based on existing core network, extended to the scenario based on functions on a virtualized domain.

Key application based on LTE Cat M1 covers the use-cases:

1. Smart metering
 1. Cat M1 for monitoring metering and utility applications based regular and small data transmissions
 2. Network coverage as a key issue.
 3. Meters are located inside buildings or basements, Cat M1's extended range leads to better coverage in hard to reach areas.
2. Smart cities
3. Cat M1 control street lighting.

6.2.1.6 SLICENET QoE Sensors

- Lighting poles reachability state
- Network traffic metrics and KPIs
- VNFs loading state machines, in case on massive IoT smart lighting application.
- Extended to the case of millions of lighting pools in a big city.

6.2.1.7 SLICENET QoE Actuators

1. Class B and Class C end-devices
2. Scale-in VNFs

3. Scale-out VNFs
4. Lighting sensors
5. Increase/decrease QoS slice parameters
6. Triggered alarms

For sake of clarity the set of VNFs (defined as a vEPC as in 4G implementation) envisaged for the use case is containing the virtualized network functions from communication service provider and network operator provider, in this case the telco operator. The entire ecosystem will be in the end 5G deployed implementation, the network elements involved in communication service and slicing. The SLICENET actuator is the “engine” responsible for controlling the SmaLi-5G system resources, operating from QoE perspective into a software-based manner, based on inputs received from the set of elements.

6.2.1.8 Other SLICENET System Components

Access network, Transport network, Virtualized Packet Core, Cloud Computing Infrastructure as a Service, Control Plane and Management plane.

6.2.1.9 External Systems

InteliLIGHT system architecture, Live Objects IoT middleware, BOX2M system architecture.

6.2.2 Detailed Steps

6.2.2.1 Preconditions

The conditions/actions that must occur before the execution of the use case in order to obtain the described behaviour:

1. Access Network provides connectivity (from LoRaWAN to LTE-M and 5G NR)
2. The system is in a functional state
3. Core Network
 1. Cloud edge
4. Service Layer
5. Control Layer

6.2.2.2 Metrics

The system is working normally, no malfunctioning in lighting poles, not impacting the KPIs (as high level QoE metrics) or network system, as low-level metrics:

- normal lighting poles functioning
- VNF`s vCPU/RAM/disk consumption rate
- end to end packet loss
- latency
- jitter
- smart lighting scheduling

6.2.2.3 Trigger

The main actions that describes the starts the use case execution:

1. scheduled smart city lighting (example given):
 1. summer time:

1. planned start: 21:00 (\pm 15 min)
2. end stop: 06:30 (\pm 15 min)
2. winter time:
 1. planned start: 19:00 (\pm 15 min)
 2. end stop: 08:30 (\pm 15 min)
2. light intensity sensors, triggered thresholds
 1. poles diming, extended to the presence scenario, where during the night, there is no or low human presence on the streets
 2. trigger to low the power light consumption (class A activity)
3. Lighting pole is powered
4. Lost connectivity with lighting pole
5. Massive connectivity session flapping
6. High CPU resources usage
7. High packet loss

6.2.2.4 Post Conditions

Success conditions: the device must communicate through the 5G network with the Cloud edge and must be able to control the lighting poles.

Failed End protection: the device will not be able to communicate through the 5G network with the Cloud edge and will not be able to control the lighting poles.

Connection between lighting poles and Lighting Management server is flapping; data sent by lighting pole lost on transit due to network congestion or VNF overloading.

6.2.2.5 Workflow

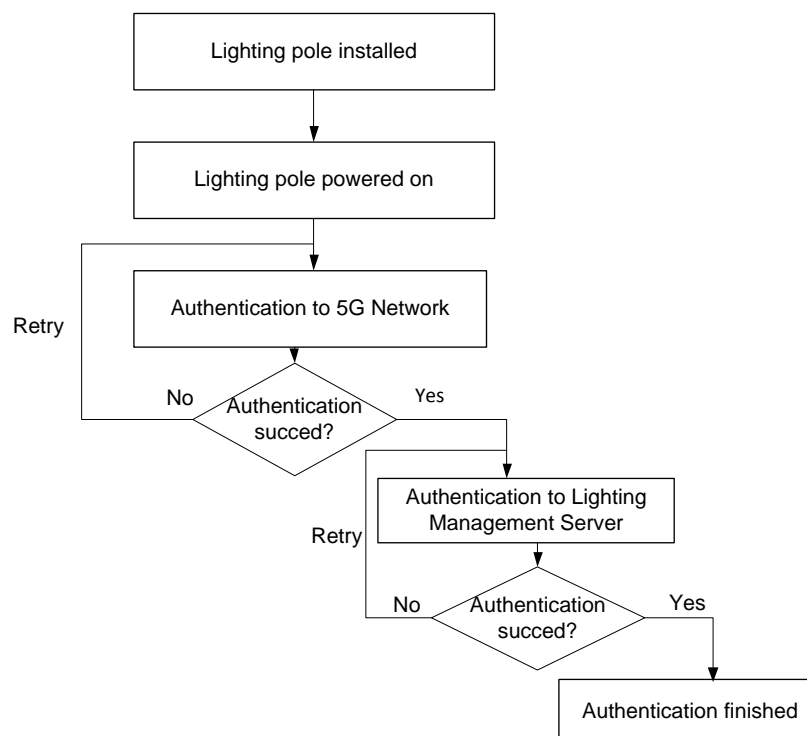


Figure 35 SmaLi-5G Provisioning flow

The lighting pole is powered on and is attempting to authenticate to 5G vCore network.

1. Lighting pole system is installed
2. Lighting pole is powered on
3. The pole system is trying to connect to the communication network
4. The system is authenticated with the communication network
 1. If authentication succeeds, go to step 5
 2. Else go to step 4, the failed cause to be analyzed at network level
5. The pole lighting system is authenticated to the management server
 1. If Yes, authentication succeeds, authentication finished, system starts working
 2. Else, go to step 5, the cause to be analyzed at management server level

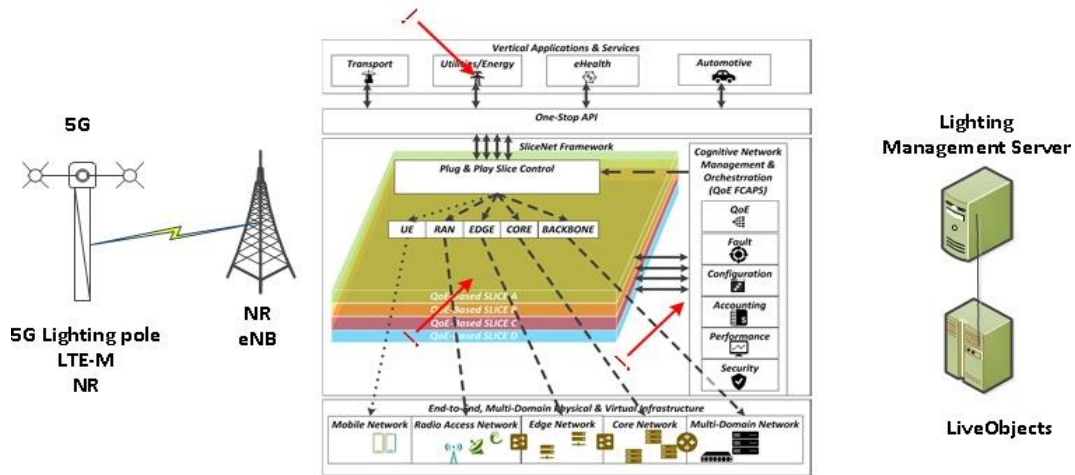


Figure 36 Integration in SLICENET architecture

6.2.3 Technical Requirements

The technical requirements described in this section are further detailed in Annex A.

6.2.3.1 Requirements on Cognition (Intelligence)

The cognition and intelligence are based on two scenarios:

1. Normal system functioning use case scenario
2. Defect system functioning scenario

For the normal system functioning scenario the cognition is following the Authentication to Lighting Management Server steps and procedures, with respect of cognition of characteristics and requirements as described in section 6.2.1.5.

For the defect system functioning scenario, the intelligence is part of management system for lighting solution.

6.2.3.2 Requirements on the One-Stop API

In case of smart lighting and smart metering it is proposed to provide the management functionality for the underlying virtual and physical infrastructure.

The solution for a large smart city implementation involves up to millions of devices connected through the communication network to the management system. The requirement is to provide access to the “slice” into an easy way, scalable and efficient, by deploying at large scale smart sensors.

Devices and sensors need to be addressable and identifiable for precise management and automation into the dedicated slice, as registered with the network and management systems.

Required level of management and control over network are oriented to slice resources over virtualized infrastructure. Smart Lighting requests the ONE-STOP-API exposed from SLICENET platform to the slice communication provider.

The general architecture of service communication for slice and slice creation is based on 3GPP TR 28.801[41]. The slice is created as a service chaining of virtualized network elements (VNFs).

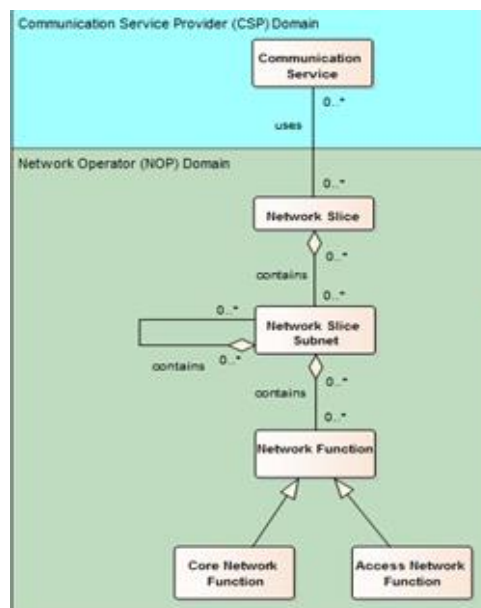


Figure 37 General services communication architecture

6.2.3.3 Requirements on Slicing/Slice

The network slicing is requested in the core part, as dynamic capabilities of scaling of virtual network functions for the dedicated lighting and metering use case. The slice requirement may be integrated as a “Smart City Slice” approach.

The slice must assure and guarantee the performance, availability, capability to cope with very large numbers of devices accessing the resources into a planned or triggered mode and must to respond to the identified Smart City lighting requests for communication. The slice should be offered and available, when it is needed.

The slice must be able to provide security capabilities, through smart isolation inside the network, by limiting access to the resources and data traffic. The network provided slice must assure also cybersecurity requirements and must be able to respond to the threats than may affect the end-to-end system functioning.

The general slicing requirements are related to NG Radio, Network, O&M and applications and network functions hosted in Cloud, with respect of power, latency, security and costs of implementation.

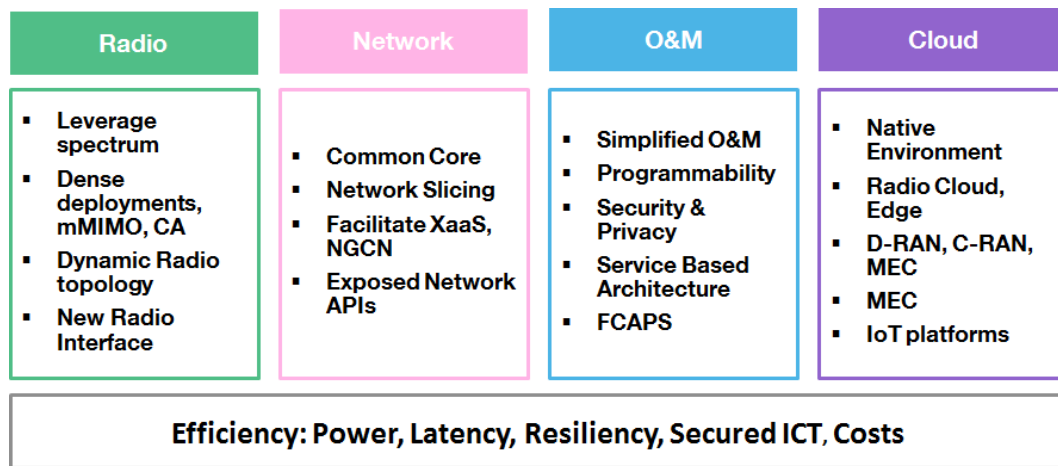


Figure 38 Telco end-to-end slicing concepts

The slicing resources needed are a composition of connectivity services resources (including PNFs and VNFs) and cloud and network resources, with monitoring capabilities and basic control over the resources.

6.2.3.4 Requirements on Multi-domain Operations

Generally, the operators are deploying a fully coverage within a city, so multi-domain networking operations for Smart City use cases may be extended to the case where part of connected devices may be provided into a sharing method within others network providers.

6.2.3.5 Requirements on RAN

The Smart City use cases for smart lighting and metering have specific requirements regarding RAN capabilities:

- High reliability
- Dense coverage
- Accommodation of small bursts of data
- Accommodate large density of devices/ km2

6.2.3.6 Requirements on MEC

This use case is not a low latency or high bandwidth solution and in this particular case, the virtualization and instantiation of this service doesn't have to stay near (location wise) to the deployment.

The Smart City use cases of lighting and metering are not mandatory deployed on MEC.

6.2.3.7 Requirements on Core

The general Core requirements are depicted by the following system architecture for the Smart City use cases, referenced in Figure 36.

The core functionality should provide the required functionalities for system communication as follows:

1. VNFs and the service chaining
2. Authentication for devices
3. VNFs: vMME, vPGW,

4. IP/Transport network

A relevant scenario is covered by the possibility of slicing definition and creation at the core network level, through the set of communication components, as VNFs structures and/or links to the PNF network. It will be defined a specific sliced system with dedicated resources for the communication capabilities within the Smart City scenario:

1. Low bandwidth needs
2. Low delay
3. Fast deployment of core system, when needed, where needed
4. Massive communication type devices
5. Large number of devices and sensors
6. High requirements for signalling capabilities
7. Sensitive response to the system triggers
8. Easy to accommodate new devices
9. Economic aspects, for business cases sustainability, accommodating of slicing principles over the dedicated hardware infrastructure

6.2.3.8 Requirements on Enterprise Network

In case of Smart Lighting use cases, involving the management server of the apps, it may be considered the scenario when the system is hosted at the solution provided facility and not being part of 5G telecom provider.

For the sake of clarity, the following diagram is presented:

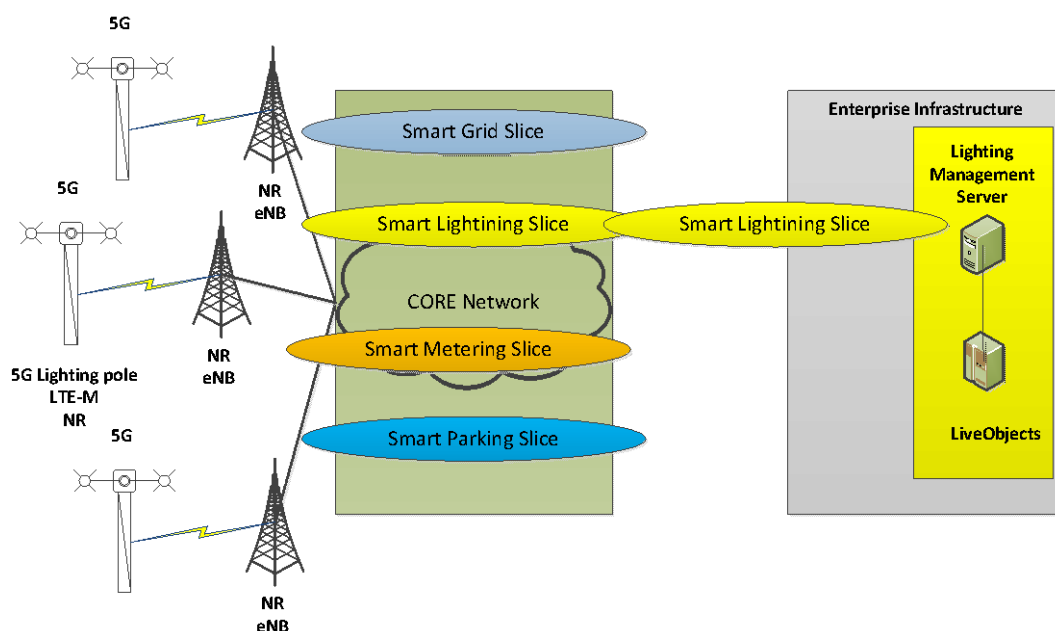


Figure 39 SmaLi-5G Inter-domain slicing concepts

In case if extending the requirements to the enterprise level, the lighting management solution will be within the enterprise infrastructure, communication needs with intelligent decision and cognition should be considered at Enterprise level. An end-2-End slice with service level capabilities are built. For the Enterprise Infrastructure, the slicing model may follow the same device class needs:

1. scheduled smart city lighting (example given):

1. summer time:
 1. planned start: 21:00 (\pm 15 min)
 2. end stop: 06:30 (\pm 15 min)
2. winter time:
 1. planned start: 19:00 (\pm 15 min)
 2. end stop: 08:30 (\pm 15 min)
2. light intensity sensors, triggered thresholds
 1. poles diming, extended to the presence scenario, where during the night, there is no or low human presence on the streets
 2. trigger to low the power light consumption (class A activity)
3. Lighting pole is powered
4. Lost connectivity with lighting pole

6.2.3.9 Non-functional Requirements

The Smart City lighting model and water metering must offer in normal condition low-power, low-energy capabilities, with basic functioning on battery extended time range, until 10 years, providing permanent or temporary scheduled or triggered functioning.

6.2.3.10 Coverage of Service Life-cycle Phases

Phase 1 [Service request / SLA negotiation]: Exposed through One-Stop API

Phase 2 [Planning / Design]: Dimensioning according to customer needs

Phase 3 [Deployment]: Delivery, installation and provisioning

Phase 4 [Operation and Monitoring]: Available through Lighting Management interface

Phase 5 [Billing]: Monthly and/or per number of devices basis

Phase 6 [Decommissioning]: At customer`s request

The life cycle should be correlated with T2.2.

6.2.4 Implementation, Evaluation and Impact

6.2.4.1 Prototyping/Testbed

The prototyping of the intelligent lighting use case will enable the management of the poles in Alba Iulia city (100 poles) on the new slicing concept, comparing the different technologies of access, from LoRaWAN to LTE-M and NB-IoT and also highlighting the KPIs. The testbed will use a dedicated slice core network.

The use case will provide a TRL of 4.

6.2.4.2 Benchmarking and Validation

The use case will be implemented and tested by Orange, in Alba Iulia city and also in the lab environment, the results will be compared with existing functionality network infrastructure based on LoRaWAN.

6.2.4.3 Relation to 5G-PPP KPIs

This use case is expected to contribute to the following performance KPIs:

1. Providing higher wireless area capacity and more varied service capabilities compared to 2010.
2. Saving up to 80% of energy per service provided.
3. Reducing the average service creation time cycle
4. Creating a secure, reliable and dependable Internet with a “zero perceived” downtime for services provision.
5. Facilitating very dense deployments of wireless communication.
6. Enabling advanced user controlled privacy.

This use case is expected to contribute to the following societal KPIs:

1. Enabling advanced User controlled privacy;
2. Reduction of energy consumption per service up to 80% (as compared to 2010);
3. European availability of a competitive industrial offer for 5G systems and technologies;
4. Establishment and availability of 5G skills development curricula (in partnership with the EIT).

This use case is expected to contribute to the following business KPIs:

1. Leverage effect of EU research and innovation funding in terms of private investment in R&D for 5G systems in the order of 5 to 10 times;
2. Reach a global market share for 5G equipment & services delivered by European headquartered ICT companies at, or above, the reported 2011 level of 43% global market share in communication infrastructure.

6.2.4.4 Technical Innovation in the Field

SLICENET will provide the transformation of Smart City Lighting use case from traditional implementation to the more programmable infrastructure, based on services and application, with a centralized open platform (open middleware). The SLICENET solution is intended to be related to the management plane and control plane, related to the communication provider but also to the communication service customer.

6.2.4.5 Business Impact in the Sector

In EU only the annual smart city benefits from 5G is estimated to reach 8.1 billion Euros in 2025. The business evolution will require transformation for the technology, with main directions as connecting everyone, connecting objects, connecting fast, being reactive, at low costs and environmental friendly. The *SmaLi-5G* use case will drive the service providers (apps providers, operators and manufacturers) for the future business evolution.

Actual smart city stakeholders expectations in the context of the new 5G technology introduction were surveyed as described in Annex B.

6.2.4.6 End User Benefits

Following the demonstration of the SmaLi-5G use case we anticipate clear benefits in implementing smart and innovative e2e solutions that will help City Hall to deploy smart end efficiently lighting systems with low energy consumption, based on the new 5G technology systems.

7 Conclusions

This document presents the results of the initial steps of the SLICENET project. SLICENET is taking a verticals-in-the-loop co-design approach in which diversified vertical sector use cases are being actively involved in the initial stages of the architecture definition and design.

A detailed description of three vertical sector use cases has been presented in this report: smart grid self-healing, eHealth smart/connected ambulance, and smart city. These use cases are expected to contribute for the 5G-PPP performance, societal, and business KPIs, and the relation to the 5G visions and requirements has been emphasized throughout the use case definitions.

The report gathers communication requirements that have been laid out from a user perspective and will aid the further design and implementation of 5G network slicing and slice management. Vertical sector requirements have been broken down in order to facilitate further impact analysis and integration in the several 5G network model components.

The next project iteration will be the definition and design of the SLICENET architecture and interfaces, for which the outcome of D2.1 should provide valuable inputs. There will be a refinement of the use case requirements during the SLICENET architecture definition – the technical requirements will be further analyzed in T2.2.

The scenarios defined for these use cases will be used to validate the SLICENET implementation in later phases of the project, in WP7 and WP8.

References

- [1] <https://slicenet.eu/> © SLICENET consortium 2017
- [2] Technopedia, 2017, "Use Case", [Online]. Available at: <https://www.techopedia.com/definition/25813/use-case>
- [3] A. Cockburn, "Writing Effective Use Cases", Addison-Wesley, 2001.
- [4] EU 5G-PPP, 2014, "5G-PPP KPIS", [Online]. Available at: <https://5g-ppp.eu/kpis/>
- [5] EU 5G-PPP SELFNET Project, "SELFNET: Framework for Self-Organised Network Management in Virtualized and Software Defined Networks" (H2020-ICT-2014-2/671672), [Online]. Available at: <https://selfnet-5g.eu/>
- [6] EU 5G-PPP, 2014, "NRG-5", [Online]. Available at: <https://5g-ppp.eu/nrg-5/>
- [7] IEC, "IEC 61850-5 Ed.2: Communication networks and systems for power utility automation – Part 5: Communication Requirements for Functions and Device Models", 2013.
- [8] IEC, "IEC 61850-8-1 Ed.2: Communication networks and systems for power utility automation – Part 8-1: Specific communication service mapping (SCSM) – Mappings to MMS (ISO 9506-1 and ISO 9506-2) and to ISO/IEC 8802-3", 2011.
- [9] IEC, "IEC 61850-9-2 Ed.2: Communication networks and systems for power utility automation – Part 9-2: Specific communication service mapping (SCSM) – Sampled values over ISO/IEC 8802-3", 2011.
- [10] IEC, "IEC TR 61850-90-1 Ed.1: Communication networks and systems for power utility automation – Part 90-1: Use of IEC 61850 for the communication between substations", 2010.
- [11] IEC, "IEC TR 61850-90-2 Ed.1: Communication networks and systems for power utility automation – Part 90-2: Using IEC 61850 for communication between substations and control centres", 2016.
- [12] IEC, "IEC TR 61850-90-5 Ed.1: Communication networks and systems for power utility automation – Part 90-5: Use of IEC 61850 to transmit synchrophasor information according to IEEE C37.118", 2012.
- [13] IEC, "IEC TR 61850-90-12 Ed.1: Communication networks and systems for power utility automation – Part 90-12: Wide area network engineering guidelines", 2015.
- [14] IEEE, "IEEE C37.118.1: IEEE Standard for Synchrophasor Measurements for Power Systems", 2011.
- [15] IEEE, "IEEE C37.118.2: IEEE Standard for Synchrophasor Data Transfer for Power Systems", 2011.
- [16] ITU-T, "ITU-T X.690: Information technology – ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)", 2015.
- [17] Efacec, "Efacec Protection and Control IEDs Selection Guide", [Online]. Available at: <http://www.efacec.pt/en/wp-content/uploads/2016/10/protection-and-control-ieds.pdf>

- [18] Efacec, "Efacec Automation Studio 3 – Portfolio of Products", [Online]. Available at: <http://www.efacec.pt/en/wp-content/uploads/2016/10/automation-studio-datasheet.pdf>
- [19] D. Brnobic, 2013, "Role of Synchrophasors in Smart Grids", WAMSTER, [Online]. Available at: <http://www.wamster.net/w2/articles/synchrophasors-role-in-smart-grids>
- [20] T. Kleiner, 2014, "Why 5G research?", 5G Research in Horizon 2020, [Online]. Available at: <https://ec.europa.eu/digital-single-market/news/5g-research-horizon-2020-webcast>
- [21] eHealth Hub, 2017, "New EU General Data Protection Regulation – GDPR: get ready in 12 steps", [Online]. Available at: <http://www.ehealth-hub.eu/data-protection-ehealth-business-regulation/> [Accessed 2017-07-26]
- [22] EUODP, "European Union Open Data Portal", [Online]. Available at: <http://data.europa.eu/euodp/en/data>
- [23] UD DATA.GOV, "The Home of the U.S. Government's open data", [Online]. Available at: <https://www.data.gov>
- [24] DATA.GOV.RO, [Online]. Available at: <http://data.gov.ro>
- [25] ISO 37120, "Sustainable development in communities - Indicators for city services and quality of life", (ISO 37120: 2014), [Online]. Available at: <https://www.iso.org/standard/62436.html>
- [26] Philips Lighting, World Council of City Data, "The Citywide Benefits of Smart & Connected Public Lighting" report assessed through ISO 37120, 2017 [Online]. Available at: <http://news.dataforcities.org/2017/03/wccd-and-philips-lighting-publication.html>
- [27] Primaria Municipiului Alba Iulia, [Online]. Available at: <http://www.apulum.ro/>
- [28] FLASHNET, [Online]. Available at: <https://www.flashnet.ro/>
- [29] BOX2M, "industrial IoT technologies", [Online]. Available at: <http://www.box2m.com/>
- [30] LoRa Alliance, 2017, "LoRa Alliance Technology", [Online]. Available at: <https://www.lora-alliance.org/technology>
- [31] M. M. F. F. Edward C Jauch and M. Chief Editor: Helmi L Lutsep, "Ischemic Stroke," Medscape, 2017. [Online]. Available: <http://emedicine.medscape.com/article/1916852-overview>. [Accessed Octy 2017].
- [32] Medscape, "NIH Stroke Scale," Medscape, 2014. [Online]. Available: <http://emedicine.medscape.com/article/2172609-overview>. [Accessed Oct 2017].
- [33] D. F. F. Bryan Bledsoe, "Mobile Stroke Units: A Device in Search of an Indication," *JEMS*, 2017.
- [34] imedalapps, "Drones to the rescue: Improved delivery of AEDs to remote patients with cardiac arrest," imedalapps, 2017. [Online]. Available: <https://www.imedalapps.com/2017/07/drone-delivery-aeds/>. [Accessed 2017].

-
- [35] C. A. e. al., "Time to delivery of an automated external defibrillator using a drone for simulated out-of-hospital cardiac arrests vs emergency medical services.," *JAMA*, no. 317, pp. 2332-2334, 2017.
- [36] JESIP, "M\ETHANE," JESIP, 2017. [Online]. Available: <http://www.jesip.org.uk/methane>. [Accessed Oct 2017].
- [37] B. B. (EU), "5G Public Private Partnership Context and Priorities," in *5G PPP Awareness & Information Day*, Brussels, 2014.
- [38] EU 5G-PPP SELFNET Project, "SELFNET: Framework for Self-Organised Network Management in Virtualized and Software Defined Networks" (H2020-ICT-2014-2/671672) [Online]. Available: <https://selfnet-5g.eu/>.
- [39] A. Cockburn, *Writing Effective Use Cases*, Addison-Wesley, 2001.
- [40] New EU General Data Protection Regulation – GDPR: get ready in 12 steps, <http://www.ehealth-hub.eu/data-protection-ehealth-business-regulation/> Accessed 2017-07-26
- [41] 3GPP TR 28.801 V1.2.0 (2017-05), 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Telecommunication management; Study on management and orchestration of network slicing for next generation network

Annex A Use Cases Requirements Tables

A.1 RAN

REQ_RAN_CN_01		
Smart Grid Use Case	Name	Support of network slicing
	Description	Applicable to both slice owner/provider and infrastructure provider: Allowing different level of sharing and isolation across resources and network functions.
	Justification	Main building block and enabler for all UCs
	Novelty	High
	Exploitability	High
	Impact on Verticals	High Provide the required level of control
Smart City Use Case	Name	Support of network slicing
	Description	Applicable to both slice owner/provider and infrastructure provider: Allowing different level of sharing and isolation across resources and network functions.
	Justification	Main building block and enabler for all UCs
	Novelty	High
	Exploitability	High
	Impact on Verticals	High Provide the required level of control

REQ_RAN_CN_02		
Smart Grid Use Case	Name	Efficient RAN and CN lifecycle management
	Description	Applicable to Slice Owner/provider: Allowing fine-grain service management and orchestration on per slice basis, shared or slice-specific, in particular through the design and runtime phases.
	Justification	Service automation for each UC and Building blocks
	Novelty	Medium-to-high
	Exploitability	High
	Impact on Verticals	Medium Allows slice owner/provider to manage their (oriented to the slice provider).

Smart City Use Case	Name	Efficient RAN and CN lifecycle management
	Description	Applicable to Slice Owner/provider: Allowing fine-grain service management and orchestration on per slice basis, shared or slice-specific, in particular through the design and runtime phases.
	Justification	Service automation for each UC and Building blocks
	Novelty	Medium-to-high
	Exploitability	High
	Impact on Verticals	Medium Allows slice owner/provider to manage their (oriented to the slice provider).

REQ_RAN_CN_03		
Smart City Use Case	Name	Support of disaggregated RAN and CN
	Description	Applicable to infrastructure provider: <ul style="list-style-type: none"> • Allowing flexible deployment of infrastructure to increase capacity, coverage, and multiplexing gain • OPEX optimization
	Justification	Separation of cell site and network processing in the data-centers Building blocks
	Novelty	High (if it is done through the orchestration)
	Exploitability	High
	Impact on Verticals	Low May need some service adaption

REQ_RAN_CN_04		
Smart City Use Case	Name	Support for resource abstraction and coordination
	Description	Applicable for both slice owner and infrastructure provider: <ul style="list-style-type: none"> • Allowing resource isolation and performance guarantees • Maximizing resource utilization and increase the total number of supported slices
	Justification	Allow isolation of network resources and state such that the exact time and frequency position of the resources are omitted. Maximize the multiplexing gain (better resource utilization)
	Novelty	High (if it is done through the orchestration)
	Exploitability	High
	Impact on Verticals	Low

	Verticals	May change the performance of the slice and infrastructure
--	------------------	--

REQ_RAN_CN_05		
Smart Grid Use Case	Name	RAN and CN KPI requirements
	Description	Applicable to slice owner: Allowing to meet the performance requirement and build the service
	Justification	Allowing to accommodate the UC performance requirements
	Novelty	High (if it is done through the orchestration)
	Exploitability	High
	Impact on Verticals	High
Smart City Use Case	Name	RAN and CN KPI requirements
	Description	Applicable to slice owner: <ul style="list-style-type: none"> • Allowing to meet the performance requirement and build the service • Low resources required by Smart Lighting UC based on KPIs
	Justification	Allowing to accommodate the UC performance requirements
	Novelty	High (if it is done through the orchestration)
	Exploitability	High
	Impact on Verticals	Medium

A.2 Control Plane

REQ_CONTROL_PLANE_01		
Smart Grid Use Case	Name	Slice Control Plane of 5G Wide-Area Network (WAN)
	Description	Control Plane shall handle e2e slices over a 5G Wide-Area Network (WAN); consequently, it: <ul style="list-style-type: none"> • Shall include Multi administrative domain handling • Might Include SDN-Orchestrator handling (for WAN links)
	Justification	The electric power grid covers wide geographical areas that may span across multiple administrative domains.
	Novelty	High
	Exploitability	High

eHealth Use Case	Name	Slice Control Plane of 5G Wide-Area Network (WAN)
	Description	Control Plane shall handle e2e slices over a 5G Wide-Area Network (WAN); consequently, it: <ul style="list-style-type: none"> • Shall include Multi administrative domain handling • Might Include SDN-Orchestrator handling (for WAN links)
	Justification	The ambulance will move at speed over a wide area, and the air interface connecting the ambulance communication infrastructure to the network will travel accordingly at speed. It is to be expected that frequent cell handovers will occur during the journey from the emergency scene back to the hospital, and this will necessitate multi administrative domain handling.
	Novelty	High One stop shop requirement for digital service providers will be novel
	Exploitability	Low Digital service providers will expect this as a service feature

REQ_CONTROL_PLANE_02		
Smart Grid Use Case	Name	Control Plane layers
	Description	Control Plane shall include three layers: <ul style="list-style-type: none"> • Service layer (when several slices are aggregated to provide one Service) • Slice layer (aggregation of several subnets) • Subnet layer
	Justification	The smart grid self-healing use case may require two different slices: one for time-critical horizontal communications between IEDs, the other for vertical communications between the IEDs and the SCADA system.
	Novelty	High
	Exploitability	High
eHealth Use Case	Name	Control Plane layers
	Description	Control Plane shall include three layers: <ul style="list-style-type: none"> • Service layer (when several slices are aggregated to provide one Service) • Slice layer (aggregation of several subnets) • Subnet layer
	Justification	The eHealth use case may require two different slices: one for the delivery of the high bandwidth video streaming service, and another for the communications with IoTs devices.
	Novelty	Medium

	Exploitability	Medium
Smart City Use Case	Name	Control Plane layers
	Description	Control Plane shall include three layers: <ul style="list-style-type: none"> • Service layer (when several slices are aggregated to provide one Service) • Slice layer (aggregation of several subnets) • Subnet layer
	Justification	Smart City Smart Lighting UC requires only one service correlated to one Slice (as KPIs defined).
	Novelty	Medium One specific service layer (smart lighting) with one slice over DSP
	Exploitability	Medium

REQ_CONTROL_PLANE_03		
eHealth Use Case	Name	System availability and reliability
	Description	Control Plane shall provide support logics for dynamic configuration of the data plane (when triggered by Cognitive)
	Justification	The ambulance service operates in a life-saving environment and requires an extremely high demand on network availability and reliability. Cognitive awareness at a level where the SliceNet system is aware of a potentially real-time life-threatening occurrence and is able to react accordingly, provides SliceNet with decision making criteria on how best to dynamically configure network resources.
	Novelty	High Raises ethical issues in terms of artificial intelligence and machine decision-making, which is currently a hot topic in other highly innovative services, such as driverless cars.
	Exploitability	High Digital service providers will market this feature as a USP

REQ_CONTROL_PLANE_04		
eHealth Use Case	Name	Slice instances status handling
	Description	Control plane shall maintain the e2e slice instances working status in order to properly handle interaction with other components (eg actions from API, actions from Cognitive, ...)
	Justification	Responsibility for maintenance of network slice instances is required to safeguard QoS and QoE, especially for life threatening services, where reliability and availability of network services is critical.
	Novelty	High
	Exploitability	High Arriving at a consensus around the ethics involved here will be an ongoing hot topic, and these discussions will raise awareness of these types of ethical features, which can be further exploited by the digital service providers.

REQ_CONTROL_PLANE_05		
eHealth Use Case	Name	Control Plane, proxy for API
	Description	Control plane shall act as proxy for received one stop API actions directed to other components (Cognitive, FCAPS)
	Justification	The justification parallels the questions asked in the Novelty part of the previous requirement. In life threatening scenarios, the digital and/or health service providers should have the capability to overwrite machine decision-making processes, through a control plane API? There would be potential ethical issues if this was not in place.
	Novelty	High Discussions around the ethics involved here will be novel.
	Exploitability	High Reaching consensus around the ethics involved here will be an exploitable feature for the digital service providers.

REQ_CONTROL_PLANE_06		
eHealth Use Case	Name	Control Plane recovery actions by Cognitive interworking
	Description	Control Plane shall be able to trigger instantiation and/or update of VNFs or vAPP as ordered by e.g. Cognitive platform to resolve QoS, QoE issues
	Justification	Notwithstanding the human intervention overwriting capability, it is important for this use case to have strong confidence in the network's ability to self-manage network resource reliability and availability.
	Novelty	High The dynamics around machine awareness decision making as part of the e2e

		process is novel.
	Exploitability	Medium Acceptance and confidence in such a feature would be marketable.

REQ_CONTROL_PLANE_07		
Smart Grid Use Case	Name	Slice Blueprint customization
	Description	Control Plane shall manage parametric slice blueprints by translating received parameters (over API) into actions via administered business logics per given slice blueprint/vertical, e.g.: <ul style="list-style-type: none"> • Identification of new VNFs and links to deploy • Configuration data of deployed VNFs (sent to FCA module) • Handling of uploaded customer vAPP
	Justification	This may be important to allow the adaptation of the slice resources when new communicating devices are added to a smart grid self-healing scheme.
	Novelty	High
	Exploitability	Medium
eHealth Use Case	Name	Slice Blueprint customization
	Description	Control Plane shall manage parametric slice blueprints by translating received parameters (over API) into actions via administered business logics per given slice blueprint/vertical, e.g.: <ul style="list-style-type: none"> • Identification of new VNFs and links to deploy • Configuration data of deployed VNFs (sent to FCA module) • Handling of uploaded customer vAPP
	Justification	This requirement offers digital service providers with a mechanism to replicate service deployment to new customers.
	Novelty	Low This is a 'nice to have' feature, but does not appear to be particularly novel.
	Exploitability	Low Would appear to have low marketability.
Smart City Use Case	Name	Slice Blueprint customization
	Description	Control Plane shall manage parametric slice blueprints by translating received parameters (over API) into actions via administered business logics per given slice blueprint/vertical, e.g.: <ul style="list-style-type: none"> • Identification of new VNFs and links to deploy • Configuration data of deployed VNFs (sent to FCA module) • Handling of uploaded customer vAPP
	Justification	Slice resources management and customization

	Novelty	Medium
	Exploitability	Medium

REQ_CONTROL_PLANE_08		
eHealth Use Case	Name	Activation of slice specific QoS and QoE metrics
	Description	At successful slice instantiation, Control Plane shall transfer concerned metrics from blueprint catalogue to Cognitive / FCAPS modules
	Justification	Cognitive module requires these metrics as part of dynamic decision-making process. Some parts, if not all, of the FCAPS module requires these metrics. For example, the Accounting module needs to have these metrics as part of the charge model for providing the service.
	Novelty	Low This is a 'nice to have' feature, but does not appear to be particularly novel.
	Exploitability	Low Would appear to have low marketability.

REQ_CONTROL_PLANE_09		
eHealth Use Case	Name	Priority Slice
	Description	Control Plane shall be able to manage priorities related to slice operations
	Justification	Slice instantiation on request by eHealth emergency services for UHD video streaming shall have higher priority.
	Novelty	High E2e priority slicing in the context of this use case is novel.
	Exploitability	High Feature offering QoS differentiation for emergency services has high degree of marketability.

REQ_CONTROL_PLANE_10		
eHealth Use Case	Name	Location based Slice instantiation
	Description	Control Plane shall manage slice subnets selection for instantiation optionally based on position of slice connected end devices
	Justification	RAN instantiated close to connected ambulances / affected disaster area in case of eHealth.
	Novelty	High Priority given to location based slicing could be coupled with other location based services, such as geo-fencing in emergency management scenarios.
	Exploitability	High Feature offering location responsiveness for emergency services has high marketability.

A.3 Data Plane

REQ_DATA_PLANE_01		
Smart Grid Use Case	Name	Physical / Virtual infrastructure programmability
	Description	The physical and virtual devices that compose the data plane infrastructure should provide capacity to be managed, configured, and re-configured if needed.
	Justification	The physical and virtual elements of the data plane infrastructure must provide tools to enable their programmability in order to provide slicing capabilities. For example, the data plane has to provide the capacity to configure and modify physical and/or virtual data paths (route, bandwidth, forwarding rules, etc.) which will be associated to network slices. Moreover, support for virtualized functions to be configured or computing resources (e.g. Virtual Machines (VMs)) to be instantiated are necessary for slice customization. Hence, the network programmability will be achieved at a lower level by enabling the configurability and manageability of the data plane infrastructure, physical and virtual.
	Novelty	High
	Exploitability	High
eHealth Use Case	Name	Physical / Virtual infrastructure programmability
	Description	The physical and virtual devices that compose the data plane infrastructure should provide capacity to be managed, configured, and re-configured if needed.
	Justification	The eHealth use case requires a flexible 'on demand' capability to setup and tear down network infrastructure, as necessitated by the requirements of the emergency situation. In some instances, this will involve life critical scenarios that demand high degrees of network capacity programmability.
	Novelty	High

		High bandwidth guaranteed QoS video streaming for emergency services is not currently available
	Exploitability	High Indications from the health service providers suggest this to be a highly exploitable requirement. This feature will be exploited by Digital Service Providers.
Smart City Use Case	Name	Physical / Virtual infrastructure programmability
	Description	The physical and virtual devices that compose the data plane infrastructure should provide capacity to be managed, configured, and re-configured if needed.
	Justification	The physical and virtual elements of the data plane infrastructure must provide tools to enable their programmability in order to provide slicing capabilities. For example, the data plane has to provide the capacity to configure and modify physical and/or virtual data paths (route, bandwidth, forwarding rules, etc.) which will be associated to network slices. Moreover, support for virtualized functions to be configured or computing resources (e.g. Virtual Machines (VMs)) to be instantiated are necessary for slice customization. Hence, the network programmability will be achieved at a lower level by enabling the configurability and manageability of the data plane infrastructure, physical and virtual.
	Novelty	High
	Exploitability	High

REQ_DATA_PLANE_02		
Smart Grid Use Case	Name	Network Slice Isolation Support
	Description	The data plane must provide the support for slice isolation, either by means of isolated logical abstractions of the physical hardware devices, in collaboration with the virtualization/control layer, or complete physical isolation if very high levels of security/privacy are required.
	Justification	Multiplexing capabilities (time/frequency/space) and physical diversity must be provided by the data plane to allow for the creation of multiple concurrent isolated network slices. Additionally, proper encapsulation and containers frameworks must be provided to guarantee the isolation integrity at the virtual data layer.
	Novelty	High
	Exploitability	High

eHealth Use Case	Name	Network Slice Isolation Support
	Description	The data plane must provide the support for slice isolation, either by means of isolated logical abstractions of the physical hardware devices, in collaboration with the virtualization/control layer, or complete physical isolation if very high levels of security/privacy are required.
	Justification	The eHealth use case mandates patient privacy.
	Novelty	High Data integrity and security required to protect user privacy.
	Exploitability	High Digital Service Providers can offer Kkey selling point of integrity and security of client data to health services providers will be the integrity and security of client data.
Smart City Use Case	Name	Network Slice Isolation Support
	Description	The data plane must provide the support for slice isolation, either by means of isolated logical abstractions of the physical hardware devices, in collaboration with the virtualization/control layer, or complete physical isolation if very high levels of security/privacy are required.
	Justification	Multiplexing capabilities (time/frequency/space) and physical diversity must be provided by the data plane to allow for the creation of multiple concurrent isolated network slices. Additionally, proper encapsulation and containers frameworks must be provided to guarantee the isolation integrity at the virtual data layer (FCAPS correlation)
	Novelty	High
	Exploitability	High

REQ_DATA_PLANE_3		
Smart Grid Use Case	Name	Physical/Virtual data plane Information Modelling Support
	Description	The data plane devices and capabilities must be exposed with a sufficiently detailed information model, either in a macroscopic scope (type of device, maximum bandwidth, number of ports, computing capabilities, virtualized function, etc...) or in a more microscopic scope (i.e. technology-dependent parameters).
	Justification	The virtualization of the physical infrastructure and a correct understanding of the capacities to be handled at the physical/virtual data plane are mandatory to enable the provisioning of multiple slices in support of the UCs.
	Novelty	High
	Exploitability	High

eHealth Use Case	Name	Physical/Virtual data plane Information Modelling Support
	Description	The data plane devices and capabilities must be exposed with a sufficiently detailed information model, either in a macroscopic scope (type of device, maximum bandwidth, number of ports, computing capabilities, virtualized function, etc...) or in a more microscopic scope (i.e. technology-dependent parameters).
	Justification	The virtualization of the physical infrastructure and a correct understanding of the capacities to be handled at the physical/virtual data plane are mandatory to enable the provisioning of multiple slices in support of the UCs.
	Novelty	High To support the levels of QoS and QoE required, it is necessary to provide this UC with data plane IMS, which is not currently available in other high bandwidth end2end wireless networks.
	Exploitability	Medium Health service providers will have an expectation that the system is sufficiently flexible to provide additional services, and as such this is seen as a de facto requirement.

REQ_DATA_PLANE_4		
Smart Grid Use Case	Name	Reliability support
	Description	Different physical/virtual resource redundancy/protection strategies should be implemented to provide different reliability levels according to criticality of the slice.
	Justification	The data plane must provide high reliability levels to avoid slice disruptions due to physical or software elements failures.
	Novelty	High
	Exploitability	High
eHealth Use Case	Name	Reliability support
	Description	Different physical/virtual resource redundancy/protection strategies should be implemented to provide different reliability levels according to criticality of the slice.
	Justification	The data plane must provide high reliability levels to avoid slice disruptions due to physical or software elements failures.
	Novelty	High Life saving/critical service differentiators, offering guaranteed QoS and QoE is currently unique.
	Exploitability	High Beneficial to the health sector as a life saving/critical service

REQ_DATA_PLANE_05		
Smart Grid Use Case	Name	Geographical Coverage
	Description	<p>The data plane must provide the necessary physical infrastructure to cover the whole operational area of the expected slice to be configured. Different coverage levels are defined:</p> <ul style="list-style-type: none"> • Very wide: up to hundreds/few thousands of km, for slices requiring country-like range (e.g smart grid). • Wide: up to tens/few hundred of km, for slices requiring regional-like range (e.g. e-health). • Medium/Urban: up to few kilometres, for slice requiring city-like coverage (e.g. smart lighting/cities) <p>The different coverage levels impose restrictions onto the transmission of the network signals, thus, heterogeneous data plane technologies should be provided to offer the desired coverage in the most efficient way.</p>
	Justification	<p>The data plane must provide the necessary physical infrastructure to cover the whole operational area of the slices provisioned.</p> <p>The smart grid self-healing use case may require two different slices: one for time-critical horizontal communications between IEDs, the other for vertical communications between the IEDs and the SCADA system. The former should require wide geographical coverage (IEDs implementing the same self-healing scheme are typically less than 100 km apart); the latter may require very wide geographical coverage (the control center may be located hundreds of km from the IEDs).</p>
	Novelty	Medium
	Exploitability	Medium
eHealth Use Case	Name	Geographical Coverage
	Description	<p>The data plane must provide the necessary physical infrastructure to cover the whole operational area of the expected slice to be configured. Different coverage levels are defined:</p> <ul style="list-style-type: none"> • Very wide: up to hundreds/few thousands of km, for slices requiring country-like range (e.g smart grid). • Wide: up to tens/few hundred of km, for slices requiring regional-like range (e.g. e-health). • Medium/Urban: up to few kilometres, for slice requiring city-like coverage (e.g. smart lighting/cities) <p>The different coverage levels impose restrictions onto the transmission of the network signals, thus, heterogeneous data plane technologies should be provided to offer the desired coverage in the most efficient way.</p>
	Justification	<p>The data plane must provide the necessary physical infrastructure to cover the whole operational area of the slices provisioned.</p>
	Novelty	<p>Medium</p> <p>Wide area coverage to be required in general for this use case, which would be</p>

		expected.
	Exploitability	Medium Health service providers offering emergency services in the field would expect to operate at a wide coverage area.
Smart City Use Case	Name	Geographical Coverage
	Description	The data plane must provide the necessary physical infrastructure to cover the whole operational area of the expected slice to be configured. Different coverage levels are defined: <ul style="list-style-type: none"> • Very wide: up to hundreds/few thousands of km, for slices requiring country-like range (e.g smart grid). • Wide: up to tens/few hundred of km, for slices requiring regional-like range (e.g. e-health). • Medium/Urban: up to few kilometres, for slice requiring city-like coverage (e.g. smart lighting/cities) The different coverage levels impose restrictions onto the transmission of the network signals, thus, heterogeneous data plane technologies should be provided to offer the desired coverage in the most efficient way.
	Justification	The data plane must provide the necessary physical infrastructure to cover the whole operational area of the slices provisioned.
	Novelty	High, at the city-like level.
	Exploitability	High, at the city level.

REQ_DATA_PLANE_06		
Smart Grid Use Case	Name	Performance Monitoring and Statistics Support of the physical and virtual infrastructure.
	Description	The data plane devices must support statistics generation in order to monitor their health but also the current performance of the slice from multiple perspectives (e.g. packet loss ratio, frame delay, signal-to-noise ratio, computing resource occupation, efficiency of network functions, etc.).
	Justification	The data sets obtained from the monitoring performed at the data plane are employed at the cognition-based management plane for the self-reconfiguration of the slice, to keep, for example, the expected QoE.
	Novelty	High
	Exploitability	High

eHealth Use Case	Name	Performance Monitoring and Statistics Support of the physical and virtual infrastructure.
	Description	The data plane devices must support statistics generation in order to monitor their health but also the current performance of the slice from multiple perspectives (e.g. packet loss ratio, frame delay, signal-to-noise ratio, computing resource occupation, efficiency of network functions, etc.).
	Justification	The data sets obtained from the monitoring performed at the data plane are employed at the cognition-based management plane for the self-reconfiguration of the slice, to keep, for example, the expected QoE.
	Novelty	Low To the service providers offering the service to the health service operator, statistical data plane health data will support SLAs, but this type of data would be normal enough for data networks.
	Exploitability	LowMedium Useful for more detailed SLAs that will be used by digital service providers.
Smart City Use Case	Name	Performance Monitoring and Statistics Support of the physical and virtual infrastructure.
	Description	The data plane devices must support statistics generation in order to monitor their health but also the current performance of the slice from multiple perspectives (e.g. packet loss ratio, frame delay, signal-to-noise ratio, computing resource occupation, efficiency of network functions, etc.).
	Justification	The data sets obtained from the monitoring performed at the data plane are employed at the cognition-based management plane for the self-reconfiguration of the slice, to keep, for example, the expected QoE.
	Novelty	High
	Exploitability	High

REQ_DATA_PLANE_07		
Smart Grid Use Case	Name	Multi-casting Support
	Description	The data plane infrastructure has to support Multicasting capability.
	Justification	By enabling multicast-based connectivity services, massive machine-to-machine communication type patterns across the configured slice are enabled. The smart grid self-healing use case relies on time-critical peer-to-peer communication between IEDs. The protocols used for the D2D communication (IEC 61850 GOOSE and IEC 61850 SV) are multicast-based.
	Novelty	High
	Exploitability	High

eHealth Use Case	Name	Multi-casting Support
	Description	The data plane infrastructure has to support Multicasting capability.
	Justification	By enabling multicast-based connectivity services, the high definition video streaming service can be viewed at multiple end points.
	Novelty	High Streaming high definition video in realtime from inside the ambulance, and offering this service to multiple end points is not currently available.
	Exploitability	Medium Health services providers have communicated this as a medium level requirement.
Smart City Use Case	Name	Multi-casting Support
	Description	The data plane infrastructure has to support Multicasting capability.
	Justification	By enabling multicast-based connectivity services, massive machine-to-machine communication type patterns across the configured slice are enabled.
	Novelty	High Multicast capabilities within slice for the network operator.
	Exploitability	High

REQ_DATA_PLANE_08		
eHealth Use Case	Name	Mobility
	Description	The data plane should support an agile handover and/or resource re-configurability.
	Justification	With mobility support, the capacity of slice end-points to travel across a geographically distributed area in support of high mobility applications is enabled.
	Novelty	Low Handover would be a standard requirement in mobile networks
	Exploitability	High Would be viewed as a standard feature

A.4 Enterprise

REQ_Enterprise_01		
eHealth Use Case	Name	Enterprise Networks
	Description	The main role of the Enterprise networks will be identifying key vertical sectors' requirements, anticipating relevant trends early and mapping them into the 5G design. For the enterprise networks perspective the challenge for 5G is to provide end-to-end network and cloud infrastructure slices over the physical infrastructure in order to fulfil specific requirements for our three use cases: SMARTGRID, EHEALTH and SMARTCITY.
	Justification	The E health use cases centred around ultra high-definition video along with cloud processing and storage. Video will be streamed from emergency situations to a cloud-based application.
	Novelty	High
	Exploitability	High Ultra-High definition video will allow for better patient outcomes.
Smart City Use Case	Name	Enterprise Networks
	Description	The main role of the Enterprise networks will be identifying key vertical sectors' requirements, anticipating relevant trends early and mapping them into the 5G design. For the enterprise networks perspective the challenge for 5G is to provide end-to-end network and cloud infrastructure slices over the physical infrastructure in order to fulfil specific requirements for our three use cases: SMARTGRID, EHEALTH and SMARTCITY.
	Justification	The SmaLi-5G smart city lighting use case is composed by lighting system, network and apps hosted in cloud. A complex UCs scenario requires enterprise approach for 5G context application.
	Exploitability	High Enabling the vertical business sector (at City Hall/partners environment level in Smart City UC) to deploy the Smart Lighting Apps.

REQ_Enterprise_02		
Smart Grid Use Case	Name	Ultra-high network reliability and availability
	Description	Maximum tolerable packet loss rate at the application layer within the maximum tolerable end-to-end latency for that application. The most demanding vertical use cases are related to eHealth and Smart City with values for availability up to 99.999%.
	Justification	Reliability and availability are critical for electric power grid protection, automation, and control.
	Novelty	High
	Exploitability	High
eHealth Use Case	Name	Ultra-high network reliability and availability
	Description	Maximum tolerable packet loss rate at the application layer within the maximum tolerable end-to-end latency for that application. The most demanding vertical use cases are related to eHealth and Smart City with values for availability up to 99.999%. For Ultra-high reliability & Ultra-low latency video <ul style="list-style-type: none"> • 50 to 500ms latency end to end. • 10 ms peak-to-peak jitter • 0.03 to 0.05% random packet loss
	Justification	Allowing clinicians to have a clear uninterrupted high resolution view of patients who are potentially suffering from ischaemic stroke is critical to good outcomes.
	Novelty	High
	Exploitability	High
Smart City Use Case	Name	Ultra-high network reliability and availability
	Description	Maximum tolerable packet loss rate at the application layer within the maximum tolerable end-to-end latency for that application. The most demanding vertical use cases are related to eHealth and Smart City with values for availability up to 99.999%.
	Justification	The Smart City UC generally requires network reliability and availability, even it is not critical as Smart Lighting infrastructure.
	Novelty	Medium
	Exploitability	Medium

REQ_Enterprise_03		
Smart Grid Use Case	Name	Density (number of devices)
	Description	The Enterprise Networks must accommodate a high number of devices (vehicles in the case of Ehealth, sensors in case of the Smart City, IEDs in case of Smart Grid) per unit area that are 5G capable, although they might not all be generating traffic simultaneously for the specified application.
	Justification	The density of communicating IEDs that integrate smart grid self-healing schemes is very low.
	Novelty	Low
	Exploitability	Low
eHealth Use Case	Name	Density (number of devices)
	Description	The Enterprise Networks must accommodate a high number of devices (vehicles in the case of Ehealth, sensors in case of the Smart City) per unit area that are 5G capable, although they might not all be generating traffic simultaneously for the specified application.
	Justification	It is envisaged that low number of devices deployed at any one time.
	Novelty	Low
	Exploitability	Low
Smart City Use Case	Name	Density (number of devices)
	Description	The Enterprise Networks must accommodate a high number of devices (vehicles in the case of Ehealth, sensors in case of the Smart City) per unit area that are 5G capable, although they might not all be generating traffic simultaneously for the specified application.
	Justification	Integration for a large Smart-City lighting system scenario.
	Novelty	High It is envisaged a large number of devices at a city level.
	Exploitability	High Intensive communication at low data rate.

REQ_Enterprise_04		
Smart Grid Use Case	Name	Position Accuracy (Location)
	Description	Enterprise Networks must generate for each of the three use cases a maximum positioning error tolerated by the application.
	Justification	The IEDs installed in the electrical power grid are stationary, and -their location is well known to the power grid operators.
	Novelty	Low
	Exploitability	Low
eHealth Use Case	Name	Position Accuracy (Location)
	Description	Enterprise Networks must generate for each of the three use cases a maximum positioning error tolerated by the application. The most demanding use cases are Ehealth and Smart City.
	Justification	For single patient events it will be important to know the location so that support and vehicle routing functionality may be offered. For multi-patient events it is important to get precise assessment of the geographical location of the incident.
	Novelty	Medium
	Exploitability	Medium Providing high accuracy will be a major value add to emergency crews and controllers.
Smart City Use Case	Name	Position Accuracy (Location)
	Description	Enterprise Networks must generate for each of the three use cases a maximum positioning error tolerated by the application. The most demanding use cases are Ehealth and Smart City.
	Justification	Identification of corresponding lighting systems.
	Novelty	Medium
	Exploitability	Medium

REQ_Enterprise_05		
eHealth Use Case	Name	Mobility (speed)
	Description	Maximum relative speed under which the specified reliability should be achieved. The most demanding use case is eHealth.
	Justification	Providing speed will be a major value add to emergency crews and controllers as time is a critical component.
	Novelty	High

	Exploitability	High
--	-----------------------	------

REQ_Enterprise_06		
Smart Grid Use Case	Name	E2E Latency
	Description	Enterprise Networks must assure a maximum tolerable elapsed time from the instant a data packet is generated at the source application to the instant it is received by the destination application.
	Justification	The smart grid self-healing use case relies on time-critical communications. Low E2E latency and deterministic communications are critical for guaranteeing the good/optimal operation of these algorithms.
	Novelty	High
	Exploitability	High
eHealth Use Case	Name	E2E Latency
	Description	Enterprise Networks must assure a maximum tolerable elapsed time from the instant a data packet is generated at the source application to the instant it is received by the destination application.
	Justification	Quality service and quality of experience will be maintained by low latency, allowing patients to be treated effectively under the instruction of hospital based medics. 50 to 500ms latency end to end. It is important that video and two-way voice communication is highly responsive to assist the paramedics at the scene.
	Novelty	High
	Exploitability	High
Smart City Use Case	Name	E2E Latency
	Description	Enterprise Networks must assure a maximum tolerable elapsed time from the instant a data packet is generated at the source application to the instant it is received by the destination application.
	Justification	The Smart City UC is fulfilled with E2E latency at acceptable values (at hundreds of ms) for proper functioning, as technology requirements.
	Novelty	Low
	Exploitability	Low

REQ_Enterprise_07		
Smart Grid Use Case	Name	Coverage
	Description	Enterprise Networks for each use case must assure an area within which or population for which the application should function correctly (the specified requirements are achieved).
	Justification	The electric power grid covers wide geographical areas that may span across multiple administrative domains.
	Novelty	Medium
	Exploitability	High
eHealth Use Case	Name	Coverage
	Description	Enterprise Networks for each use case must assure an area within which or population for which the application should function correctly (the specified requirements are achieved). The our three use cases have strong requirements on geographic and/or population coverage.
	Justification	Wide geographical coverage is needed to ensure that incidents that occur in any location may be supported.
	Novelty	High
	Exploitability	High Medical emergencies may occur at any location so this feature will be highly exploitable.
Smart City Use Case	Name	Coverage
	Description	Enterprise Networks for each use case must assure an area within which or population for which the application should function correctly (the specified requirements are achieved).
	Justification	The UCs of smart lighting to cover any location within the city.
	Novelty	High Coverage at the city level.
	Exploitability	High

REQ_Enterprise_08		
Smart Grid Use Case	Name	Data Rate
	Description	Required bit rate for the application to function correctly. It corresponds to the user experienced data rate as defined by ITU. Critical in all the use cases with different values.
	Justification	It is critical to provide the necessary data rate for guaranteeing QoS for the time-critical applications and for mission-critical SCADA communications. The provided data rate should also ensure QoE, particularly for manual SCADA operations.
	Novelty	High
	Exploitability	High
eHealth Use Case	Name	Data Rate
	Description	Required bit rate for the application to function correctly. It corresponds to the user experienced data rate as defined by ITU. Critical in all the use cases with different values.
	Justification	High quality video will result in better outcomes for patient treatment. Ultra high definition video require rates ranging from 60 to 150 Mbps
	Novelty	High
	Exploitability	High
Smart City Use Case	Name	Data Rate
	Description	Required bit rate for the application to function correctly. It corresponds to the user experienced data rate as defined by ITU. Critical in all the use cases with different values.
	Justification	The Smart City UC is requiring low rates per device, but is impacted at the level of a city, where thousands of devices communicates simultaneous in a slice.
	Novelty	Medium
	Exploitability	Medium

REQ_Enterprise_09		
eHealth Use Case	Name	Service Deployment Time
	Description	Duration required for setting up end-to-end logical network slices characterized by respective network level needs required for supporting services of each particular use case.
	Justification	Consultation and negotiation will be handled by digital service providers on behalf of end-users. DSPs will configure and deploy the ultrahigh definition

		video ehealth support system
	Novelty	High Services will be deployed and maintained by digital service providers.
	Exploitability	High
Smart City Use Case	Name	Service Deployment Time
	Description	Duration required for setting up end-to-end logical network slices characterized by respective network level needs required for supporting services of each particular use case.
	Justification	The service deployment is handled by the CSP, that plays in this situation also the role of DSP, that will influence the service deployment time.
	Novelty	High Service deployment and functioning based on defined scheduled.
	Exploitability	High

REQ_Enterprise_10		
Smart Grid Use Case	Name	Security and privacy of user`s data
	Description	The enterprise infrastructure must ensure globally the protection of resources and encompassing several dimensions such as authentication, data confidentiality, data integrity and access control
	Justification	Security aspects are critical to smart grid communications. Although confidentiality is not the greatest concern for these applications, availability and integrity are crucial, particularly when using a public communication infrastructure. Authentication and access control are very important for the smart grid. Ensuring that unauthorized users never gain control of the power system equipment is crucial.
	Novelty	High
	Exploitability	High
eHealth Use Case	Name	Security and privacy of user`s data
	Description	The enterprise infrastructure must ensure globally the protection of resources and encompassing several dimensions such as authentication, data confidentiality, data integrity and access control
	Justification	Citizens should be protected under the General data protection regulations
	Novelty	High This will be extremely high for the health use case as citizens should be protected under the General data protection regulations. De-identification, encryption in both transit and rest should be used to protect the privacy of

		patients.
	Exploitability	High This will also be extremely important considering cross domain networks.
Smart City Use Case	Name	Security and privacy of user`s data
	Description	The enterprise infrastructure must ensure globally the protection of resources and encompassing several dimensions such as authentication, data confidentiality, data integrity and access control
	Justification	System protection for different attacker/exploiters (Internal/external).
	Novelty	Medium Secure transmission and application integrity.
	Exploitability	Medium Deployment of secured and controlled Smart City/Smart Lighting application.

REQ_Enterprise_11		
Smart Grid Use Case	Name	Identity
	Description	Characteristic to identify sources of content and recognize entities in the system
	Justification	Devices should be addressable and identifiable to allow for ownership management with automated inclusion in the slices allocated to the organization that deploys the equipment.
	Novelty	Medium
	Exploitability	Medium
eHealth Use Case	Name	Identity
	Description	Characteristic to identify sources of content and recognize entities in the system
	Justification	It will be crucial to accurately identify crews, location and if possible the patient needing treatment.
	Novelty	High All entities should be identified with a globally unique identifier
	Exploitability	High

Smart City Use Case	Name	Identity
	Description	Characteristic to identify sources of content and recognize entities in the system
	Justification	System management and corrective actions to be taken
	Novelty	Medium
	Exploitability	Medium Identification of proper SmaLI-5G poles and lighting system cases

REQ_Enterprise_12		
Smart Grid Use Case	Name	Autonomy and low power consumption
	Description	Time duration for a component in which it is operational without power being supplied. It relates to battery lifetime, battery load capacity and energy efficiency. The system must also assure a low power consumption.
	Justification	During power outages, the IEDs must be able to operate and communicate on battery power for extended time periods.
	Novelty	Medium
	Exploitability	Medium
eHealth Use Case	Name	Autonomy and low power consumption
	Description	Time duration for a component in which it is operational without power being supplied. It relates to battery lifetime, battery load capacity and energy efficiency. The system must also assure a low power consumption.
	Justification	Ultra high definition cameras and deployment vehicles such as drones need to conserve power. Charging ports should be available between intermittent events.
	Novelty	Low
	Exploitability	Low
Smart City Use Case	Name	Autonomy and low power consumption
	Description	Time duration for a component in which it is operational without power being supplied. It relates to battery lifetime, battery load capacity and energy efficiency. The system must also assure a low power consumption.
	Justification	Implementation of use case business requirements of low-power.
	Novelty	High

		Smart City use case is focused on low-power consumption, energy reduction
	Exploitability	Medium

REQ_Enterprise_13		
Smart Grid Use Case	Name	Data Volume
	Description	Measure the quantity of information transferred (downlink and uplink) per time interval over a dedicated area.
	Justification	<p>The 5G must guarantee the minimal bandwidth levels for the smart grid peer-to-peer communications and for the communication with the SCADA system.</p> <ul style="list-style-type: none"> • Event-driven communications (IEC 61850 GOOSE) are time-critical, asynchronous, and must account for sporadic data bursts; • Synchrophasor measurements (IEC 61850 SV) are time-critical and are continuously streamed from/to IEDs; • Communications with the SCADA system are asynchronous and do not have time constraints as demanding as the previous two. These communications include IEC 61850 MMS messages, file transfers, remote engineering operations, and other.
	Novelty	High
	Exploitability	Medium
eHealth Use Case	Name	Data Volume
	Description	Measure the quantity of information transferred (downlink and uplink) per time interval over a dedicated area.
	Justification	High quality live video streams and storage of video will be useful for control, treatment, auditing and debriefing purposes.
	Novelty	High Sustained streams of high definition video at 150 Mbps can be expected for minutes to hours at the time, resulting in very large data volumes that need to be stored and archived.
	Exploitability	High
Smart City Use Case	Name	Data Volume
	Description	Measure the quantity of information transferred (downlink and uplink) per time interval over a dedicated area.
	Justification	Linear data traffic volumes to be measured and analyzed for data patterns statistics.
	Novelty	Medium
	Exploitability	Medium Analytics for system functioning

REQ_Enterprise_14		
Smart Grid Use Case	Name	Ease of deployment and cost efficiency (flexibility in deployment)
	Description	The development on the three enterprise segments corresponding to our use cases must be done in an easy and with an efficient cost.
	Justification	Ease of deployment and cost efficiency are both very relevant for electrical power system owners to consider the use of a public communication infrastructure for their mission-critical communications.
	Novelty	High
	Exploitability	High
eHealth Use Case	Name	Ease of deployment and cost efficiency (flexibility in deployment)
	Description	The development on the three enterprise segments corresponding to our use cases must be done in an easy and with an efficient cost.
	Justification	There will be a large number of distinct end-users such as ambulance providers, ambulance control centres and hospitals who wish to avail of the system.
	Novelty	High Successful rollout of the health connected ambulance use case for high-definition video will be dependent upon ease of deployment
	Exploitability	High
Smart City Use Case	Name	Ease of deployment and cost efficiency (flexibility in deployment)
	Description	The development on the three enterprise segments corresponding to our use cases must be done in an easy and with an efficient cost.
	Justification	Low Costs, fast deployments, fast service provisioning.
	Novelty	High Low cost deployment over large and dense geographical area, flexibility of networks deployments
	Exploitability	High

REQ_Enterprise_15		
Smart Grid Use Case	Name	Interoperability between the three use cases
	Description	Enterprise Networks must identifies the common characteristic, common architectural resources and developments requirements of our three use cases and take into account if this is possible to share the common parts for an easier and cheaper development.
	Justification	QoS and QoE must be guaranteed for the smart grid applications, taking into consideration that it must coexist with other users, devices, and/or applications using the same communication network, such as the ones covered by the eHealth and Smart City use cases.
	Novelty	High
	Exploitability	High
eHealth Use Case	Name	Interoperability between the three use cases.
	Description	Enterprise Networks must identifies the common characteristic, common architectural resources and developments requirements of our three use cases and take into account if this is possible to share the common parts for an easier and cheaper development.
	Justification	There is no direct link between the use cases, however to demonstrate the efficiency of slicing these three use cases should coexist together on the same infrastructure.
	Novelty	High This is one of the core features of slicing whereby diverse use case requirements can be served efficiently over a common infrastructure
	Exploitability	High
Smart City Use Case	Name	Interoperability between the three use cases
	Description	Enterprise Networks must identifies the common characteristic, common architectural resources and developments requirements of our three use cases and take into account if this is possible to share the common parts for an easier and cheaper development.
	Justification	Common enterprise system requirements for UCs.
	Novelty	Medium Identify common characteristic with Smart Grid use case requirements, for QoS/QoE, power, costs model
	Exploitability	Medium

A.5 FCA

REQ_FCA_01		
Smart Grid Use Case	Name	Role functions handled in FCA operations
	Description	The FCA components shall operate on the basis of role-associated capabilities and the set of FCA functions shall be limited by the management roles as defined for Slicenet.
	Justification	In the smart grid use case, the vertical plays the role of Digital Services Consumer (DSC) – the set of FCA functions available to the vertical should be limited accordingly.
	Novelty	High
	Exploitability	High
eHealth Use Case	Name	Role functions handled in FCA operations
	Description	The FCA components shall operate on the basis of role-associated capabilities and the set of FCA functions shall be limited by the management roles as defined for Slicenet.
	Justification	The Digital Services Provider will consume these FCA functions
	Novelty	Low-Medium
	Exploitability	Low-Medium
Smart City Use Case	Name	Role functions handled in FCA operations
	Description	The FCA components shall operate on the basis of role-associated capabilities and the set of FCA functions shall be limited by the management roles as defined for Slicenet.
	Justification	For the Smart City use-case the Digital Service Provider offers the smart lighting slice accordingly to parameters(KPIs), monitor and configure.
	Novelty	Medium FCA operation at DSP/slice level
	Exploitability	Medium

REQ_FCA_04		
Smart Grid Use Case	Name	FCA supporting multi-domain slicing operations
	Description	FCA operations shall be based on the transfer of data across multi-domains whereas the upper layer operator can receive/send data for all underneath/upper cross-domain managed objects associated to NSIs. The agreement between the involved operators is assumed to be in place.
	Justification	The electric power grid covers wide geographical areas that may span across multiple administrative domains.
	Novelty	High
	Exploitability	Medium
Smart City Use Case	Name	FCA supporting multi-domain slicing operations
	Description	FCA operations shall be based on the transfer of data across multi-domains whereas the upper layer operator can receive/send data for all underneath/upper cross-domain managed objects associated to NSIs. The agreement between the involved operators is assumed to be in place.
	Justification	<i>The Smart City UC – Smart Lighting may span multiple administrative domains, at the city level, based on active shared available resources, requiring multi-domain slicing operations.</i>
	Novelty	High Inter-domain FCA
	Exploitability	High Ensuring end-to-end FCA through different administrative-domains, solving HA in multi domain operating scenario.

REQ_CM_01		
Smart Grid Use Case	Name	Configuration of Network Functions and Transport Network
	Description	The Configuration module shall support the configuration of an existing Network Function and Transport Network upon orders received from: <ul style="list-style-type: none"> • Cognitive as per performance monitoring of NSI • API as per orders from Service Customer
	Justification	This may be useful for adapting the slice resources when new communicating devices are added to a smart grid self-healing scheme.
	Novelty	High
	Exploitability	Low

eHealth Use Case	Name	Configuration of Network Functions and Transport Network
	Description	The Configuration module shall support the configuration of an existing Network Function and Transport Network upon orders received from: <ul style="list-style-type: none"> • Cognitive as per performance monitoring of NSI • API as per orders from Service Customer
	Justification	The Digital Service Provider will most likely require an API to setup configs to functions such as use case prioritisation levels.
	Novelty	Low
	Exploitability	Low
Smart City Use Case	Name	Configuration of Network Functions and Transport Network
	Description	The Configuration module shall support the configuration of an existing Network Function and Transport Network upon orders received from: <ul style="list-style-type: none"> • Cognitive as per performance monitoring of NSI • API as per orders from Service Customer
	Justification	Configuration of network functions related to the communications services within the slice.
	Novelty	High
	Exploitability	High

REQ_FM_CM_01		
eHealth Use Case	Name	Priority handling
	Description	The FCA components shall operate following the priority of the NSI, e.g. in case of queued orders, the ones referring to a priority NSI are handled first.
	Justification	The eHealth use case requires priority handling to manage immediate setup of forward path resources, such as video communication links, and any high priority return path links, offering life threatening assistance.
	Novelty	Medium
	Exploitability	High Useful marketing feature for the DSP to be able to say to the HSP that they can offer priority based services

REQ_AM_01		
eHealth Use Case	Name	Metering info objects collection
	Description	The Accounting module in NSS layer shall be able to collect metering info objects, pertaining to the use of resources (e.g. use of memory, CPU, storage), as coming from the underneath VNFs/PNFs/TNs and to transfer them into aggregated data to the upper layers Accounting module (NS, CS).
	Justification	Dependency for business model flexibility.
	Novelty	Low
	Exploitability	Low

REQ_AM_02		
Smart Grid Use Case	Name	e2e accounting bill for the Service Customer
	Description	The Accounting module in the highest layer (either CS or NS) shall be responsible to correlate the info metering objects events, as received from underneath layers (NSS), and to provide a single bill to the Service Customer. The correlation algorithm can also take in input conditions relating to SLA monitoring, e.g. degree of SLA violation. This requirement applies to both Single and Multi-domain slices. For Multi-domain, an off-line agreement between operators is assumed for the exchange of metering data.
	Justification	The accounting bill and SLA must be adjusted to the smart grid requirements. Communication QoS is critical for smart grid applications and should be closely monitored.
	Novelty	High
	Exploitability	High
eHealth Use Case	Name	e2e accounting bill for the Service Customer
	Description	The Accounting module in the highest layer (either CS or NS) shall be responsible to correlate the info metering objects events, as received from underneath layers (NSS), and to provide a single bill to the Service Customer. The correlation algorithm can also take in input conditions relating to SLA monitoring, e.g. degree of SLA violation. This requirement applies to both Single and Multi-domain slices. For Multi-domain, an off-line agreement between operators is assumed for the exchange of metering data.
	Justification	Dependency for business model flexibility.
	Novelty	Low
	Exploitability	Low

Smart City Use Case	Name	e2e accounting bill for the Service Customer
	Description	The Accounting module in the highest layer (either CS or NS) shall be responsible to correlate the info metering objects events, as received from underneath layers (NSS), and to provide a single bill to the Service Customer. The correlation algorithm can also take in input conditions relating to SLA monitoring, e.g. degree of SLA violation. This requirement applies to both Single and Multi-domain slices. For Multi-domain, an off-line agreement between operators is assumed for the exchange of metering data.
	Justification	The DSC receives from DSP (for Smart City UC the operator) one service bill, even the service is single or multi-domain sliced.
	Novelty	High
	Exploitability	High DSC end-to-end accounting

REQ_AM_03		
Smart Grid Use Case	Name	Inter-operator accounting for multi-domain slices
	Description	For the multi-domain slices, the Accounting module in the highest layer (either CS or NS) shall be responsible to aggregate data per administrative domains in order to produce bills for inter-operator accounting purposes. It is assumed an off-line agreement between operators for the exchange of metering data.
	Justification	It is important that inter-operator accounting is ensured by the network operator that provides the network service to the power grid operator.
	Novelty	High
	Exploitability	High
eHealth Use Case	Name	Inter-operator accounting for multi-domain slices
	Description	For the multi-domain slices, the Accounting module in the highest layer (either CS or NS) shall be responsible to aggregate data per administrative domains in order to produce bills for inter-operator accounting purposes. It is assumed an off-line agreement between operators for the exchange of metering data.
	Justification	Dependency for business model flexibility.
	Novelty	Low
	Exploitability	Low

A.6 MEC

REQ_MEC_01		
eHealth Use Case	Name	Performance (QoS/QoE) requirements support
	Description	MEC should help in meeting the end-to-end performance (QoS/QoE) requirements from the verticals' use cases in terms of bandwidth/throughput, end-to-end delay, jitter, packet loss ratio (or bit error rate) etc., which will be used to programme the data plane and to inform the definition of a set of rules and requirements associated with the use case specific MEC Apps.
	Justification	It is vital for the health use case that the mobile edge provides sufficient computing resources to enable machine learning assessment of video frames captured by paramedics at the location. We have developed support vector machine software that can help assess patient's demeanour and we wish to provide this analysis as close to the edge as possible to enable accurate and effective support for paramedics on the scene and to send summary information to clinicians at the awaiting emergency department. Moreover, edge processing can dramatically compress the data and allow us to highlight frames and image segments that are of most interest to the use case.
	Novelty	High There is a high level of novelty for the use of MEC in this use case. One IEEE paper has already been published on the topic.
	Exploitability	High There is high potential for significant benefits in terms of patient outcome for this use case.
Smart City Use Case	Name	Performance (QoS/QoE) requirements support
	Description	MEC should help in meeting the end-to-end performance (QoS/QoE) requirements from the verticals' use cases in terms of bandwidth/throughput, end-to-end delay, jitter, packet loss ratio (or bit error rate) etc., which will be used to programme the data plane and to inform the definition of a set of rules and requirements associated with the use case specific MEC Apps.
	Justification	The Smart City UC does not requires MEC Apps for Smart Lighting.
	Novelty	Low
	Exploitability	Low

REQ_MEC_02		
Smart Grid Use Case	Name	Security requirements support
	Description	MEC should help in managing the security and privacy required by certain use cases.
	Justification	Although confidentiality is not critical for this specific application, the network slicing system compliancy with cybersecurity requirements is crucial, since the envisioned solution for the protection and control implementation in Smart Grids relies on critical communications (device to device and with the SCADA system). This is particularly relevant when the solution is implemented based in public communications networks. Since a high level of availability and data integrity must be ensured, safe transmission path selection and encryption for data integrity are critical.
	Novelty	High
	Exploitability	High
eHealth Use Case	Name	Security requirements support
	Description	MEC should help in managing the security and privacy required by certain use cases.
	Justification	Mobile edge computing is vitally important to provide as secure and privacy aware digital services to paramedics trying to ascertain patient condition at the scene of an emergency. Under GDPR guidelines it is crucial that informed consent is given by patients where identifying data are captured. By providing mobile edge computing it would be possible to obfuscate identifying features of patients thereby ensuring their privacy. Moreover, edge computing can be leveraged provides high levels of encryption to ensure that data is transmitted and stored securely.
	Novelty	High This use case would present novel uses for privacy and security aware mobile edge computing.
	Exploitability	High Using mobile edge computing to ensure privacy and security will deliver enormous benefits to digital service providers who are trying to commercialize this technology across Europe.

REQ_MEC_03		
eHealth Use Case	Name	Specific Use-Case Driven Requirements for MEC Apps and their availability
	Description	A catalogue with the description of all the required and/or desired applications to be run in the MEC host(s) for a 5G vertical user. The description should include the purpose of the App and the performance (QoS/QoE) and security requirements for that App. Examples may include eHealth Apps to process patients' visual info at the edge (rather than in the connected ambulance or in the hospital platform), video processing Apps, IoT Apps, and any other QoE Apps to offer functionality aiming at addressing any close-to-device processing. The App software availability should be specified and links be given if possible.
	Justification	The main application to be run at the mobile edge will be the patient tracking software developed by the Sigma group at the Cork Institute of Technology. A paper on the system is currently being published through the conference proceedings of the BIBM IEEE conference. This application uses modules for vision processing and support vector machine analysis.
	Novelty	High
	Exploitability	High

REQ_MEC_04		
eHealth Use Case	Name	MEC Apps lifecycle and package management support
	Description	A 5G vertical user should be allowed to indicate how their use case specific Apps running in the MEC host(s) should be managed, and/or may be allowed to manage the lifecycle of Apps themselves via a user application lifecycle management proxy. Lifecycle and package management of Apps may include Apps on-boarding, querying, enabling, disabling, deleting, instantiating, terminating, and maybe relocating Apps in and out of the MEC system etc.
	Justification	Digital service providers should be allowed to deploy mobile edge computing services to health end-user customers. Containerisation could be used to facilitate deployment to edge computing resources. Digital service providers can develop business models whereby customers will be charged for invoking mobile edge computing support. It would be important to be able to segment the market and offer value-added services to the health stakeholders on a case-by-case basis. Offering life-cycle support to digital service providers will facilitate this.
	Novelty	High
	Exploitability	MEC Apps lifecycle and package management support

REQ_MEC_05		
eHealth Use Case	Name	MEC mobility support
	Description	MEC should take into account mobility support requirements for certain use cases, e.g., the mobility of the 5G vertical user may lead to the involvement of additional/new MEC hosts (servers) belonging to the same edge or different edges of the 5G network. Technologies include VM migration and inter-DU/CU (BBU) handover may be required.
	Justification	It will be vitally important to facilitate mobility in the health use case, as emergencies can occur anywhere across a wide geographical location. Containerisation would be the best mechanism to facilitate this as Dockerised compute components could be deployed to the mobile edge computing resources closest to the medical emergency incident.
	Novelty	High
	Exploitability	High

REQ_MEC_06		
Smart Grid Use Case	Name	Multiple 5G operators support
	Description	The MEC platform may need to support scenarios where multiple 5G operators are involved.
	Justification	It may be necessary to resort to multiple 5G operators in order to ensure coverage and signal strength/quality in all the geographical areas reached by the electrical power grid. Multiple 5G operators support may be necessary to deal with the scheduling and synchronization of communications, since the devices may be spread across wide areas due to the typical wide area coverage of the Smart Grid. Both for protection coordination and for differential protection, and regardless of the implemented architecture, peer-to-peer communications between IEDs and with the substation controller or the control centre must be seamless.
	Novelty	High
	Exploitability	Medium
eHealth Use Case	Name	Multiple 5G operators support
	Description	The MEC platform may need to support scenarios where multiple 5G operators are involved.
	Justification	On engaging with clinical stakeholders it was agreed that medical emergencies can occur anywhere across a wide geographical area, therefore it will be necessary to invoke the support from multiple 5G operators to ensure continued delivery of video streams to awaiting clinicians. However on a pilot basis it may be reasonable to target a single operator in the first instance and later if possible see if multi-domain support is feasible.

	Novelty	High
	Exploitability	High

REQ_MEC_07		
Smart Grid Use Case	Name	MEC services support
	Description	An MEC service is a service provided and consumed either by the MEC platform or an MEC App. Potential required services may include Radio Network Information (e.g., RAN conditions), Location (user location information), Traffic Engineering (traffic redirection etc.) etc.
	Justification	It may be useful to take advantage of MEC services for optimizing both the D2D communications and the communication with the SCADA system. MEC services may also be useful for improving/guaranteeing QoS under harsh network conditions, by allowing applications to react to and attempt to fix or mitigate network problems.
	Novelty	High
	Exploitability	Medium
eHealth Use Case	Name	MEC services support
	Description	An MEC service is a service provided and consumed either by the MEC platform or an MEC App. Potential required services may include Radio Network Information (e.g., RAN conditions), Location (user location information), Traffic Engineering (traffic redirection etc.) etc. It would be highly useful to access mobile edge computing services such as user location information and traffic engineering data in order to optimise and adapt the service to end users.
	Justification	Having access to location data would be highly valuable for ambulance emergency controllers in order to coordinate responses to incidents and route patients the most suitable service.
	Novelty	High
	Exploitability	High

A.7 One Stop API

REQ_ONE_STOP_API_01		
Smart Grid Use Case	Name	Layering/Role Support
	Description	The sliceable infrastructure is expected to be layered according either to the initial architecture concept or to any refined version of it. On the other hand the roles identified by the ALB proposal may be also used to identify which roles the vertical is expected to request/utilise and which roles the slice owner will provide on its own. E.g. a vertical may require subnetwork resources or communication services. The OSA (One Stop API) must provide the means to define which layers/roles a vertical requires.
	Justification	In this context, electric power utilities (power grid operators) are digital service customers.
	Novelty	High
	Exploitability	Low
eHealth Use Case	Name	Layering/Role Support
	Description	The sliceable infrastructure is expected to be layered according either to the initial architecture concept or to any refined version of it. On the other hand the roles identified by the ALB proposal may be also used to identify which roles the vertical is expected to request/utilise and which roles the slice owner will provide on its own. E.g. a vertical may require subnetwork resources or communication services. The OSA (One Stop API) must provide the means to define which layers/roles a vertical requires.
	Justification	Digital service providers will be the main conduit through which slice net layered functionality will be deployed. The main use case will be centred around ultra high-definition video in simplex mode and voice communication and full duplex mode. Layers should be configured to support quality of service for this communication. The digital service provider will access a one-stop shop/portal to procure and configure the services.
	Novelty	High
	Exploitability	High
Smart City Use Case	Name	Layering/Role Support
	Description	The sliceable infrastructure is expected to be layered according either to the initial architecture concept or to any refined version of it. On the other hand the roles identified by the ALB proposal may be also used to identify which roles the vertical is expected to request/utilise and which roles the slice owner will provide on its own. E.g. a vertical may require sub-network resources or communication services. The OSA (One Stop API) must provide the means to define which layers/roles a

		vertical requires.
	Justification	The Smart City Smart Lighting UC is the customer requiring communication services from the DSP(in this case telco operator)
	Novelty	High
	Exploitability	Medium

REQ_ONE_STOP_API_02		
Smart Grid Use Case	Name	Geographical coverage support
	Description	The OSA must provide the means for the definition of geographical coverage constraints that have to be satisfied.
	Justification	It would be important to define the geographical area for each self-healing application. The power system devices are spread-out over large areas, but are stationary – the geographical boundaries for each scheme should not be hard to define. This could be used for determining the coverage by the different network operators.
	Novelty	Medium
	Exploitability	High
eHealth Use Case	Name	Geographical coverage support
	Description	The OSA must provide the means for the definition of geographical coverage constraints that have to be satisfied.
	Justification	The E-health use case scenario centred around the connected ambulance concept and paramedics with wearable ultra high definition video cameras providing hospital-based assistance in the event of emergencies. These emergencies can occur within any geographical location is the coverage so it is paramount that quality of service provided across a wide geographical area.
	Novelty	High High-quality ultra high-definition video over a wide geographical area will be a novelty, particularly where it involves switching of domains
	Exploitability	Geographical coverage support

Smart City Use Case	Name	Geographical coverage support
	Description	The OSA must provide the means for the definition of geographical coverage constraints that have to be satisfied.
	Justification	All the Smart City involved objects are fix within the geographical area, so even the coordinates are well known, the OTA may give support to slice definition at the edge of the network (Next Generation Radio)
	Novelty	High Resources allocation for slicing supporting
	Exploitability	Medium

REQ_ONE_STOP_API_03		
eHealth Use Case	Name	Logical topology support
	Description	Similar to the physical topology constraints the OSA must provide the means for the definition of physical topology constraints that have to be satisfied. Logical topology aspects must be based on the topological aspects of the various layers a slice might be consisting of.
	Justification	It would be important for SliceNet to select the optimal topology for low latency communication.
	Novelty	High There will be high novelty by allowing topology to be configured across domains
	Exploitability	High
Smart City Use Case	Name	Logical topology support
	Description	Similar to the physical topology constraints the OSA must provide the means for the definition of physical topology constraints that have to be satisfied. Logical topology aspects must be based on the topological aspects of the various layers a slice might be consisting of.
	Justification	Logical topology correlated with physical topology may be chained as a set of NE(VNFs)
	Novelty	High
	Exploitability	High

REQ_ONE_STOP_API_04		
Smart Grid Use Case	Name	Performance requirements support
	Description	The layered slice model must identify performance metrics and KPIs per layer. Aspects like bandwidth, reliability, latency should be possible to be defined via the OSA.
	Justification	Communication performance and reliability are critical for this application. It must be possible to define these parameters in the OSA. There should also be a way of knowing how some of the slice resources/ performance options will be affected by other feature choices (e.g., maybe if you choose to have data encryption or redundancy you will not be able to ensure the same latency values that you would without these features).
	Novelty	High
	Exploitability	High
eHealth Use Case	Name	Performance requirements support
	Description	The layered slice model must identify performance metrics and KPIs per layer. Aspects like bandwidth, reliability, latency should be possible to be defined via the OSA.
	Justification	Low latency service delivery should be available at the data plane with sufficient available bandwidth to maintain minimal video quality.
	Novelty	High
	Exploitability	High
Smart City Use Case	Name	Performance requirements support
	Description	The layered slice model must identify performance metrics and KPIs per layer. Aspects like bandwidth, reliability, latency should be possible to be defined via the OSA.
	Justification	Performance metrics & KPIs are defined per layer in the DSP (telco operator) through OTA, with a service catalogue support and may be correlated with FCA_X requirements.
	Novelty	High One-stop service parameter defining in the DSP
	Exploitability	High

REQ_ONE_STOP_API_05		
Smart Grid Use Case	Name	Security requirements support
	Description	The layered slice model must identify security aspects per layer. Aspects like data encryption, integrity, isolation, etc. should be possible to be defined via the OSA.
	Justification	<p>Security aspects are critical to smart grid communications. Although confidentiality is not the greatest concern for these applications, availability and integrity are crucial, particularly when using a public communication infrastructure.</p> <p>Some of the cybersecurity threats that can be more critical for these applications are:</p> <ul style="list-style-type: none"> • Denial of service; • Man-in-the-middle attacks; • Replay attacks. <p>Some of these threats can be mitigated by encrypting the data exchanged by IEDs and exchanged by the IEDs and the SCADA system.</p> <p>Since data encryption is computationally heavy and confidentiality is not as important as speed for this application, a solution based on encrypted hashes is adequate.</p> <p>The OSA should provide several cybersecurity features from which the slice customer could select the more adequate options for their application.</p> <p>If security features affect the communication performance, this should be visible to the DSC.</p>
	Novelty	High
	Exploitability	High
eHealth Use Case	Name	Security requirements support
	Description	The layered slice model must identify security aspects per layer. Aspects like data encryption, integrity, isolation, etc. should be possible to be defined via the OSA.
	Justification	Must meet GDPR compliance.
	Novelty	High
	Exploitability	High
Smart City Use Case	Name	Security requirements support
	Description	The layered slice model must identify security aspects per layer. Aspects like data encryption, integrity, isolation, etc. should be possible to be defined via the OSA.
	Justification	Security within the Smart City Smart Lighting UC based on defined security aspects (integrity, isolation, etc) responding to different attacks are necessary, correlated with Security UC_Req, level of security defined through API, at the authorization level of accessing the slice(username/passwords, 2FA), communication with the slice(encryption, hashing), VNFs chaining

		communication level(security groups), protocols, integrated with the management plane.
	Novelty	High
	Exploitability	High

REQ_ONE_STOP_API_06		
Smart Grid Use Case	Name	End devices support
	Description	End devices (i.e. sensors) can be a defining aspect of a slice. Therefore end devices should be possible to be identified for automated inclusion in slices. OSA should allow identification of end devices either by use of specific unique IDs (IMEI/SIM) or by any other workflow (pairing, NFC, location based). Once identified end devices should be clearly addressable.
	Justification	All IEDs that are part of the self-healing schemes should use unique IDs and should be clearly addressable.
	Novelty	High
	Exploitability	Medium
eHealth Use Case	Name	End devices support
	Description	End devices (i.e. sensors) can be a defining aspect of a slice. Therefore end devices should be possible to be identified for automated inclusion in slices. OSA should allow identification of end devices either by use of specific unique IDs (IMEI/SIM) or by any other workflow (pairing, NFC, location based). Once identified end devices should be clearly addressable.
	Justification	The system must support pairing with wifi and Bluetooth enabled devices.
	Novelty	Medium
	Exploitability	Medium

REQ_ONE_STOP_API_07		
Smart Grid Use Case	Name	Redundancy support
	Description	OSA should support definition of redundancy aspects per slice layer.
	Justification	Availability and reliability are critical for smart grid self-healing. Redundancy could help and may even prove necessary for reaching the required levels of availability/reliability for these applications. If redundancy affects the communication performance, this should be visible to the DSC.
	Novelty	High

	Exploitability	High
eHealth Use Case	Name	Redundancy support
	Description	OSA should support definition of redundancy aspects per slice layer.
	Justification	Sufficient redundancy must be provided to support quality of service high-definition video simplex communication with full duplex voice.
	Novelty	High
	Exploitability	High
Smart City Use Case	Name	Redundancy support
	Description	OSA should support definition of redundancy aspects per slice layer.
	Justification	High Availability (including resiliency/redundancy) at the DSP, that will be reflected in the DSP (telco operator), by defining sets of “parameters” for service resiliency/redundancy: ex: VNFs replicated, rules of accessing the back-up slice network in case of primary slice network failure
	Novelty	High
	Exploitability	High

REQ_ONE_STOP_API_08		
Smart Grid Use Case	Name	Mesh and ad-hoc networking support
	Description	Decentralized mesh networking should be supported by the OSA.
	Justification	This option should be available, but it will probably not be used for this application since the device geographical distribution is very sparse and they are often located in remote rural areas, where there are not many access points.
	Novelty	High
	Exploitability	Low
eHealth Use Case	Name	Mesh and ad-hoc networking support
	Description	Decentralized mesh networking should be supported by the OSA.
	Justification	Nesh networking may not be needed by this use case but need to be explored further
	Novelty	Low
	Exploitability	Low

REQ_ONE_STOP_API_09		
Smart Grid Use Case	Name	Event and policy support
	Description	For a given layered slice, OSA should offer the possibility for the definition of event processing workflows for the enforcement of certain policies (e.g. configuration of slice components depending on metrics or events).
	Justification	One possible application would be the automatic adjustment of slice resources according to the number of devices integrating the self-healing scheme (n.b., not all communicating devices are part of the self-healing scheme – this number cannot be determined automatically, it must be provided by the DSC). This feature could reduce communication costs by not allocating network resources while they are not needed.
	Novelty	High
	Exploitability	Low
eHealth Use Case	Name	Event and policy support
	Description	For a given layered slice, OSA should offer the possibility for the definition of event processing workflows for the enforcement of certain policies (e.g. configuration of slice components depending on metrics or events).
	Justification	Network congestion events should be detected and the network configured resolve.
	Novelty	High
	Exploitability	High
Smart City Use Case	Name	Event and policy support
	Description	For a given layered slice, OSA should offer the possibility for the definition of event processing workflows for the enforcement of certain policies (e.g. configuration of slice components depending on metrics or events).
	Justification	Event and policy support applicable at DSP level, correlated with FCA_X, that will requests configuration services at slice chaining components, requiring resources (memory, CPU).
	Novelty	High OSA support for the UCs functionality approach, programmability and automation for required resources
	Exploitability	High

REQ_ONE_STOP_API_10		
Smart Grid Use Case	Name	Resource dimensioning/scaling support
	Description	For a given layered slice, OSA should offer the possibility for the definition of the number of required resources that have to be allocated. Otherwise, the resources are calculated on the basis of the identified performance, topology, etc. requirements.
	Justification	The number of connected devices is limited and can be provided by the customer (electrical power utility). It must be possible to increase the number of devices and consequently increase the amount of used resources over time.
	Novelty	Low
	Exploitability	Medium
eHealth Use Case	Name	Resource dimensioning/scaling support
	Description	For a given layered slice, OSA should offer the possibility for the definition of the number of required resources that have to be allocated. Otherwise, the resources are calculated on the basis of the identified performance, topology, etc. requirements. Resources could be calculated based on requirements defined by the digital service provider.
	Justification	Scaling would be needed for multi-patients events.
	Novelty	Medium
	Exploitability	Medium

REQ_ONE_STOP_API_11		
eHealth Use Case	Name	Mobility constraints support
	Description	OSA should allow for the definition of mobility constraints that may be required at specific slice layers
	Justification	Maximum mobility should be provided in jurisdictions defined by the service provider. Privacy and security may offer constraints.
	Novelty	Low
	Exploitability	High

REQ_ONE_STOP_API_12		
Smart Grid Use Case	Name	Resource sharing
	Description	OSA should allow for the definition whether resource allocation should to be in a shared or dedicated mode
	Justification	This option should be made available to the power system operator. Some may require dedicated resources for smart grid applications. In the cases resource sharing is allowed, QoS and QoE must be guaranteed. This would likely require prioritizing certain types of traffic (IEC 61850 SV and GOOSE messages should have the highest priority).
	Novelty	Medium
	Exploitability	High
eHealth Use Case	Name	Resource sharing
	Description	OSA should allow for the definition whether resource allocation should to be in a shared or dedicated mode
	Justification	Sharing would be acceptable as long as the quality of service is maintained.
	Novelty	High
	Exploitability	Medium Would be relevant if DSPs target a number of verticles/customers.

REQ_ONE_STOP_API_13		
eHealth Use Case	Name	Communication scheduling and startup latency
	Description	OSA should allow for the definition of scheduled communications to eliminate delays due to startup processes for scheduled communications (schedules should be adjustable).
	Justification	Would be important to minimize the start-up time for emergency scenarios.
	Novelty	High
	Exploitability	High

A.8 Security

REQ_SECURITY_01		
Smart Grid Use Case	Name	Slice isolation
	Description	<p>The SliceNet framework MUST provide</p> <ul style="list-style-type: none"> • Slice Isolation & Availability • Enhanced encryption • Policy
	Justification	<ul style="list-style-type: none"> • Slice Isolation & Availability <p>Slices instantiated for the UC must be sufficiently isolated to prevent access to smart grid data to unauthorized parties.</p> <p>Further, as a critical service, the smart grid slice instances must guarantee that the service is not disrupted by resource contention, DoS attacks or infrastructure failure.</p> <p>To achieve these goals an effective security management layer is required as well as mechanisms to monitor the state of the deployed security mechanisms (service assurance). Management and service assurance solutions must involve all operators/domains over which the slice is deployed.</p> <ul style="list-style-type: none"> • Enhanced encryption <p>Network layer traffic tagging (VLAN, MPLS, VXLAN) with associated traffic shaping may provide the baseline isolation of the slice networking. However, an additional layer of isolation may be necessary, in the form of end-2-end encrypted communication channels between slice elements that process critical data.</p> <p>Since data encryption is computationally heavy and confidentiality is not as important as speed for this application, a solution based on encrypted hashes is adequate.</p> <p>This functionality may be provided as an add-on service, e.g, though specialized VNFs, controlled through the slice management layer.</p>
	Novelty	High
	Exploitability	High
Smart City Use Case	Name	Slice isolation
	Description	<p>The SliceNet framework MUST provide</p> <ul style="list-style-type: none"> • Slice Isolation & Availability <p>Slices instantiated for the UC must be sufficiently isolated to prevent exposure of privacy sensitive patient data to unauthorized parties.</p> <p>Further, as a critical service, the e-Health slice instance must guarantee that the service is not disrupted by resource contention, DoS attacks or infrastructure failure.</p> <p>To achieve these goals an effective security management layer is required as well as mechanisms to monitor the state of the deployed security mechanisms (service assurance). Management and service assurance solutions must involve all operators/domains over which the slice is</p>

		<p>deployed.</p> <ul style="list-style-type: none"> Enhanced encryption Network layer traffic tagging (VLAN, MPLS, VXLAN) with associated traffic shaping may provide the baseline isolation of the slice networking. However, an additional layer of isolation may be necessary, in the form of end-2-end encrypted communication channels between slice elements that process sensitive data. This functionality may be provided as an add-on service, e.g, though specialized VNFs, controlled through the slice management layer. Policy The security component of slice management layer must be able to account for applicable regulatory requirements with respect to data encryption, data storage and processing. This includes ACL for generated content, geographical locations of processing VNFs and data storage and interfaces to functions specific to the e-Health domain.
	Justification	The E2E security concepts are mandatory for the UC scenario as it will be assured the safe system functioning, at DSP and CSP level.
	Novelty	Medium
	Exploitability	High

REQ_SECURITY_02		
Smart City Use Case	Name	Isolation and availability at scale
	Description	Key requirements for the Smart Lighting UC is availability and isolation of the slice. A particular challenge in this context is the large scale of the UC. Thus, the employed methods for securing the communications with smart lighting devices and the associated access control mechanisms must efficiently scale to potentially millions of entities managed within a slice.
	Justification	The secured smart-lighting slice isolation is impacting the technical approach for UC implementation in terms of availability.
	Novelty	High Proper smart lighting system request system availability and performance, provided also from communication security, extended to wide areas.
	Exploitability	High HA through secure sliced network, responding to system functioning requirements

REQ_SECURITY_03		
Smart Grid Use Case	Name	Slice integrity and low latency communications
	Description	<ul style="list-style-type: none"> • Availability Availability aspects are common with all UCs. • Integrity Integrity features may be implemented as an add-on service as specialized VNF. This includes the selection of a trusted communication paths and the assurance/monitoring of the configured mechanisms. • Low latency The UC requires message forwarding with low latency and accurate timing requirements. To this end, the employed encryption schemes and mechanisms for ensuring the data integrity must be implemented in a way that doesn't impose a significant penalty on performance. • Protection against cyber attacks As a critical infrastructure, the slice isolation must provide mechanisms to detect and mitigate cyber-attacks. These may include hooks for analyzing network traffic using Intrusion Detection Systems (IDS) and similar threat detection product. The associated monitoring interfaces must be compatible with any deployed data integrity mechanisms, without limiting the performance (low latency) of the elements deployed within the UC slice.
	Justification	Provide secured digital communication services
	Novelty	High
	Exploitability	High
Smart City Use Case	Name	Slice integrity and low latency communications
	Description	<p>In terms of secure communications, the Smart City UC favours availability and data integrity over confidentiality (1st: availability; 2nd: integrity; 3rd: confidentiality).</p> <ul style="list-style-type: none"> • Availability Availability aspects are common with all UCs. • Integrity Integrity features may be implemented as an add-on service as specialized VNF. This includes the selection of a trusted communication paths and the assurance/monitoring of the configured mechanisms. • Low latency The UC requires message forwarding with low latency and accurate timing requirements. To this end, the employed encryption schemes and mechanisms for ensuring the data integrity must be implemented in a way that doesn't impose a significant penalty on performance. • Protection against cyber attacks

		As a critical infrastructure, the slice isolation must provide mechanisms to detect and mitigate cyber-attacks. These may include hooks for analyzing network traffic using Intrusion Detection Systems (IDS) and similar threat detection product. The associated monitoring interfaces must be compatible with any deployed data integrity mechanisms, without limiting the performance (low latency) of the elements deployed within the UC slice.
	Justification	Provide secured digital communication services
	Novelty	High The Smart City UC is requiring availability, integrity through protection from different cyber security attacks addressing the integrity of the slice within digital service provider.
	Exploitability	High

A.9 Plug and Play

REQ_PLUG_AND_PLAY_01		
Smart Grid Use Case	Name	Slice Control Exposure
	Description	The SliceNet P&P Control MUST provide specific means to monitor the slice instance KPIs, mostly in terms of performances and resources availability. In the context of the SliceNet SmartGrid use case, the control and management of a slice instance is not foreseen to be directly operated by the vertical, while it should be fully mandated to the network operator or slice provider, leveraging on its own cognitive based mechanisms and procedures.
	Justification	The SmartGrid use case proposed in SliceNet does not rely on the use of proprietary network functions for its self-protection effectiveness, although this option may be useful for other smart grid applications. Therefore the minimum set of P&P Control functions required by the SmartGrid use case refers to the possibility to monitor the slice instance status and behaviour.
	Novelty	High
	Exploitability	Medium
eHealth Use Case	Name	Slice Control Exposure
	Description	The SliceNet P&P Control MUST offer to the slice digital service provider primitives and APIs to access the design and composition of network slice instances on the one hand, and the operation, configuration and lifecycle management of network functions (including proprietary ones) on the other. The P&P control MUST also offer slice instance performance KPIs to allow the slice consumer monitor the status of its own slices.
	Justification	A balance must be struck between scope of functionality and ease-of-use. The P&P functionality will be offered by a digital service provider (i.e. slice provider) who engaged with the key health end-user stakeholders. Monitoring of KPIs will be essential. The ability to deploy network functions to the edge of the network will also be useful to these stakeholders.

	Novelty	High Control of the slice will provide high novelty to stakeholders in the health sector.
	Exploitability	High Digital service providers will be able to exploit this by offering bespoke plug and play solutions that can provide enhanced network functionality.
Smart City Use Case	Name	Slice Control Exposure
	Description	The SliceNet P&P Control MUST provide access to slice instance general system KPIs to allow slice consumers to monitor performances and availability of end-to-end slices in real-time. It is envisaged that the Smart City use case, and in particular the Smart Lighting scenario, does not require the slice consumer (e.g. the city council or light distribution company) to have direct control or management slice instance resources and lifecycle.
	Justification	The Smart City use case aims to migrate current LoRaWAN implementation of the Smart Lighting scenario towards a full end-to-end 5G architecture. Most of the network functions needed to realize and operate the Smart Lighting slices in the 5G environment will be own and managed by the slice provider (virtual EPC, network traffic monitoring, loading state functions, etc.). A basic level of control exposure is therefore required by slice consumers, who mostly will need to monitor the slice status and performance and manage their services accordingly.
	Novelty	Medium
	Exploitability	Medium

REQ_PLUG_AND_PLAY_02		
Smart Grid Use Case	Name	Onboarding of proprietary sensing/monitoring functions
	Description	The SliceNet P&P Control SHOULD offer dedicated primitives to allow the vertical actor onboard and operate proprietary functions capable to expose application-specific metrics. These functions could be integrated and composed as part of slice instances, aiming at supporting and providing to the network operator or slice provider additional and vertical-specific KPIs to monitor QoS and QoE.
	Justification	The SmartGrid self-protection procedures proposed in SliceNet rely on specific and standard-based network communications among IEDs and SCADA's functions. The vertical actor, e.g. the power distribution company, could provide dedicated functions exposing application-specific metrics for these communications (e.g., GOOSE failure indication, out-of-order packet indication) as a mean to support the cognitive techniques of the slice provider or network operator.
	Novelty	High

	Exploitability	Medium
eHealth Use Case	Name	Onboarding of proprietary network function(s)
	Description	The SliceNet P&P Control MUST provide the possibility to onboard proprietary network functions offered by the slice consumer (e.g. the health service provider), and instantiate and compose them within slice instances.
	Justification	The slice consumer, in the context of the eHealth use case, could have its own network functions for specific eHealth services and purposes to be chained in the end to end slice instance, like network functions for i) patient facial recognition and demeanour and ii) control/management of the BluEye technology and remote camera platform technology in the connected ambulance case. The P&P control MUST allow to onboard, instantiate and use them to monitor the demeanour of patients using machine learning algorithms deployed at the edge.
	Novelty	High This will represent high novelty as there will be smart functionality available for the health scenarios at the edge.
	Exploitability	Medium Digital service providers will be able to offer this as a value-added service to health service providers
Smart City Use Case	Name	Onboarding of proprietary monitoring functions
	Description	The SliceNet P&P Control COULD expose dedicated primitives to let the slice consumer onboard and operate proprietary network functions providing additional KPIs coming from the application or vertical specific space. The aim of these functions is to aid the slice provider monitoring and cognitive mechanisms with application-specific KPIs.
	Justification	In the scenario of the Smart Lighting, the slice consumer (e.g. the light distribution company or the city council) might own application-specific virtualized functions/applications for monitoring of vertical-proprietary KPIs. For Smart Lighting these could be specific virtualized functions for lighting poles reachability state (typically part of the lighting solution management platform in the state-of-the-art) that if integrated in the slice instances (i.e. onboarded and instantiated as part of the end-to-end slice) could enhance the slice provider monitoring and cognitive functions with the aim of improving QoS and QoE management.
	Novelty	High
	Exploitability	Medium

REQ_PLUG_AND_PLAY_03		
Smart Grid Use Case	Name	Access to runtime configuration of proprietary sensing/monitoring functions
	Description	The SliceNet P&P Control SHOULD offer the possibility to directly operate the proprietary functions provided, at least in term of runtime configuration. This allows to properly adapt these functions following the dynamics of the SmartGrid, e.g. when new IEDs are deployed in the grid (or when the grid is expanded in general).
	Justification	When the slice consumer, e.g. the power distribution company, onboard its own functions for sensing or monitoring purposes, it is highly recommended that it could have access to their operation to apply the proper configuration logics (e.g. in the case of GOOSE or MMS case) and ensure to fully benefit from their integration and composition in end to end slice instances.
	Novelty	High
	Exploitability	Low
eHealth Use Case	Name	Access to runtime configuration of proprietary network function(s)
	Description	The SliceNet P&P Control MUST provide access to the runtime configuration of those proprietary network functions instantiated as part of end to end slices, offering to the slice consumer full control of their specific technology and logic.
	Justification	Specific eHealth proprietary network functions will need to be configured and operated following proper and specific procedures and mechanisms, which follow logics known by the slice consumers only (having them the required health-care background).
	Novelty	High This will represent high novelty as there will be smart functionality available for the health scenarios at the edge.
	Exploitability	High Digital service providers will be able to offer this as a value-added service.
Smart City Use Case	Name	Access to runtime configuration of proprietary monitoring functions
	Description	The SliceNet P&P Control COULD expose specific primitives to let the slice consumer operate the proprietary functions onboarded and instantiated as part of end-to-end slices. This could limit to access to runtime configuration of the application-specific monitoring functions. This way, in the case of the Smart Lighting scenario, the slice consumer could have enough control over these functions allowing to apply the proper logics following the dynamicity of the lighting management systems.
	Justification	In the specific case of proprietary functions provided by the slice consumer and integrated as part of end-to-end slice instances, it is preferable that their operation and configuration is directly controlled by the slice consumer itself to fully exploit its knowledge of the vertical applications space, and thus assure the best integration with other network functions composing the slice.

	Novelty	High
	Exploitability	Medium

REQ_PLUG_AND_PLAY_04		
eHealth Use Case	Name	Access to lifecycle management of proprietary network function(s)
	Description	The SliceNet P&P Control COULD offer the possibility to directly manage the lifecycle of the proprietary network functions instantiated in end to end slice instances. This could enable the slice consumer to have higher control and management of its slice resources and functions in specific critical scenarios, like natural disasters.
	Justification	The slice consumer (e.g. the health services provider) could apply its own scaling logics to the proprietary network functions according to real-time eHealth services' needs (e.g. increase the number of BlueEye and facial recognition VNFs when high density of connected ambulances in the same geographical area).
	Novelty	High This will represent high novelty as there will be smart functionality available for the health scenarios.
	Exploitability	High Digital service providers will be able to offer this as a value-added service.

REQ_PLUG_AND_PLAY_05		
eHealth Use Case	Name	Access to primitives/APIs for network traffic control
	Description	The SliceNet P&P Control COULD offer dedicated control primitives to allow the slice digital service provider have access to network traffic control, at least from a predefined set of configuration options. The aim is to ensure, from a consumer perspective, that latency is minimised by selecting the optimal network configuration.
	Justification	Although it is envisaged that for eHealth use case purposes the slice network traffic control will be delegated to the slice provider cognitive techniques (to guarantee QoS/QoE), this could P&P control feature could help to assure that there is continuous ultra-high-definition video along with full duplex voice between the paramedic ambulance and hospital. In the case of the connected ambulance it will be important to ensure continuous video stream to the medic based in the hospital when assessing the situation at the scene.
	Novelty	Medium
	Exploitability	High Digital service providers will be able to offer this as a value-added service.

Annex B 5G Technologies Business Requirements and Expectations Survey

B.1 Smart Grid Survey

B.1.1 Survey Template

The purpose of this questionnaire is to gather user requirements and expectation in the context of the new 5G technology introduction.

About Efacec Mission & Role in the project

EFACEC (www.efacec.com), a company of the EFACEC Power Solutions Group, the largest Portuguese group in the electromechanical area. The automation in distribution with self-healing solutions is surely a critical challenge to consider in this transformational evolution towards Smart/Smarter Grid. Self-healing will enable system operators to benefit from a significant reduction in the outage duration, number of affected customers as well as in the number of switching manoeuvres required during network reconfiguration procedure involved in Fault Detection Isolation and service Restoration (FDIR).

Smart Grid Self-Healing presents several technical challenges. Concerning the grid automatic reconfiguration based on advanced FDIR algorithms (one of the main features), this process is influenced by the switchgear technologies available and by the high availability and very low-latency communication capability of the ICT infrastructure. Concerning communication, the achievement of the desirable level of response for the implementation of distributed Self-Healing solutions based in peer-to-peer communications, with ultra-low-latency and high availability and reliability, involves nowadays' high investment in dedicated communication networks, managed by the utility.

Alternatively, the use of public, namely 5G mobile networks to support those communications emerges as a new paradigm within the scope of utilities critical systems' management, since it allows deployments almost anywhere in the grid, without changing the present communication framework. Meanwhile, the use of public networks to provide critical data communications raises some concerns, mainly related with cyber security and quality of service – namely signal coverage, availability and latency. In particular, latency is extremely important, once in power systems protection the management of switchgear devices imposes severe latency and time-delay requirements concerning communication, hardly satisfied by the present communication infrastructures. Moreover, for the use of public networks to support the communications in management of electrical energy critical infrastructures it is crucial to gain the confidence of the system operators, in exchanging their very specific critical data over a shared network, reinforcing the need for higher cyber-security and intrusion guaranties from network providers. All these challenges entail investments that must be cost effective which should take into account the global revenue achieved through system's reliability improvement. Within the SliceNet project (www.slicenet.eu), Altice Labs (formerly Portugal Telecom Innovation) and EFACEC will be responsible jointly to deploy in laboratory this 5G Smart Grid Self-Healing use case in Portugal. Altice Labs 5G SliceNet infrastructure will be integrated with the EFACEC Smart Grid hardware/software components for the demonstrator.

5G short overview:

5G technologies have the potential to offer ubiquitous access, rapid provision of end-to-end services and increased data speed. 5G also adds a key technological capability: definition of a dedicated and adaptive virtualized network and IT infrastructure with embedded security tailored to the need of the business (higher bandwidth, lower latency and reduced jitter) through the whole lifecycle.

This truly enables the digital transformation that will provide to the society unprecedented capabilities for communication supporting very high bit rates, low latencies, huge device densities, ready for cloud-based services, virtual reality, augmented reality, artificial intelligence, factory automation, utilities, agriculture, self-driving and self-slice network management. 5G will enable new use cases through new business models and verticals with a fundamental reduction in overall costs and operational efficiency increase, making the technology sustainable through enabling value creation for customers.

The 5G Key Performance Indicators are the following:

- 1000 times higher mobile data volume per geographical area.
- 10 to 100 times more connected devices.
- 10 times to 100 times higher typical user data rate.
- 10 times lower energy consumption.
- End-to-End latency of < 1ms.
- Ubiquitous 5G access including in low density areas

5G is intended to deliver solutions, architectures and technologies for the coming decades with huge potential of creating new markets, business models and innovation opportunities and actions in areas such as Smart Grids, Smart Cities, e-Health, Intelligent Transport, Education, Agriculture, Media and Entertainment.

A European Commission¹² study reveal that the benefits of 5G for automotive, healthcare, transport and utilities sector in Europe starting from 2025 are estimated at 113 billion per year.

Questionnaire:**1. Company description and activities, yearly turnover estimate:**

a. Please select the main activity(ies)

- Power Generation
- Power Transmission
- Power Distribution
- EScO
- Retail
- Other(s) (please specify)

¹² Identification and quantification of key socio-economic data to support strategic planning for the introduction of 5G in Europe, A study prepared for the European Commission DG Communications Networks, Content & Technology

Turnover: [_____]

Select number of employees:

- <10 10 ÷ 100
 101 ÷ 1000 >1000

2. Communication solution:

- a. Please select the key features for the communication solution in order to meet your current or/and future needs:
- Connections with guaranteed quality of service (e.g., bandwidth, delay, jitter)
 - Connections with best effort quality of service
 - Connections with rapid provision of new services
 - Connections with ultra-low latency (< 10 ms)
 - Connections with broadband access everywhere
 - Connections with high user mobility
 - Connections with ultra-reliable communications
 - Others: please fill in below
- b. Please select the communication solution(s) you have in place or intend to use:
- Internet/Intranet for office use (daily business)
 - Wi-Fi Hot Spots for visitors Internet Access
 - VPN solution with encryption capabilities
 - Smart City Platform (please further specify the application(s), e.g., smart lighting, smart metering, smart grid etc.)
 - Machine to machine communication platform
 - e-Health or mobile health applications
 - Electric power grid applications
 - Others: please fill in below

Please add here any other relevant details in case of "Electric power grid applications" or "Others"

3. Please rate the relevance of the 5G technology for your business:

- 1** **2** **3** **4** **5**

1) Very low, as we don't see any 5G business opportunities

- 2) Low, as we may consider 5G business opportunities
- 3) Medium, as we expect 5G business opportunities
- 4) High, as we shall consider 5G as an enabler for our business development
- 5) Very High, as we will contribute to 5G services definition

Please respond to questions 4-7 if you rated with grades 3-5 question 3.

4. Thinking of your current and future business which is the key enabler for migrating towards 5G solutions?:

	Degree of importance			
	Not important	Low	Medium	High
Cost efficiency	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
new business opportunities	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Opportunity to enhance your current business model	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Faster time to market for your products	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
No real key enabler, it will be market trend	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Please add here any other relevant details

- 5. Leveraging on the key enablers selected at question 4, please detail:**
- a. **how they could support your current business needs? (E.g do you consider that new 5G technologies could bring the right automation and optimize your current business operating costs?)**

b. which specific Electric Power Grid applications do you envision 5G technologies to foster your current business strategy

	No Impact	Medium Impact	High Impact	No response
Operations Management (SCADA/EMS/DMS, WFM, etc)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
VHV/HV Grid Protection and Control	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
MV Grid Protection and Automation (DA, FDIR, VVC, etc)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
LV Grid Automation	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
DER, Storage, Microgrids and/or EV infrastructure	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Asset and Maintenance Management (asset monitoring, CBM, etc)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Outage Management	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Metering	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Customer/Consumer Integration	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Smart City Integration	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Others	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

If others, please specify:

6. Leveraging on the key enablers selected at question 4, please detail

a. how they could support your future business needs? (E.g. Do you consider that 5G technology could enable new business models that you could be part of?)

b. which specific Electric Power Grid applications do you envision 5G technologies to foster your future business strategy

	No Impact	Medium Impact	High Impact	No response
Operations Management (SCADA/EMS/DMS, WFM, etc)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
VHV/HV Grid Protection and Control	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
MV Grid Protection and Automation (DA, FDIR, VVC, etc)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
LV Grid Automation	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
DER, Storage, Microgrids and/or EV infrastructure	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Asset and Maintenance Management (asset monitoring, CBM, etc)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Outage Management	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Metering	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Customer/Consumer Integration	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Smart City Integration	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Others	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

7. What is your amount of investments for new technologies introduction during the next three years (Euros)?

- <50.000 50.000 ÷ 500.000 500.000 ÷ 1.000.000 > 1.000.000

Please fill in more precise values if the case:

B.2 eHealth Survey

B.2.1 Survey Template

5G technologies have the potential to offer ubiquitous access, rapid provision of end-to-end services and increased data speed. It will provide to society unprecedented capabilities for communication supporting very high bit rates, low latencies, huge device densities, ready for cloud-based services, virtual reality, augmented reality, artificial intelligence, factory automation, utilities, agriculture, self-driving and self-slice network management.

CIT-Infinite (<http://iotinfinite.org/>) and its SLICENET partners are investigating how 5G technology can play an enabling role in the transformation of the delivery of healthcare through the design of better-connected, integrated and coordinated services. For example, our 5G “Connected Ambulance” concept aims to advance the emergency ambulance services as they develop new collaborative models with their healthcare stakeholders to help create improved experiences and outcomes for patients in their care.

We would appreciate it if you would fill out the following questionnaire on how 5G can transform healthcare. The survey should take between 5-10 minutes to complete. By completing this survey you are in with a change to win a €100 Amazon voucher.

Questionnaire:

1. Email Address:

2. Please provide us a short description of your organization and its activities:

3. Please provide a link to your company's web site:

4. Select number of employees:

- <10
- 10 ÷ 100
- 101 ÷ 1000
- >1000

5. Please select the communication solution(s) you have in place or intend to use:

- Internet/Intranet for office use (daily business)
- Wi-Fi Hot Spots for visitors Internet Access
- VPN solution with encryption capabilities
- Smart City Platform
- M2M communication platform
- eHealth or mobile health applications
- Others:

6. What does the new 5G concept represent for your organization?

7. What features do you consider useful for your current business needs?

8. In terms of 5G performance, please rank the following in order of preference.

	1st	2nd	3rd	6th
10-100 times higher typical user data rate	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Ubiquitous 5G access including in low density areas	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10 times lower energy consumption	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

10-100 times more connected devices	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
End-to End latency <1ms	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1000 times higher mobile data volume per geographical area	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

9. In the context of 5G potential offering please rate the importance of the following, considering: Strongly Disagree (1) Disagree (2) Neutral (3) Agree (4) Strongly Agree (5)

	1	2	3	4	5
Improved Cost Efficiency	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Increase Reliability	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Self-Management w/o need to communicate to service provider	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
High speed to market faster service creation time	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
More varied service capabilities	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

10. Please add any other relevant details here:

--

11. Do you believe that 5G technologies could accelerate your next business opportunities? If so, then please provide some examples:

--

12. Thinking of your current and future business which is the key enabler for migrating towards 5G solutions?

	Not important	Low	Medium	High
Cost efficiency	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
new business opportunities	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Opportunity to enhance your current business model	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
No real key enabler, it will be market trend	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

13. Please add any other relevant details here:

14. Please rate the relevance of the 5G technology for your business:

Mark only one oval.

- Very low, as we don't see any 5G business opportunities
- Low, as we may consider 5G business opportunities
- Medium, as we expect 5G business opportunities
- High, as we shall consider 5G as an enabler for our business development
- Very High, as we will contribute to 5G services definition

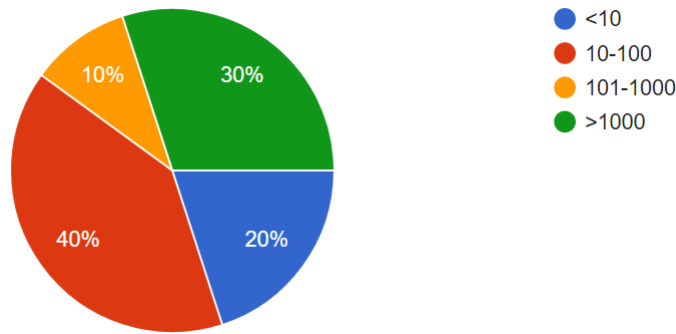
B.2.2 Survey Analysis

5G technologies have the potential to offer ubiquitous access, rapid provision of end-to-end services and increased data speed. It will provide to society unprecedented capabilities for communication supporting very high bit rates, low latencies, huge device densities, ready for cloud-based services, virtual reality, augmented reality, artificial intelligence, factory automation, utilities, agriculture, self-driving and self-slice network management.

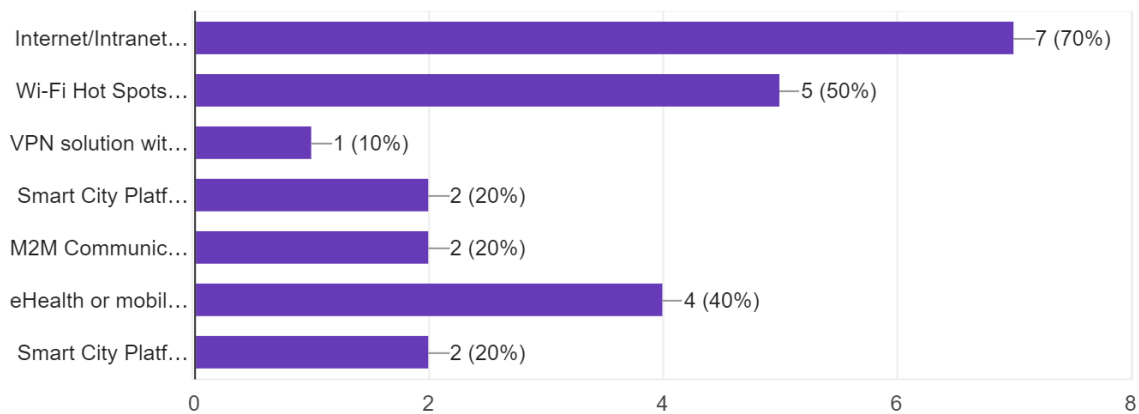
CIT-Infinite (<http://iotinfinite.org/>) and its SLICENET partners are investigating how 5G technology can play an enabling role in the transformation of the delivery of healthcare through the design of better-connected, integrated and coordinated services. For example, our 5G "Connected Ambulance" concept aims to advance the emergency ambulance services as they develop new collaborative models with their healthcare stakeholders to help create improved experiences and outcomes for patients in their care.

Preliminary results from 10 respondents.

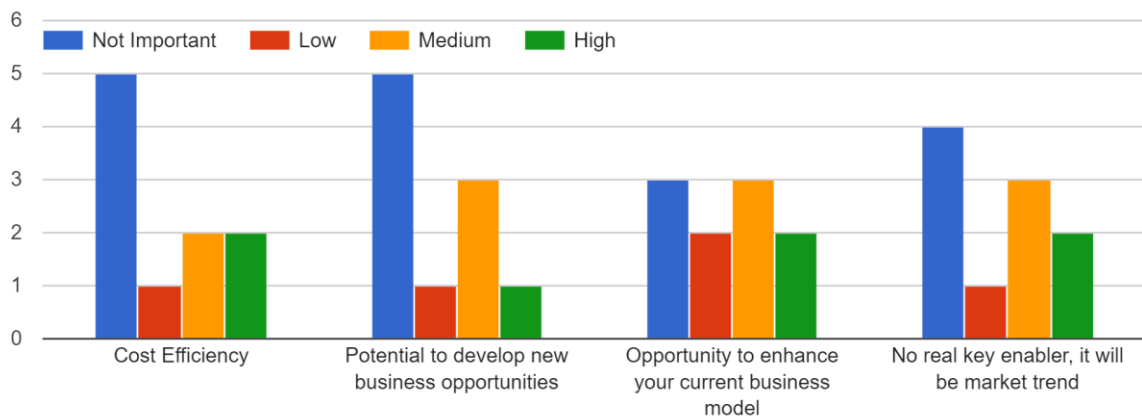
How many employees does your organisation have?



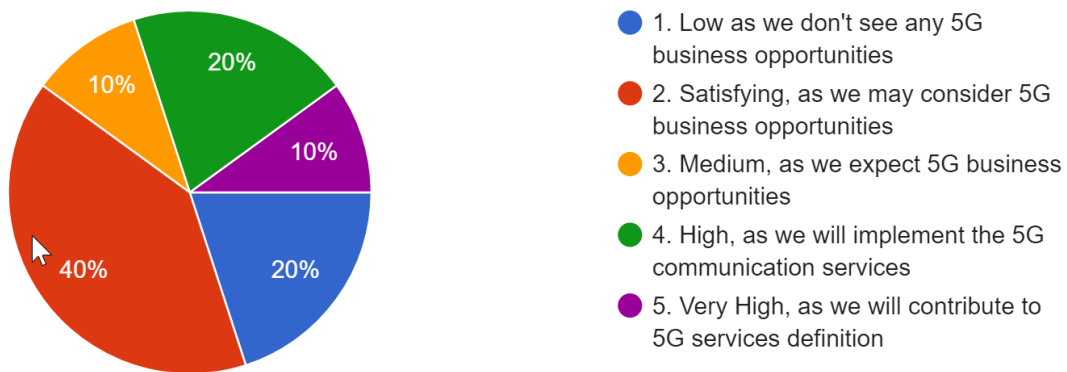
Please select the communication solution(s) you have in place or intend to use



When thinking of your current and future business, which is the key enabler for migrating towards 5G solutions?



Please rate the relevance of the 5G technology for your next generation communication services approach



B.3 Smart City Survey

B.3.1 Survey Template

The purpose of this questionnaire is to gather user requirements and expectation in the context of the new 5G technology introduction.

Orange Romania Mission

Orange Romania(www.orange.ro) is continuously involved in the development and the founding of new business opportunities, leveraging on the all new 5G ecosystem. Orange anticipates the implementation of the new 5G technology by being present in two projects, SLICENET (www.slicenet.eu) and MATILDA, part of EC H2020 research and innovation actions, and also in Working Groups that sustain the standardization for 5G. Orange strongly believes that 5G will be rather revolutionary that evolutionary and will disrupt the market as we know it. We are moving from the era in which the Telco provider is providing ubiquitous connectivity to the era in which the operator provides ubiquitous services and application sustained through strategic partnerships with the relevant stakeholders (application providers, verticals, etc.).

5G short overview:

5G technologies have the potential to offer ubiquitous access, rapid provision of end-to-end services and increased data speed. 5G also adds a key technological capability: definition of a dedicated and adaptive virtualized network and IT infrastructure with embedded security tailored to the need of the business (higher bandwidth, lower latency and reduced jitter) through the whole lifecycle.

This truly enables the digital transformation that will provide to the society unprecedented capabilities for communication supporting very high bit rates, low latencies, huge device densities, ready for cloud-based services, virtual reality, augmented reality, artificial intelligence, factory automation, utilities, agriculture, self-driving and self-slice network management. 5G will enable new use cases through new business models and verticals with a fundamental reduction in overall costs and operational efficiency increase, making the technology sustainable through enabling value creation for customers.

The 5G Key Performance Indicators are the following:

- 1000 times higher mobile data volume per geographical area.
- 10 to 100 times more connected devices.
- 10 times to 100 times higher typical user data rate.
- 10 times lower energy consumption.
- End-to-End latency of < 1ms.
- Ubiquitous 5G access including in low density areas

5G is intended to deliver solutions, architectures and technologies for the coming decades with huge potential of creating new markets, business models and innovation opportunities and actions in areas such as Smart Cities, e-Health, Intelligent Transport, Education, Agriculture, Media and Entertainment.

A European Commission¹³ study reveal that the benefits of 5G for automotive, healthcare, transport and utilities sector in Europe starting from 2025 are estimated at 113 billion per year.

Questionnaire:

1. Company description and activities, yearly turnover estimate:

Turnover: [_____]

Select number of employees:

- <10 10 ÷ 100
 101÷1000 >1000

2. Communication solution:

- a. Please select the key features for the communication solution in order to meet your current or/and future needs:
- Connections with guaranteed quality of service (e.g., bandwidth, delay, jitter)
 - Connections with best effort quality of service
 - Connections with rapid provision of new services
 - Connections with ultra-low latency (< 10 ms)
 - Connections with broadband access everywhere
 - Connections with high user mobility
 - Connections with ultra-reliable communications
 - Others: please fill below
- b. Please select the communication solution(s) you have in place or intend to use:

¹³ Identification and quantification of key socio-economic data to support strategic planning for the introduction of 5G in Europe, A study prepared for the European Commission DG Communications Networks, Content & Technology

- Internet/Intranet for office use (daily business)
- Wi-Fi Hot Spots for visitors Internet Access
- VPN solution with encryption capabilities
- Smart City Platform (please further specify the application(s), e.g., smart lighting, smart metering, smart grid etc.)
- M2M communication platform
- e-Health or mobile health applications
- Others: please fill in below

Please add here any other relevant details in case of "Smart City Platform", "M2M communication platform", "e-Health" or "Others"

3. Please rate the relevance of the 5G technology for your business:

- | | | | | |
|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|
| 1 | 2 | 3 | 4 | 5 |
| <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
- 1) Very low, as we don't see any 5G business opportunities
 - 2) Low, as we may consider 5G business opportunities
 - 3) Medium, as we expect 5G business opportunities
 - 4) High, as we shall consider 5G as an enabler for our business development
 - 5) Very High, as we will contribute to 5G services definition

Please respond to questions 4-7 if you rated with grades 3-5 question 3

4. Thinking of your current and future business which is the key enabler for migrating towards 5G solutions?

	Degree of importance			
	Not important	Low	Medium	High
Cost efficiency	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
new business opportunities	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Opportunity to enhance your current business model	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Faster time to market for your products	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
No real key enabler, it will be market trend	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Please add here any other relevant details

5. Leveraging on the key enablers selected at question 4, please detail how they could support your current business needs? (E.g do you consider that new 5G technologies could bring the right automation and optimize your current business operating costs?)

6. Leveraging on the key enablers selected at question 4, please detail how they could support your future business needs? (E.g. Do you consider that 5G technology could enable new business models that you could be part of?)

7. What is your amount of investments for new technologies introduction during the next three years (Euros)?

<50.000 50.000 ÷ 500.000 500.000÷1.000.000 > 1.000.000

Please fill in more precise values if the case:

B.3.2 Survey Analysis

Orange Romania built a Survey Template Questionnaire structured in 3 parts:

- Overview of Orange Romania mission in the context of 5G
- Overview of 5G main benefits
- Set of question to be answered by the interviewees which are depicted in Table 13 together with their relevance

Table 13 5G Survey Questionnaire and relevance

Question	Relevance
1. Company description and activities, yearly turnover estimate, number of employees	Size of the company & domain in which the company is present
2. Communication solution: a. Please select the key features for the communication solution in order to meet your current or/and future needs: b. Please select the communication solution(s) you have in place or	a. Understand which are the most relevant 5G performance advantages for the interviewees b. Overview the status quo in terms of communication solution.

intend to use:	
3. Please rate the relevance of the 5G technology for your business.	Rate the relevance of 5G technology for the interviewee and based on the grade pass to the next questions in the survey
4. Thinking of your current and future business which is the key enabler for migrating towards 5G solutions?	Understand the business rationale for the interviewee to migrate to the 5G technologies
5. Leveraging on the key enablers selected at question 4, please detail how they could support your current business needs? (E.g do you consider that new 5G technologies could bring the right automation and optimize your current business operating costs?)	Complement the business rationale from question 4 with the details in order to extract better the advantages the interviewees expects from 5G technology for their current business model.
6. Leveraging on the key enablers selected at question 4, please detail how they could support your future business needs? (E.g. Do you consider that 5G technology could enable new business models that you could be part of?)	Complement the business rationale from question 4 with the details in order to extract better the advantages the interviewees expects from 5G technology for their future business need.
7. What is your amount of investments for new technologies introduction during the next three years (Euros)?	Understand the potential of investment for new technologies (not necessarily 5G)

The questionnaire was sent to different businesses from Romania active in various domains. The name of the business partner will not be disclosed; however Table 14 depicts the domains and few details about the company objectives. For sake of clarity in Table 14 only the company that responded to the survey are included. Also, it is relevant to note that the survey was run in parallel on three channels: email, phone and face to face meetings. This assures that each of the companies had all the details and clarification needed in order to provide relevant responses for the survey.

Table 14 Group of responders

Responder	Domain	Objective
Company 1	cyber security	Provides variety of services including penetration testing,, trainings and competitions.
Company 2	service integrator	Provides integration services to business mainly based on Cisco equipment
Company 3	cyber security	Provides penetration tests as a service
Company 4	equipment provider	Multinational company offering full solutions for connectivity for FTTA (fibre to the antenna), overvoltage protection and outdoor power cabinets for telecommunication operators and OEM companies.
Company 5	automotive	Multinational company providing automotive parts
Company 6	e-health	Researching and developing different 3D machinery for additive manufacturing with plastic, metal and biomass.
Company 7	air transport services	Flight operator owning aircrafts and part of International Air Transport Association (IATA)
Company 8	Smart City	Service Consumer for Smart City use case

Analyzing results

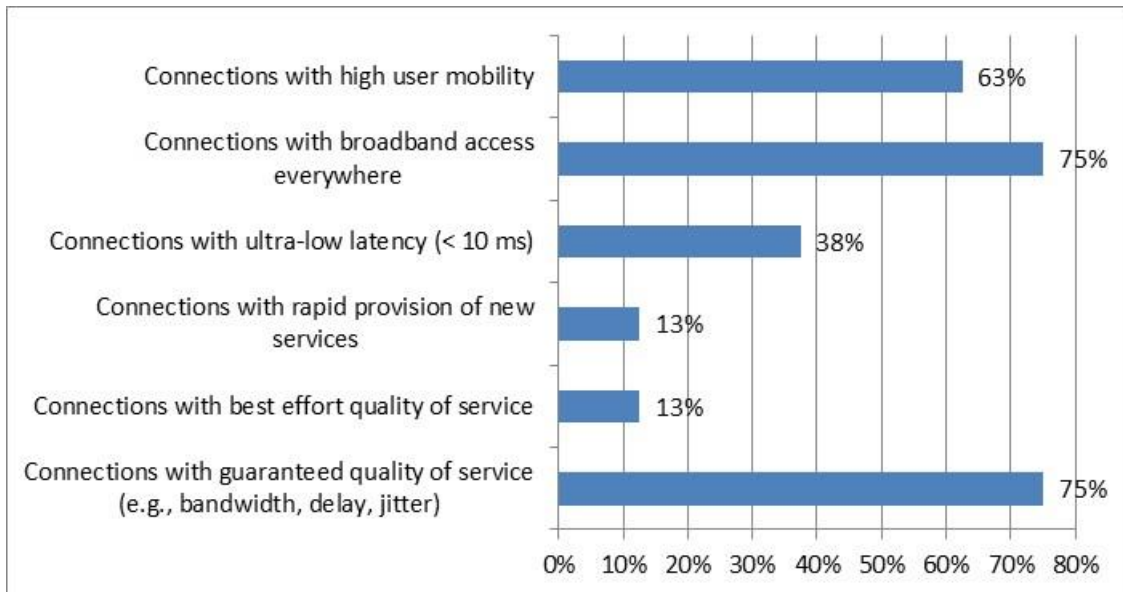
Table 15 depicts the gathered responses.

Table 15 Questionnaire centralized responses

	Comp. 1	Comp. 2	Comp. 3	Comp. 4	Comp. 5	Comp. 6	Comp. 7	Comp. 8
1. Company description and activities, yearly turnover estimate, number of employees	small enterprise	medium enterprise	small enterprise	large enterprise	large enterprise	small enterprise	large enterprise	public institution
2a. Please select the key features for the communication solution in order to meet your								
Connections with guaranteed quality of service	yes	yes		yes	yes	yes		yes
Connections with best effort quality of service						yes		
Connections with rapid provision of new services						yes		
Connections with ultra-low latency (< 10 ms)					yes	yes	yes	
Connections with broadband access everywhere		yes	yes	yes		yes	yes	yes
Connections with high user mobility				yes	yes	yes	yes	yes
Connections with ultra-reliable communications				yes	yes			
Others: please fill below								
2 b. Please select the communication solution(s) you have in place or intend to use:								
Internet/Intranet for office use (daily business)	yes	yes	yes	yes	yes	yes	yes	yes
Wi-Fi Hot Spots for visitors Internet Access	yes	yes		yes	yes	yes	yes	yes
VPN solution with encryption capabilities	yes			yes	yes	yes	yes	yes
Smart City Platform								yes
M2M communication platform		yes		yes		yes		
e-Health or mobile health applications						yes		
Others: please fill in below								
3. Please rate the relevance of the 5G	1	4	1	4	5	5	3	3
4. Thinking of your current and future business which is the key enabler for migrating towards 5G								
Cost efficiency		medium		medium	N/A	medium	medium	medium
new business opportunities		high		high	high	high	low	high
enhance current business model		medium		high	N/A	high	medium	medium
Faster time to market		medium		medium	N/A	high	low	low
No real key enabler, market trend		N/A		not important	N/A	high	not important	medium
5. Leveraging on the key enablers selected at question 4, please detail how they could support your current business needs? (E.g. do you consider that new 5G technologies could bring the right automation and optimize your current		low latency, high bit rate		M2M communication enhancements	N/A	remote operation of medical equipment	robotic process automation	N/A
6. Leveraging on the key enablers selected at question 4, please detail how they could support your future business needs? (E.g. Do you consider that 5G technology could enable new		virtualization		smart cities	autonomous driving	working collaborative on medical equipment	N/A	N/A
7. What is your amount of investments for new technologies introduction during the next three years (Euros)?		50.000-500.000		500.000-1.000.000	over 1mEur	50.000-500.000	50.000-500.000	<50.000

We can observe from Figure 40 that more than 60% of the responders consider that the following features are key in the context of 5G technology:

- Connection with high user mobility
- Connection with broadband access everywhere
- Connection with guaranteed quality of service



**Figure 40 Key features and relevance for responders
(% of responders selected the key features)**

From 8 responders only 6 considered that the 5G technology will be relevant for their business, hence the results presented hereinafter refer to these 6 companies. The two companies which responded that 5G technologies is not relevant are both small enterprises active in the domain of cyber security, mainly handling penetration tests. In this context, they do not consider that 5G shall change or affect their operating model, which is not necessarily true considering the high degree of virtualization 5G brings.

The 6 responders graded on an importance scale (not important, low, medium, high) the key enablers for migrating towards 5G solutions. The statistics can be found in the next graphs below.



Figure 41 5G Key enabler - business model & cost efficiency statistics

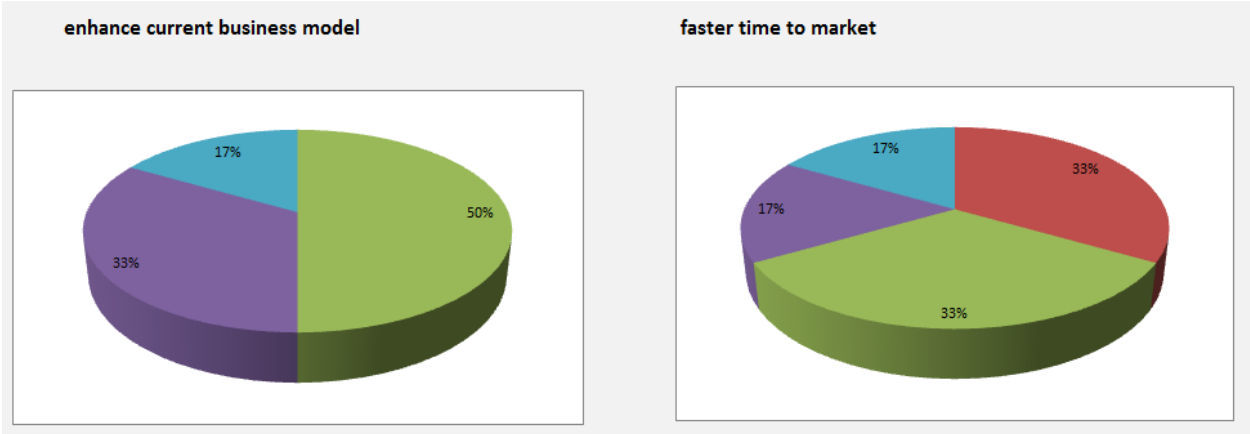


Figure 42 5G Key enabler – enhanced business model & time to market

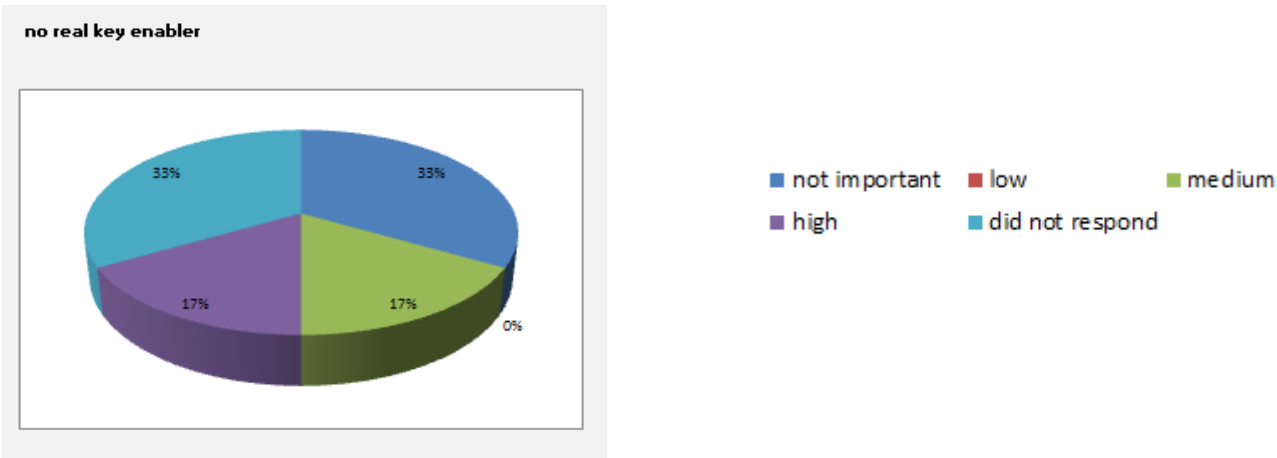


Figure 43 5G market trend relevance

Over 80% of the responders consider that 5G will enable new business models and hence new lines of revenues. This is key for a business in a competitive market; it could be observed that this enabler was preferred in the detriment of cost efficiency. Leveraging on 5G technology, the responders see a high potential in the following areas: virtualization, smart cities, autonomous driving, collaborative working on medical equipment (regardless the location).

In terms of investments, the responders are reserved, only one considers an investments of over 1mEur. However, this should not be taken as reference, as there are many unknown aspects at this point in time related to costs and solutions.

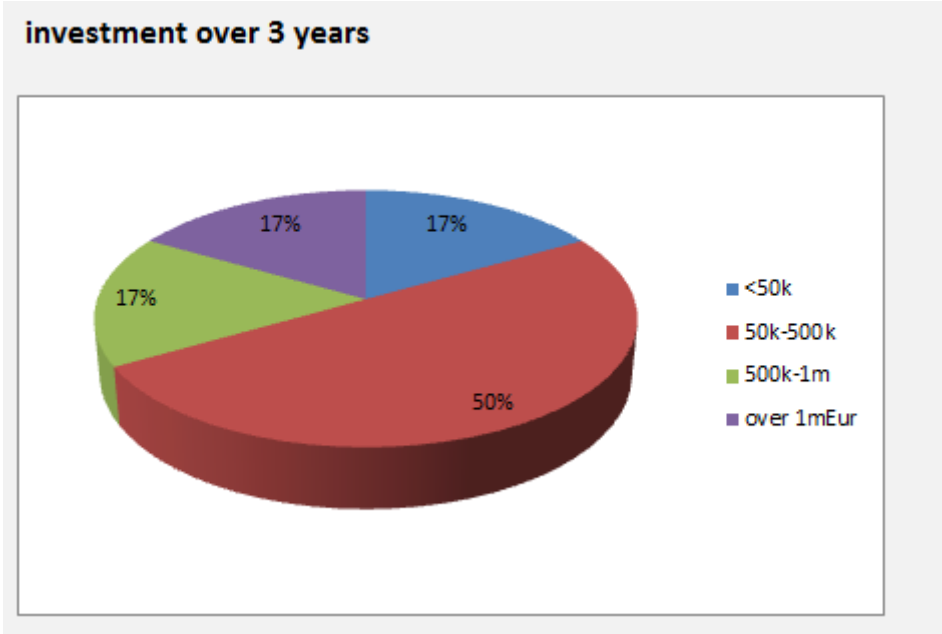


Figure 44 New technology investments estimation

[end of document]